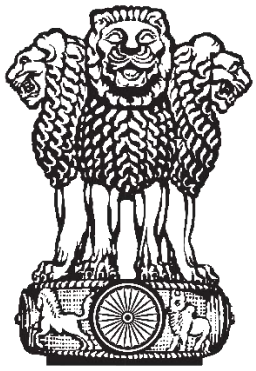
Version 5.0 – Final

09 October 2014



सत्यमेव जयते

NATIONAL INFORMATION SECURITY POLICY AND GUIDELINES

MINISTRY OF HOME AFFAIRS

GOVERNMENT OF INDIA

Disclaimer

The Ministry of Home Affairs (MHA), Government of India, is aware of the cyber security policies, guidelines, and standards as identified and practiced by various government organizations in India. The role of MHA is specialized and focuses on establishing guidelines to help secure the "information" which may impact internal security and national security. These guidelines are based on the analysis of existing global security standards, and frameworks; and the emerging trends and discourse in the wake of persistent threats, and cyber-attacks on critical infrastructure of nations globally.

The scope of MHA's "National Information Security Policy & Guidelines" encompasses Government and Public Sector organizations and associated entities and third parties, for protecting the information under their control or ownership during information's life-cycle including creation, storage, processing, accessing, transmission, destruction etc.

The objective of this document is to improve the information security posture of an organization possessing any information, including classified information, and does not restrict organizations from adopting additional stringent practices over and above these guidelines. Organizations may evaluate various additional measures for the security of information they possess for protecting their information depending upon the sensitivity, criticality and importance of such information in the overall Internal Security and National Security interest of the country.

Foreword

Ministry of Home Affairs (MHA) has been designated as the lead agency for the protection of the "Information" in Cyberspace. The Ministry is tasked with finalizing and issuing guidelines on the codification and classification, of information, and keeping it updated in the ever expanding cyberspace. Earlier, MHA has issued the manual of departmental security instructions 1994 which is presently applicable and is being used today by all the Government Ministries/departments/agencies.

The government at all levels, central, state and local, is increasingly using Information and Communication Technologies (ICT) to enhance productivity, improve efficiency in service delivery, speed-up development in all sectors of economy and improve the governance while safeguarding overall Internal Security and National Security interests of the country.

Paper based records, which were earlier held in the files and filing cabinets, are now created, stored, processed, accessed, transmitted and destroyed in electronic formats. Such information can be accessed from different parts of the country by authorized personnel; however, this information is also vulnerable to unauthorized access which can compromise confidentiality, availability and integrity of information through cyber-attacks from anywhere in India or from outside the Indian borders. Adoption of international standards and best practices for security of information in the complex and borderless cyber space has, therefore, become paramount to protect national information assets in the overall national security interest. This is more important for organizations dealing with strategic information related to internal security, national security, economic security, and external affairs which handling large data/ information in electronic format. Also, the critical infrastructures such as power, banking and finance, telecommunications, transport, air traffic control etc., which are using ICT for increasing efficiency and productivity, are prone to cyber-attacks. This can have a crippling effect on the nation's stability, economy and security.

This policy document on "National Information Security and Guidelines 2014" includes a comprehensive review of the "Manual on Departmental Security Instructions" of 1994 for the present day information security requirements in the Cyber space to address the above mentioned challenges. It will serve as an extension to the existing "Manual on Departmental Security Instructions", 1994 which primarily addresses the handling of the security of paper based information.

The National Information Security Policy and Guidelines (NISPG) has been prepared by the Ministry of Home Affairs, based on the experience of the existing security standards and frameworks and the global best practices and experience of implementation in the wake of expanding information security threat scenario. This policy document will supplement the existing guidelines issued by DeitY, NIC, IB and NTRO for the security of ICT infrastructure, assets, networks, applications, user management, email etc. I hope that the organizations directly involved in handling the information in any form, including the digital form, which is relevant to the internal security and national security shall implement these guidelines and make further suggestions, if any, to improve the next version of NISPG.

(Anil Goswami)

Union Home Secretary

Executive summary

The digital world is a reality today in all aspects of our lives. Digital infrastructure is the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments and free societies. Lacs of people across the country rely on the electronic services in cyberspace every day. As never before, Information and Communication Technology (ICT) is fostering transnational dialogue and facilitating the global flow of information, goods and services. These social and trade links have become indispensable to our daily lives as well as the economy of our country. Critical life-sustaining infrastructures that deliver electricity and water, telecommunication, Internet and broadband connectivity, control air traffic, and support our financial systems all depend on networked information systems. The reach of networked technology is pervasive and global. For all nations, the underlying digital infrastructure has become a critical national asset. Therefore improving and securing this digital infrastructure in all its dimensions including increased availability of next generation broadband connectivity, citizen/ customer centric applications and services, security of information, is critical to India's future.

Traditionally, information available with the government has been safely managed by keeping it in paper records throughout its lifecycle i.e. creation, storage, access, modification, distribution, and destruction. However, to make all government services accessible to the common man in his locality, through efficient service delivery outlets, along with transparency & reliability, the government has steadily graduated towards using electronic formats of information. Now, several forms of information have been converted to the electronic format by the ministries, departments and agencies, both in the central as well as state governments. The classification, storage and protection of such information in electronic format have always remained an area of concern. The challenge, as with the information contained in paper format, remains the same, namely the ability to categorize, protect, archive, discover, and attribute information during its useful life and eventual destruction. Even though the lifecycle of information remains the same in electronic documents and online transactions, the methods to secure information in electronic environment are different. In the present age, the "Manual of Departmental Security Instructions", issued in 1994, is no longer sufficient to protect against the threats facing electronic forms of information.

Information security is one of the important components of cyber security and is gradually taking centre stage in the national security deliberations and discussions. In fact, it has become a key component of national security design and is shaping international strategies of nations globally. Threats to information are increasingly organized and targeted, helping criminals, state actors and hacktivists to reap immense benefits out of information compromise, theft or espionage. Cybercriminals can carry out identity theft and financial fraud; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals or disrupt critical infrastructures by exploiting the vulnerabilities in any system connected to the Internet. The cybercriminals could be located anywhere in the world and they can target a particular user, system or a particular service in a country or a region. Worse still, the cybercriminals can cover their tracks so that they cannot be traced. It is extremely difficult to prove whether the cybercriminal is an individual, a gang, a group of state actors or a nation-state.

As the government broadens the scope of its drive to move towards e-governance and embraces technology for citizen-centric services, it faces threats from multiple sources. Each government process or project introduces a different level of complexity as a result of varied data transactions,

involvement of multiple players, and exposure to increasing compliance requirements, diverse operational and infrastructure environments and embracing of technological innovations. This complexity is true of the private sector as well, even though they are early adopters of technology and innovation. Such complexity associated with the lifecycle of information poses serious challenges in managing and governing security and ensuring compliance. Thus, it is essential to establish a focused policy initiative for the security of information and to sensitize public and private sector towards national security concerns and drive their actions for securing information. This will not only secure the IT systems but also instill trust in IT services provided by the government agencies, which can further expand and help in improved e-governance services to various stakeholders.

Information security brings up a set of different problems that have the potential to challenge the comfort in the conventional methods of managing security concerns. Cyber threats do not respect physical boundaries. They explore and innovate, discovering new methods for compromising security. Further, the identity of the attacker and the source is difficult to ascertain. Attribution in cyberspace has emerged as an intimidating challenge. In most cases, it is extremely difficult to collect irrefutable evidence against a cyber-attacker, and almost impossible to link any cyber-attack to nation-states, even if clearly established.

Current symptoms of problem in India

Securing sensitive information is important for the strategic security and defense of a country. Economic stability of the country depends on uninterrupted operations of banking and finance; critical infrastructure such as power generation and distribution, transport systems of rail, road, air and sea; which in turn are critical dependent on ICT. It is important for national security and continued prosperity of people. For example, the financial sector in India uses ICT extensively – it is an early adopter of leading and emerging technologies. It is not surprising to note that intellectual property developed both in public and private sector also contributes to the economic growth of a nation in a knowledge based economy. Cyberattacks are specially targeted at companies and organizations to steal intellectual property in what is known as economic espionage. Malware like Stuxnet and Flame have provided evidence of cyberattacks leading to kinetic and long lasting damage to strategic capabilities of a nation, and of espionage, respectively.

The public sector, although increasingly relying on ICT, has not fully awakened to the challenges of information security. The private sector, which makes investments in information security for intrinsic requirements, needs to ensure that these security practices are also aligned with national security concerns. So far, even though focus has been on improving ICT systems and providing e-governance services by various institutions, the IT systems and business processes have not placed the desired emphasis on Information Security. The time has come to drive both sectors towards a strong information security culture, which is sensitive to national imperatives. There have been revisions of Departmental Security Instructions and Guidelines from DeitY, IB, NIC and NTRO to streamline and tighten up the various aspects of documentation, personnel and physical security procedures. However, a comprehensive approach for managing information security was missing.

Consideration of the underlying causes of the problem

Information security is not merely a technology problem; it requires alignment with organizational processes as well as the legal and regulatory framework in the nation. However, for successful and

optimized implementation of security, organizations need to weigh their strategic and financial options, establish a policy framework to set directions, define or comply with standards for ensuring baseline, establish procedures for ensuring consistency of operations and issue guidelines for implementation which must be carried out in spirit, and not just for the sake of obtaining a certificate. The compliance to the defined Information Security (IS) processes/ guidelines needs to be periodically audited both by internal and external auditors. Organizations are yet to awaken completely to embrace these challenges and incorporate measures and align their efforts to the cause of national security. The drivers for security go beyond securing ICT assets and protection of intellectual property rights (IPRs), where public and private entities have invested the bulk of their resources and efforts. Cyber Security and National Security require adequate priority and attention from organizations, beyond their usual areas of focus. Information security policy measures should address the requirements of legal framework, provide strategic measures and develop a mechanism to address various problems related to standards, procedures and guidelines. The policy needs to be aligned to the requirements of National Security, Cyber Security, IPR and Privacy protection.

The National Information Security Policy and Guidelines

Ministry of Home Affairs (MHA) has been entrusted with the responsibility of coordinating and overseeing information security initiatives of public as well as private sector. It is empowered to create a National Information Security Policy and Guidelines (NISPG), define procedures for handling information and issue guidelines for security of classified information assets. Accordingly, a Cyber Security Committee under the chairmanship of JS (P-II), MHA with members from other stakeholder organizations was formed for this purpose. However, draft guidelines on protection of information in cyberspace and codification and classification (of electronic documents), prepared by this committee was not found to be comprehensive. In view of the fact that MHA and Intelligence Bureau (IB) do not have in-house expertise to handle a highly technical and advanced subject like this, it was proposed to outsource the work to National Institute of Smart Governance (NISG)/Data Security Council of India (DSCI) to develop a robust and comprehensive policy document, given DSCI's experience in developing the DSCI Security Framework (DSF©), which was formulated in consultation with the Indian Industry which has experience in offering secure IT solutions to clients in over 90 countries, and DSCI's engagement with International Standards Organization (ISO) in the development of global security standards

The work plan for creation of NISPG included a study of existing laws, regulations and practices within the Government of India, international best practices followed worldwide and security requirements of various regulatory bodies. A review of global best practices, frameworks and information security standards was undertaken to understand and incorporate global learnings and align the developed practices with the same. Two workshops involving senior representatives from about 40 public sector organizations and Industry were also conducted, in addition to receiving their inputs over email. Based on learnings from these frameworks, emerging disciplines, and viewpoint of the industry, specific guidelines and detailed control objective and statements have been developed. This policy document will supplement the existing guidelines issued by Deity, NIC, IB and NTRO for the security of ICT infrastructure, assets, networks, applications etc. and would serve as an extension to the existing Manual on Departmental Security Instructions of 1994, which primarily addresses the handling of the security of paper based information.

Approach

This document elaborates baseline Information security policy and highlights the relevant security concepts and best practices, which government ministries, departments, and organizations must implement to protect their information. The policy recommends creation of a security division within each government organization, with the responsibility of planning, implementing and governing all tasks related with information security in a comprehensive and focused manner. The security division is expected to perform risk analysis based on threat and risk assessment emanating from the adoption of technology. Further, the document provides guidance and control objectives aligned in eight main domains and six additional areas which form the core of information security practices and frameworks globally. These domains are essential for implementation of an effective information security program, since they address the specifics which have become essential for its effectiveness. The contribution of each domain to the success of the information security program is intertwined with the level of maturity and success of all the other domains. Thus, together they help create a baseline for a robust information security program.

The following core domains have been covered as part of this document. These are:

1. Network and Infrastructure security
2. Identity, access and privilege management
3. Physical security
4. Application security
5. Data security
6. Personnel security
7. Threat and vulnerability management and
8. Security and incident management

Further, guidelines have been provided for technology specific ICT deployment and trends:

1. Cloud computing
2. Mobility and Bring Your Own Device (BYOD)
3. Virtualization
4. Social media

Additionally, guidelines for essential security practices have been provided:

1. Security testing
2. Security auditing
3. Business continuity
4. Open source technology

Each domain is supported by a brief introduction about its relevance to information security along with an outline of the importance of establishing practices pertinent to that domain. This is supported by essential guidelines which encompass various processes and procedures under which the information may traverse during its lifecycle.

The guidelines are reinforced with the help of specific control objectives and statements which will help organizations initiate their journey towards establishing a security baseline and further help them in obtaining maturity in these practices. To help the readers of this document appreciate the work already undertaken globally in the field of information security, the annexures have been updated with a brief summary of some globally accepted information security frameworks, standards and practices. The readers can comprehend the guidelines and controls provided in this document, from the detailed chart which provides mapping of guidelines and controls mentioned in this manual with that of other globally accepted frameworks, standards, practices and controls such as ISO 27001 (2005 as well as 2013), SANS 20, NTRO 40 and FISMA. There are 112 different guidelines and 135 controls and 181 implementation guidelines defined in NISP as against 133 controls in ISO 27001, 40 controls defined by NTRO, 20 controls by SANS and about 200 controls by FISMA. Further, some guidance has also been provided on the methodology which may be used by the organizations for carrying out risk assessments for the purpose of information security.

The first and second drafts of the "National Information Security Policy and Guidelines" (NISPG) were circulated by MHA in January 2014. Since then, feedback and suggestions have been received from various ministries, departments and agencies on the guidelines contained in the NISPG. The feedback received has provided valuable insight into specific areas to improve the guidelines. Further guidance was added in Version 3.0 of the document encompassing areas such as business continuity, security testing and security audits. Additionally, guidance on securing technology specific areas has also been incorporated, based on the feedback received from various departments. These guidelines include security measures for cloud computing, BYOD and virtualization. In the current version i.e. NISPG 4.0, implementation guidelines have been added to help organizations in comprehending requirements of each domain, along with additional controls and areas that have emerged after the feedback from some other government agencies.

Establishing visibility over information and its lifecycle

Organizations need to establish a process of identification and discovery of information at each of its operational processes, relationships and functions. Information is an empowerment and has a strategic as well as an economic value associated with it. The security posture of the organization has to be dynamic and should evolve with the change in the value of information, underlying ICT infrastructure, information access methods and threat ecosystem. It should have the ability to address the security requirements of all data transactions across all possible data leakage scenarios. The security solutions should help address security of information, not only at the different layers of ICT infrastructure, but also in the extended operational ecosystem, i.e. other ministries and agencies may be given access to information. This should also provide guidance for securing emerging technology platforms such as mobility, cloud computing, virtualization etc. While designing the strategy for security, information centric approach in operational lifecycle should be an important consideration. The identified information item and its characteristics such as its origin, sensitivity, strategic and economic value, geography of operation, access methods and the department(s) or the financial ecosystem within which transactions take place along with the operations performed on the information help identify the security requirements.

Developing an information centric security framework

The consideration of information security in the life cycle is important from people, process and technical design perspective. Information can be classified based on its category or type, sensitivity,

value and the context throughout its life cycle. The departments should ensure that there exists a structural thought process in designing information security initiatives, such that adequate measures are taken with respect to formation, grouping and arrangement of countermeasures for security of information. It is also important that adequate efforts are taken for integrating information security measures with the enterprise ICT architecture to address contemporary and changing threats to information. Moreover, an organization should have capability towards responsiveness to the new issues or threats through integrating internal and external intelligence measures, deployment of tools, techniques and methods in identifying threats, collaboration mechanisms which generate timely and desired response from other security and ICT infrastructure management processes. Finally, departments should have the ability to identify, alert, evoke responses and resolve a data breach in a timely manner. This requires integration with other security processes and ICT infrastructure management processes, arrangement and relationships with external parties or bodies and standardization of procedures defined and deployed for handling data breaches. To make all this possible, departments need to focus on establishing accountability through design and implementation of an ownership structure for information security, where tasks and responsibilities are clearly distributed with respect to administrative and technical arrangements required for information security.

The way forward

Increasing digitization of information, expanding exposure of government organizations due to connectivity and the use of external providers, rising dependence on the global ICT supply chain are posing serious threats to information security. Growing instances of cyber espionage involving serious information breaches, call for action at a higher level. The Government of India recognizes this challenge – more so in the context of national security.

National Information Security Policy and Guidelines, which focuses on security of information possessed both by public (Government and PSUs) and private sector, is an important step towards achieving new age goals of national cyber security. The policy is directed to build and foster an ecosystem for information security in the organizations (operating in public as well as private domain) that addresses the National Security requirements.

Dr. Nirmaljeet Singh Kalsi,
Joint Secretary (Police-II) and

Chief Information Security Officer
Ministry of Home Affairs, Government of India

A. Version Control

Version Number	Version Details	Identifier	Date
1.0	Final Draft	Final draft	17 January 2014
1.1	Final Draft	Additional annexures added to Final Draft Change 1: Annexure added – Mapping Of Guidelines and Controls Mentioned In the National Information Security Policy Change 2: Annexure added – Mapping of ISO27001:2013 with NISP controls Change 3: Annexure added – Mapping of NISP Guidelines & Controls with NIST Cyber Security Framework	19 February 2014
2.0	Final Draft	Change 1: Annexure added – Information Security Control Matrix Change 2: Revision of guideline titles for G11, G18, G30, G32, G37, G51, G54, G61, G62 Change 3: Revision of guideline text for G1, G10, G11, G13, G36 Change 4: Revision of control titles for C9, C11, C12, C15, C33, C36, C45, C50, C69, C76, C78, C99, C101, C102, C106, C121, C122, C123 Change 5: Revision of control text for C18, C26, C100	21 February 2014
2.1	Final Draft	Added section 1.5 - Information security – focus areas Added section 3.3 - National information security policy and guidelines review and update Revision of text of section 4 - Scope Added section 6.2 - Security Risk Assessment Revision of title for section 6.3 as Principles for establishing security framework	21 March 2014

		Added section 6.3.1 – Core security goals Revision of title for section 6.4 as Security audit Revision of title for section 6.4.1 as Security audits Added section 6.4.3 – Coordination with agencies Added section 6.5 - Exception to implementation of recommended guidelines and controls Revision of text of section 8.1 – Security division	
3.0	Final Draft	Revision of text of section 10 – Domains impacting information security under section 10.9 and 10.10 Added section 20 – Guidelines for technology specific ICT deployment Added section 21 – Guidelines for essential security practices Revision of title for Annexure 1 as References Annexure added – Feedback received from various Ministries/ departments on NISPG Added guideline on LAN security in section 12.3.5 as G5 Added guideline on Wireless architecture in section 12.3.6 as G6 Added guideline on Notification to agencies in section 16.3.8 as G42 Added guidelines on cloud computing in section 20.1.2 as G65, G66, G67, G68, G69, G70, G71, G72, G73, G74, G75 Added guidelines on mobility and BYOD in section 20.2.2 as G76, G77, G78, G79, G80 Added guidelines on virtualization in section 20.3.2 as G81, G82, G83, G84, G85, G86, G87 Added guidelines on security testing in section 21.1.2 as G88, G89, G90, G91 Added guidelines on security auditing in section 21.2.2 as G92, G93, G94, G95 Added guidelines on business continuity in section 21.3.2 as G96, G97, G98, G99, G100, G101 Added control on LAN security in section 12.4.9 as C9 Added control on Wireless LAN in section 12.4.13 as C10 Added control on Infrastructure protection in	15 May 2014

		section 14.4.13 as C58 Added control on Vulnerabilities knowledge management in section 18.4.4 as C114 Added control on Sharing of log information with law enforcement agencies in section 19.4.5 as C129 Added control on Log information correlation in section 19.4.7 as C131 Added control Communication of incidents in section 19.4.14 as C138 Revision of guideline titles for G29, G30, and G32 Revision of guideline text for G42, G44 and G45 Revision of control titles for C6, C11, C73, C88, and C91 Revision of control texts for C25, C39, C42, C92, C96, C99, C100, C103, C107, C127, C133, C136, C137 Revised annexure 14 – Risk Assessment for information security Revised annexure 15 – Glossary Added Annexure 17 – Feedback received from various Ministries/ Departments on NISPG	
4.0	Final Draft	Addition of new domains/ areas - Social media, open source technology Addition of Information handling guidance in section 28 Realignment of section 20 and section 21 to present each area separately Addition of implementation guidelines to all domains/ areas Revision of Annexures	26 July 2014
5.0	Final	Document review	10 October 2014

B. Table of Contents

1. Overview 13
2. Purpose 19
3. Document distribution, applicability and review 20
4. Scope 20
5. Supplementary documents and references 21
6. Approach 22
7. Information classification guidelines 26
8. Information security organization overview 27
9. Framework 28
10. Domains impacting information security 30
11. Guidelines structure and components 33
12. Network and infrastructure security 34
13. Identity, access and privilege management 46
14. Physical and environmental security 55
15. Application security 64
16. Data security 71
17. Personnel security 79
18. Threat and vulnerability management 85
19. Security monitoring and incident management 91
Guidelines for technology specific ICT deployment 100
20. Cloud computing 100
21. Mobility & BYOD 104
22. Virtualization 108
23. Social media 112
Guidelines for essential security practices 114
24. Security testing 114
25. Security auditing 116
26. Business continuity 119
27. Open source technology 121
Information handling matrix 123
28. Adoption matrix based on information classification 123
29. Annexures 167

1. Overview

1.1. Background

1.1.1. Traditionally, information available with the government has been safely managed by keeping it in paper records throughout its lifecycle i.e. when it is created, stored, accessed, modified, distributed, and destroyed. This information could be strategic, demographical, historical, legal, or may contain financial statements, procedural documents, data of citizens, industry or resources etc. Even though the lifecycle of information remains the same in electronic documents, the methods to secure information in electronic environment are significantly different. The challenges, as with the information contained in paper format, remain of similar nature, namely the ability to categorize, protect, archive, discover, transmit and attribute information during its useful life and eventual destruction

1.1.2. Information and Communication Technology (ICT) has empowered the government to create generate, store, transmit, and access information with much ease and efficiency. However, the importance of incorporating effective, state-of-the-art information security measures is being realized now. The departments, agencies and divisions recognize the security concerns in the electronic environment and are creating policies to secure the information in all stages of information lifecycle. The government and its officers have tremendous experience in securing paper documents. For example, several manual methods such as use of catalogs and paper-based chain-of-custody logs help keep track of the locations of files within secure record rooms. It is also known that information in the paper format may be exposed to physical damage, fraud or modification which may be sometimes difficult to track. The government is aware of the benefits of electronic form of information - it has not only been able to identify and gain visibility over the type of information available with its various departments, and agencies, but also attribute changes or modification to this information to specific personnel, thus making it easier to categorize, archive, discover and attribute

1.1.3. The government organizations deploy a number of technologies and in the process access, store and analyze vast amount of information. While the ease of access to information in the electronic format has helped revitalize governance, there are a number of threats which are emerging and required to be tackled on top priority. Today, information has acquired critical status for regulatory initiatives, policies and strategies, e-Governance, user services, financial transactions; however, security threats are becoming more organized and targeted, which pose serious threats – and in the event of any compromise of information, it could lead to major threats to internal and national security, and/or embarrassment to the government. Information is the reason for empowerment as well as a concern of threat for government organizations and needs a specific and granular focus on information which is created, stored, processed, transacted or accessed. Additionally, the IT infrastructure of a government organization is getting significantly transformed through increasing use of technical innovations, work-flow applications, mobility and extension to allow its usage by other stakeholders, partners, and service providers from the private sector

1.1.4. Complexity of information is a big hurdle in managing and governing security, privacy and compliance. Each government process or project introduces a different level of complexity as a result of wide-ranging data transactions, involvement of multiple stakeholders, exposure to

diverse set of infrastructure environments, networks, devices, platforms and information assets

1.2. Key areas of national concern for ministries/ departments/ agencies (management)

1.2.1. **Meeting dynamic security threats:** Protecting information has not typically been considered as a strategic element by the top level executives in the ministries/ departments/ agencies (management); even after promulgating various regulatory measures, global threats and many security incidents. Information security remains an afterthought, either as a line item or – even worse – not addressed at all by the top bureaucracy in the ministries/ departments/ agencies. The growing complexity of managing information security, rising exposure of an organization and close inter-linkage of Government information with the strategic security of the nation necessitates the elevation of the security function

1.2.2. **Creating visibility over activities and operations:** The security threat environment is becoming more widespread and dangerous and it is important that ministries/ departments/ agencies have visibility over their activities, functions and operations. Security as a discipline has also evolved over a period of time. The stimuli have been many - the dynamic threat landscape, threats to national security, internal security concerns, strengthening regulatory regime, privacy issues, economic value of information, research & innovation, globalization, business models, emerging technologies, etc.

1.2.3. **Intelligence gathering, knowledge management and skill development:** For an organization to be secure in today's technology driven work environment, it is important that it keeps track of all the latest developments in the field of information security – be it skills, technologies or services. An organization is required to provide strategic attention to security through commitment in all the facets of information security i.e. people, process and technology. It should be equipped with adequate knowledge, tools and techniques and human resources for gathering, assessing and presenting information security events to the top executive management levels in the ministries/ departments/ agencies. The aspects of designing, implementing and governing security although a key challenge for a ministries/ departments/ agencies, need to be addressed suitably by a framework for managing the affairs of security

1.3. Ministries/ Departments/ Agencies/ Management commitment towards Information security

1.3.1. **Introduction:** Information security program implementations often suffer due to inadequate resources—commitment of the ministries/ departments/ agencies, time, budget, human resources or expertise. By understanding the challenges of meeting compliance objectives, an organization can understand and appreciate the level of commitment required towards information security to overcome the obstacles and appreciate the gains achieved through implementing effective security practices. The following concerns emerge as executives in the ministries/ departments/ agencies decode the complexity and inter-linkage of security and performance:

1.3.1.1. **Coverage of security risks:** The foremost goal of an organization's risk management process is to protect the organization, and its ability to perform its functions, not just protect its information and assets. Therefore, the security risk management process should be treated as an essential management function of the ministries/ departments/ agencies/

organizations, rather than a technical function carried out by the IT system administrators alone

1.3.1.2. **Protection from interruption in services:** Ineffective security measures due to inadequate budget/commitment or inflexibility of the ministries, departments, agencies and their subordinate organizations to obtain advanced security capability, may cause disruption of vital services/ offerings. Information is one of the most important assets of an organization. Ensuring the confidentiality, integrity, and availability of this strategic asset allows ministries, departments, agencies and their subordinate organizations to carry out their objectives and realize their goals in a responsible manner

1.3.1.3. **Non-availability of information:** Risks to operations can arise through a variety of sources, in some cases resulting in damage to infrastructure and the complete shutdown of the services. For example, loss of all Internet connectivity, denial of service attacks, APTs, ransom-ware, physical theft etc and environmental factors (e.g., power outages, floods, and fires) can result in a loss of availability of key / strategic information, rendering any ministries, departments, agencies and their subordinate organizations incapable of achieving their objectives. Investment in security can assist in mitigating risks to operations

1.3.1.4. **Financial loss due to disclosure/ theft of information:** Inappropriate security measures may have a huge impact on an organizations financial position. A data breach may not only have direct financial loss, but will also dissolve the trust of residents, citizens, suppliers, other government bodies etc. Further, in order to minimize the damage of the breach, the organization may have to incur additional expenses

1.3.1.5. **Non- compliance with legal/ regulatory requirements:** The ministries, departments, agencies and their subordinate organizations may face administrative and/or legal actions for not complying with security advisories. Security is ultimately the responsibility of executive management Secretary, Joint Secretary, Managing Directors, CEOs, Directors, head of the department heads and other senior program officials of the ministries/ departments/ agencies/ organizations. The Management should deploy proactive security to enable delivery of its services and enhance value of the organization, rather than viewing security as an afterthought or as a reactionary mechanism to legislation, regulation, security event and oversight

1.3.1.6. **Investment and resource channelization disproportionate with risks:** Ignoring security as a design principle results in ad hoc investments, which more often than not focuses on adding controls after the systems are made operational—or in the worst case, after an organization has had a security breach or incident. The ministries, departments, agencies and their subordinate organizations may not realize the specific performance gains and financial savings by building security into systems as they are developed. However, these save the organization from incurring huge unbudgeted costs in covering up post an incident or breach

1.4. Need for an information-centric approach

1.4.1. While designing a strategy for security, information-centric approach in operational lifecycle should be an important consideration. Information and its attributes such as its origin, creator, nature of transaction, life, sensitivity, strategic importance and the operations performed on the information are some of the factors which help identify security requirements. Government ministries, departments, agencies and their subordinate organizations need to establish a process of identification and discovery of information for each of its processes, relationships and functions. The security posture has to be dynamic and should evolve with change in the value of information, information access methods and threat ecosystem. The capability of security processes and infrastructure to address information security should not only cover the different layers of ICT infrastructure, but also address the extended government ecosystem and new trends like mobility, big data and cloud computing. The consideration of information security in the lifecycle of information is also important from people, process and technical design perspective

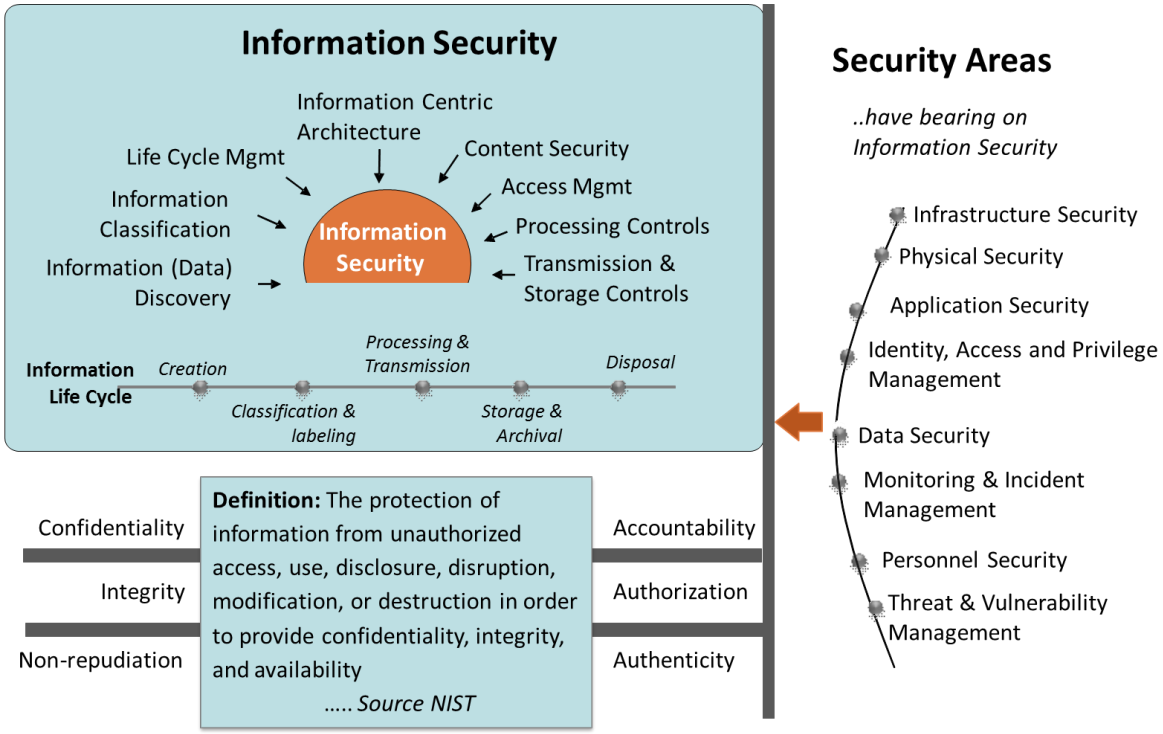


Figure 1: Domains impacting information security

1.4.2. Information can be classified based on its category or type, sensitivity, value and the context throughout its lifecycle. Ministries, departments, agencies and their subordinate organizations should ensure that a structural thought process in designing information security initiatives and measures is taken with respect to formation, grouping and arrangement of countermeasures for security of information. Moreover, they should have capability for responding to emerging threats by gathering intelligence on the nature of threats; deploying tools, techniques and methods to identify threats, build collaboration mechanisms which generate timely response from other security & IT infrastructure management processes

1.4.3. To make all this possible, organizations require a focused accountability and ownership structure for information security, where tasks are clearly distributed with respect to

administrative and technical arrangements. The IT initiatives of an organization need to be revitalized to incorporate the principles of information security. The disciplines of security, presented in this document, need to be carefully and diligently implemented

1.5. Information Security – focus areas

1.5.1. **Managing scale and complexity:** The increasing scale and complexity of organizations requires a more coordinated and collaborative security approach. The information age demands right proportions of security and requires graduation of security from a technical specialty to an operational strategy. The scope and reach of security function has been expanding with innovative and extensive use of IT for operational transactions, changing the nature of IT infrastructure and the ability of threats that impact the security posture of an organization in different directions and at different layers. Organization should be well equipped to overcome these aspects establish some key objectives which demonstrate its commitment to security

1.5.2. **Alignment of security with processes and functions:** The ministries, departments, agencies and their subordinate organizations need to distinguish between security related operational tasks from strategic security tasks. They need to estimate all security elements which are distributed across the organizational ecosystem. This requires significant efforts in building security characteristics and aligning the security function with organizational processes and IT, thereby ensuring that security hygiene is reflected across the organization. The management needs to focus its efforts on helping the organization identify enterprise information assets, processes and information resources and the commensurate protection required to secure them. To achieve this, the security function needs to work in close consultation and coordination with the ministries, departments, agencies and their subordinate organizations and sub functions to conduct risk assessments, and help them articulate the confidentiality, integrity and availability requirements of their resources, and develop appropriate security practices to ensure non-repudiation, accountability, authenticity and due authorization for information handling

1.5.3. **Compliance with laws and regulations:** The responsibilities of, and the extent of the role of security function within an organization is expanding; crossing the traditionally defined boundaries of IT, and covering all horizontal and vertical functions of ministries/ departments/ agencies/ organizations. Based on the nature of work and information handled, each horizontal and vertical function of an organization may need to comply with several laws and regulations. The Secretary/ the top management needs to drive security in all organizations functions and should promote adequacy of role & responsibility and efficacy of skills within its operational units. This will help ensure compliance with information security laws, regulations, standards, and guidance which are applicable to different departments and units, breach of which poses a severe threat not only to the organization's reputation, but also towards national security and internal security of the nation

1.5.4. **Formulating effective security functions and divisions:** Meeting the information security needs, necessitates ministries, departments, agencies and their subordinate organizations to focus on effective information security practices and functions which integrate security into the strategic and daily operations of an organization, focuses more on information-centric security strategy and ensures that security is part of the design principle and maturity of

security practices acts as a key differentiator in service delivery. Formulating effective security function in the organization ensures integration and builds collaboration between security, IT and other organizations functions

1.5.5. **Allocation of budgets:** There is a need for an effective and responsive security organization that is competent and committed in managing the complexity of security affairs and aligned to departmental requirements. For that to happen there is a need for provisioning adequate budgetary commitments towards security. This will help security to act not only as deterrence but as also as an operational advantage. Globally, there are many studies which suggest that budget for security should be proportional to the size of the organization or proportional to its IT budget. On an average, globally the budget for security varies between 8-10% of the ICT budget. However there are various parameters which should be evaluated before defining the security budget, it may be the sensitivity of information that ministries, departments, agencies and their subordinate organizations possess, the amount of transactions through varied platform, involvement of third parties, etc. Ministries, departments, agencies and their subordinate organizations should ensure that security budgets should be based on reasonable analysis and risks to operations and the allocation should depend on threat scenarios and risk to information

1.5.6. **Availability of security professionals and tools:** Apart from investing in adoption of newer technology platforms for better business effectiveness, ministries, departments, agencies and their subordinate organizations should also be committed towards investment in hiring skilled resources, procuring tools or increasing the efforts of the existing workforce. In order to augment the existing skills and expertise, top executives should be flexible to outsource specialized activities/operations to Subject Matter Experts (SME's) and be open to hire external consultants and experts post due security vetting. The ministries, departments, agencies and their subordinate organizations should also be flexible in changing procedural aspects of managing security and consult with the hired ICT organization to evaluate and implement effective security technologies and architecture

1.5.7. **Building and fostering culture of information security:** While protection of information is of paramount importance, ministries, departments, agencies and their subordinate organizations should support the broader aim of securing the enterprise. This requires fostering a culture of information security through commitment from top leadership who need to demonstrate the strategic nature and value of information to its workforce in the enterprise. This may be achieved by establishing the principles of protecting information assets for the organization, as a priority. The ministries, departments, agencies and their subordinate organizations should focus on imbibing a "risk-aware" culture across the ministries, departments, agencies and their subordinate organizations concerned, ensuring that key personnel fully understand the risk implications associated with their assets, processes and information

2. Purpose

2.1. Purpose of NISPG

2.1.1. The National Information Security Policy and Guidelines (NISPG), developed by the Ministry of Home Affairs once implemented, will help classify and protect the classified information possessed by ministries, departments, agencies and their subordinate organizations, and public sector undertakings. Breach of such classified information may have an impact on national security, or may cause unfavorable impact on internal security

2.1.2. This document elaborates baseline information security policy and highlights relevant security concepts and best practices, which government ministries, departments, agencies and their subordinate organizations should implement to protect their classified information

2.1.3. These guidelines will help ministries, departments, agencies and their subordinate organizations to establish minimum security processes and controls and devise appropriate information security programs. The ministries, departments, agencies and their subordinate organizations may need to apply enhanced security measures commensurate with risks identified with their specific operating environment and the information being handled by them

2.1.4. These guidelines will help organizations to focus on security objectives and strategy to protect their classified information, during every stage of information lifecycle such as creation, acquiring, storing, accessing, processing, transacting, retaining or disposal. These guidelines will help drive organizations towards designing, implementing and operating focused information security initiatives

2.1.5. The NISPG aims to provide:

2.1.5.1. Guidance to organizations to prioritize and focus attention and efforts in classification of information and securing such classified information

2.1.5.2. Guidance to security staff of ministries, departments, agencies and their subordinate organizations for deriving security measures and controls commensurate with the criticality and sensitivity of classified information

2.1.5.3. Guidance to drive security implementation

3. Document distribution, applicability and review

3.1. Distribution

3.1.1. The MHA shall distribute this document to all ministries, who will be further responsible for circulating the same to their departments, agencies and subordinate organizations and bodies including public sector undertakings (PSUs) and e-Governance projects etc., under their purview

3.2. Applicability

3.2.1. All ministries, departments, organizations, bodies, agencies including public sector undertakings (PSUs) and e-Governance projects etc., of the Government of India

3.2.2. All organizations included in the list above, shall ensure that the policy, guidelines, procedures and controls detailed in this document, are also adhered to by the private enterprises those support, maintain, manage or operate the information systems, facilities, communication networks, manpower etc. and in the process the information is created, accessed, stored, transacted, disposed and processed by or on behalf of the ministries, departments, agencies and their subordinate organizations through appropriate means.

3.3. NISPG review and update

3.3.1. The guidelines and controls detailed in this document shall be reviewed and updated to reflect the updated /current environment, or atleast once in every two year, whichever is earlier

3.3.2. The “Guidelines for technology specific ICT deployment” shall be reviewed and updated to reflect current technological environment or atleast once every year, whichever is earlier

3.3.3. The “Guidelines for essential security practices” shall be reviewed and updated to reflect the current technological environment or atleast once every year, whichever is earlier

4. Scope

4.1. Scope

4.1.1. The NISPG issued by MHA provide guidance in setting up baseline information security practices within government ministries, departments, agencies and their subordinate organizations.

4.1.2. The following guidelines, procedures and controls shall be implemented at all levels within ministries, departments, agencies and their subordinate organizations., including all e-Governance projects, to protect the confidentiality, integrity and availability of information created, accessed, stored, processed, transacted or retained or disposed of by them; while establishing and maintaining accountability, and non- repudiation of actions over classified information in its lifecycle

4.1.3. This policy extends to all of the following within ministries, departments, agencies and their subordinate organizations: top management, users, system owners, staff/managers, system administrators, developers and operators, including contractors and third party service providers or any other party on their behalf, which maintain, manage, operate or support information systems, facilities, and/or communications networks etc.

5. Supplementary documents and references

5.1. References

5.1.1. The policies and procedures suggested in this document take into account the previous guidelines issued by various competent bodies and authorities of the government e.g. 'Computer Security Guidelines' 2006' by Intelligence Bureau (IB), 'Cyber Security Policy for Government of India' by National Informatics Centre (NIC), Guidelines and controls mentioned in "Cyber Security Policy for Government of India" ver 2.0 released 30th August, 2010, Guidelines issued by National Critical Information Infrastructure Protection Centre, National Technical Research Organization and various 'Security Guidelines' issued by CERT-In. The directions laid out in this document are inclusive in nature and have referred to the content and suggestions from the above mentioned guidelines, wherever appropriate. However, the ministries, departments, agencies and their subordinate organizations concerned are advised to consult the previous documents on the same subjects as well

5.1.2. MHA has done extensive work of studying various, international and national standards and regulatory guidelines prevalent in the information security domain worldwide. The guidelines have been influenced by, and draw references from, the global standards and practices such as ISO 27001 (2005 as well as 2013), NIST Special Publication 800-53, Federal Information Security Management Act (FISMA) of USA, SANS "20 Critical Security Controls", Control Objectives for Information and Related Technology (COBIT) for information technology (IT) management and IT governance, PCI –DSS, DSCI Security Framework (DSF) etc.

6. Approach

6.1. Security of classified information

6.1.1. **Securing classified information in government and public sector processes lifecycle**: The ministries, departments, agencies and their subordinate organizations should ensure that they establish appropriate processes and capabilities to secure information throughout its lifecycle i.e. as information is created, accessed, modified, stored, processed, transacted, transmitted, deleted, disposed of or destroyed. Information can be classified based on its category or type, sensitivity, value and the context throughout its lifecycle

6.2. Security risk assessment

6.2.1. **Conducting periodic risk assessment:** Security risk assessments should be conducted periodically to evaluate risks and associated threats leading to loss of confidentiality, integrity and availability of information. Threat and vulnerabilities associated with the information must also be evaluated for their potential impact, including impact on internal and national security.

6.2.2. **Risk assessment framework:** Due to the diverse nature of operations of different organizations there can be no single approach recommended for risk assessment. However, to develop a risk based methodology which helps develop resilience to changing threat environment, ministries, departments, agencies and their subordinate organizations need to integrate information security risk assessment with the broader risk management framework for operations. Frameworks such as ISO 27005:2008 or others may be referred to based on the organization's requirements

6.2.3. **Periodicity of risk assessments:** Information security risk assessment should be an on-going activity, triggered early into the lifecycle of system design and development. It should be conducted at least once every year or when changes are made to existing information assets or when threat perception over information and information systems changes. For systems containing classified data, a thorough risk assessment should be conducted at-least once every quarterly

6.2.4. **Methodology:** A comprehensive security risk assessment may include methodologies prescribed in Section 18 of this document for threat and vulnerability management

6.2.5. **Additional insights:** A comprehensive information security risk assessment will also provide insights into expected ICT security expenditure, thereby helping formulate budgets and estimate costs and help strategic decision making

6.3. Principles for establishing organization wide security framework

6.3.1. **Core security goals:** Information security frameworks should be designed to ensure confidentiality, integrity, availability of information to authenticated and authorized users, while establishing accountability over transactions conducted over the lifecycle of information and establishing non- repudiation of information, across layers of people, process and technology

6.3.1.1. **Architecture:** Adequate steps must be taken for integrating information security measures with the IT architecture of organizations to address contemporary security threats.

Capability to respond to new issues or threats through integrating internal and external intelligence measures, deployment of tools, techniques and methods in identifying threats, which generate timely and desired response from other security & IT management processes, must be established

6.3.2. **Security division structure**: The ministries, departments, agencies and their subordinate organizations must establish accountability and ownership structure for information security, where tasks are clearly distributed with respect to administrative and technical arrangements required for information security. The head of security must report directly to the head of the ministries, departments, agencies or organizations and not to the IT head.

6.3.3. **Deployment of professionals and skill development**: The ministries, departments, agencies and their subordinate organizations must ensure that trained professionals in the field of Information Security are deployed to address their Information Security initiatives, at appropriate levels. Further, adequate measures to train existing users, human resources, to acquaint them with best practices for securing information and align them with the overall objectives of the organization for protection of information and information assets must be undertaken at periodic intervals. Every new employee should go through the information security awareness program which could be organized in-house. Also every employee should be given training in information security atleast once every two years.

6.4. Security audit

6.4.1. **Security audits**: The ministries, departments, agencies and their subordinate organizations must conduct appropriate evaluation, testing and audits of all organizational structures, mechanisms, policies, procedures, technologies and controls to ensure their alignment with the implementation objectives of the information security policy and guidelines at regular intervals. Areas of improvement should be identified and a mechanism to improve the overall deployment of such structures, mechanisms, policies, procedures, technologies and controls should be undertaken

6.4.2. **Identification and response to data breach**: The ministries, departments, agencies and their subordinate organizations should develop the ability to identify, alert, evoke responses & resolve a data breach in timely manner

6.4.3. **Coordination with agencies**: The ministries, departments, agencies and their subordinate organizations should interact with relevant agencies in the domain of information security to gather and share intelligence about threats and vulnerabilities

6.5. Exception to implementation of recommended guidelines and controls

6.5.1. The ministries, departments, agencies and their subordinate organizations are expected to conduct a thorough risk assessment and use the practices outlined in this document to help implement a framework within the organization

6.5.2. The ministries, departments, agencies and their subordinate organizations must exercise its own discretion in customizing and adapting the guidelines mentioned in this document, while upholding the core objectives and principles of the NISPG. Further, the ministries, departments, agencies and their subordinate organizations are free to deploy relevant

capabilities in the form of tools, solutions etc. to help implement information security practices and its governance framework

6.5.3. The MHA, through its agencies, may seek compliance in the form of audit reports to demonstrate adherence to controls and guidelines specified in the NISPG from ministries, departments, agencies and their subordinate organizations

6.5.4. In case some guidelines and controls are not adhered to, ministries, departments, agencies and their subordinate organizations should be able to substantiate their stance by reproduction of appropriate documentation specifying at a minimum, the following parameters:

6.5.4.1. Reason for non-conformance to guidelines

6.5.4.2. Risk evaluation reports detailing the risks due to non-conformance

6.5.4.3. Additional controls implemented, if any

6.5.4.4. Timeline for introduction of recommended controls

6.5.5. Such instances should also be brought to the notice of the Information security steering committee (*refer section 8*) and a formal signoff should be undertaken in all cases, where guidelines specified under the NISPG are not followed

6.6. Limitations

The figure below summarizes the overall security ecosystem by explaining the relationship between national security, cyber security, organization security and information security. The policy focuses on protection of classified information and hence intends to only provide guidance, procedures and controls which are relevant to this specific area. While it is beyond the scope of this document to detail every single practice involved in the design, implementation, configuration, management and security enforcement, an effort has been made to capture information security measures through security domains.

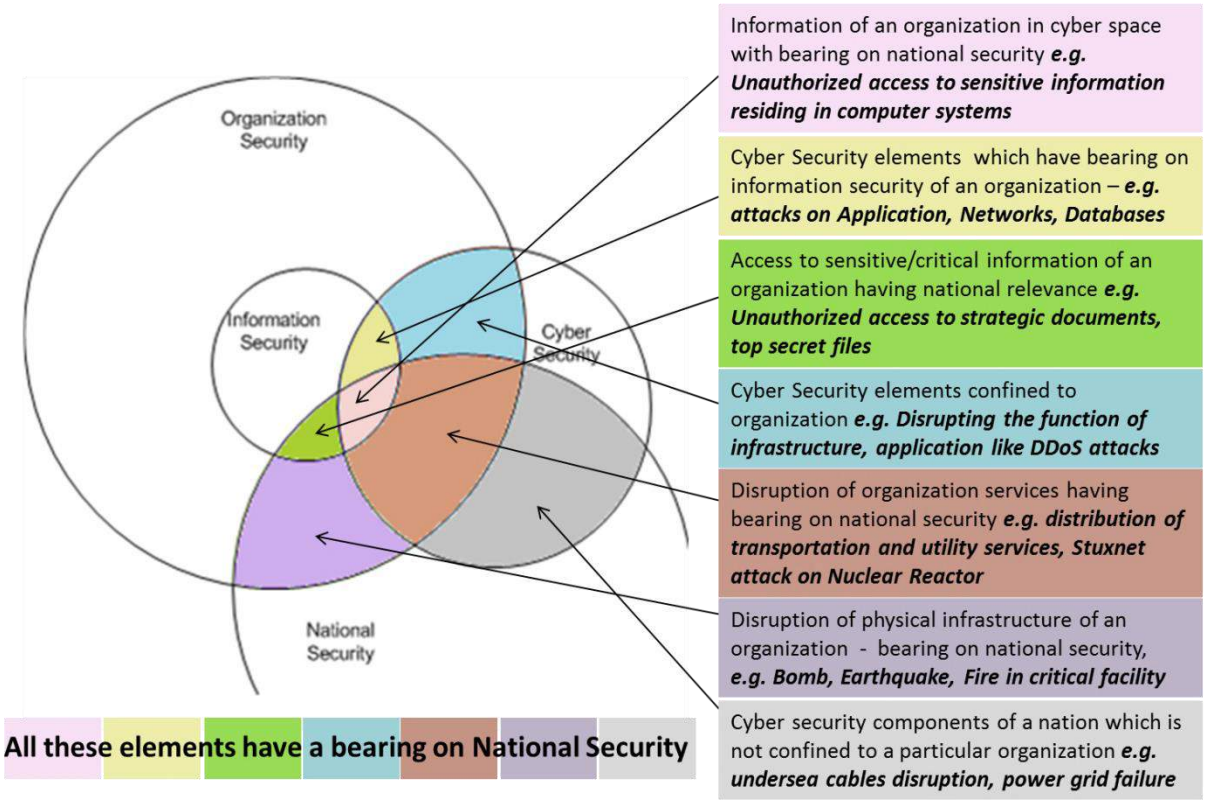


Figure 2: Each area encompasses information which has ramifications towards National Security

7. Information classification guidelines

7.1. Information classification

All information available with organizations should be classified into one of the following categories (based on existing classification of Manual on paper records Issued by Ministry of Home Affairs, 1994):

7.1.1. Top Secret: Information, unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for nation's closest secrets and is to be used with great reserve

7.1.2. Secret: Information, unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used

7.1.3. Confidential: Information, unauthorized disclosure of which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization, or could affect the organization in its functioning. Most information, on proper analysis, will be classified no higher than confidential

7.1.4. Restricted: Information, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose

7.1.5. Unclassified: Information that requires no protection against disclosure. e.g. Public releases

7.2. **Information handling:** Appropriate information handling procedures must be developed, commensurate with the level of classification. *For further guidance on information management and handling refer Adoption matrix based on information classification table below*

8. Information security organization overview

8.1. Security division

8.1.1. **Role of Chief Information Security Officer (CISO):** The responsibility of security management should be entrusted to the "Security Division" under the charge of the Chief Information Security Officer (CISO). Its role cuts across the traditionally defined boundaries of IT and covers all the horizontal and vertical functions of an organization. CISO's role is detailed below:

8.1.1.1. Design, implement, monitor and govern an organization-wide information security program

8.1.1.2. Ensure information security risk assessments and audits are performed as necessary. Oversee risk assessment exercise to understand the threats to key information assets, analyze risks with the concerned divisions of the organization

8.1.1.3. Design information security related policies, procedures and processes to ensure confidentiality, integrity, availability of classified information while establishing accountability, authorization and non- repudiation of actions over information

8.1.1.4. Review policies, procedures and standard operating procedures

8.1.1.5. Work on positioning of security division, so as to make it more effective

8.1.1.6. Devise programs for capacity building and oversee information security training and development of personnel. Additionally, the CISO should establishing mechanisms for information security awareness in the organization

8.1.1.7. Liaison with relevant agencies to gather intelligence about prevailing threats and best practices

8.1.2. **Reporting structure:** The Chief Information Security Officer (CISO) or equivalent will report directly to the Secretary concerned of the respective Ministry/ Department

8.2. Information security division & roles

(Refer "Cyber Security Policy for Government of India" ver 2.0 released 30th August, 2010)

8.2.1. The following roles are required based on the fact that each Ministry/ Department/ Organization is located in one of more location/ Bhawan and each location/ Bhawan has one or more Ministries / Departments / Organizations.

8.2.1.1. **National Information Security Officer (NISO)**: Responsible for cyber security of all Ministries/ Departments of Government of India

8.2.1.2. **Chief Information Security Officer (CISO):** Responsible for cyber security in the respective Ministry/ Department. This role is to be designated by the respective Ministry/ Department

8.2.1.3. **Cyber Security Administrator (CSA):** Responsible for technical functions, related to cyber security for Ministries/ Departments

8.2.1.4. **Information Security Officer (ISO):** Responsible for administrative functions related to security for every location of the Ministry/ Department. This role is to be designated by the Ministry/ Department for each location of the Ministry/ Department

8.2.1.5. **System Administrator (SA):** Responsible for performing functions, that requires system administration privileges of the user systems, for each location of the Ministry/ Department

8.2.1.6. **Network Security Administrator (NSA):** Responsible for managing the security of the networks per location/ Bhawan. This role will be performed by the service provider

8.2.1.7. **National Security Operations Center Head (NSOC):** Responsible for managing the NSOC round the clock. This responsibility will be handled by the service provider

8.2.1.8. **NSOC Administrator**: Responsible for administration of the NSOC round the clock

8.2.1.9. **NSOC operator**: Responsible for operations of the NSOC round the clock

8.3. Information Security Steering Committee (ISSC)

8.3.1. An Information Security Steering Committee (ISSC) under the chairmanship of the Secretary of the concerned Ministry should be established

8.3.2. The members of the ISSC should comprise of:

8.3.2.1. IT Head or equivalent

8.3.2.2. Chief Information Security Officer (CISO)

8.3.2.3. Financial Advisor

8.3.2.4. Representative of National Critical Information Infrastructure Protection Center (NCIIPC), or representative of Department of Electronics and Information Technology (DeitY)

8.3.2.5. Any other expert to be nominated by the ministry or department

9. Framework

9.1. Standard for information security management

9.1.1. The ministries, departments, agencies and their subordinate organizations should ensure enforcement of a globally accepted standard of information security management and governance. Reference to the standard used, should be documented in the ministry/ departments security policy, or in some other high level document, developed by the Chief Information Security Officer (CISO), and approved by the ISSC

9.1.2. The implementation of information security and its governance requires coordinated effort between designated personnel and well defined framework for governance. The governance process and the personnel tasked with governance of information security should be stated in the security policy, and brought to the notice of ISSC

9.2. Introduction to globally accepted Information security management standards

9.2.1. There are several standards accepted globally which help an organization conduct risk assessment , gap analysis and govern security implementation at different levels such as network access points, user authentication, applications etc. across the people, process, and technology (PPT) layers. There are several information security management standards which are adopted by organizations worldwide. The ministries, departments, agencies and their subordinate organizations may use such globally accepted standards to design, implement and govern information security within their organization and mandate all partner organizations and third parties to implement similar practices

(*For more details on globally accepted information security management standards refer to Annexure 10*)

10. Domains impacting information security

10.1. Overview

10.1.1. **Alignment with security framework:** While following the above framework, the ministries, departments, agencies and their subordinate organizations should consider developing strategy and competence in specific disciplines to enhance security. The NISPG has identified eight core domains namely, network and infrastructure security, identity and access management, physical security, application security, data security, personnel security, threat & vulnerability management, security monitoring & incident management. Additionally, the areas of security audit, security testing and business continuity, which cut across all domains, have been covered as part of the guidelines. Further, guidelines for technology specific areas such as virtualization, cloud computing, mobility and social media are provided in a separate section

10.1.2. **Achieving maturity in security domains:** Domains mentioned above need to be understood critically for security of classified information. Strategies for each of them, along with tactical guidelines for implementation, and security controls are essential for making security robust. The ministries, departments, agencies and their subordinate organizations should organize, allocate and drive resources towards each of these security domains and strive to achieve maturity over time to counter the increasing threats and attacks

10.1.3. Information security domains

10.1.3.1. **Network and infrastructure security:** The architectural plan of locating information in a network arrangement and other infrastructure security arrangements such as internal and external connections to information, protocols that are used to transfer information, preparedness to withstand attacks etc. require specific consideration and treatment from the perspective of securing information

10.1.3.2. **Identity and access management:** Sensitivity and criticality of information specifies the requirements with respect to ability of an individual or group of users to access and perform a set of operations on the said information. The increasing reliance on third parties and external SMEs makes it imperative for the organization to secure itself against risk arising from misuse of identities or additional or illegitimate access provided to the users

10.1.3.3. **Physical security:** Organizations generally have multiple touch points from where information can be accessed physically. To add to that, technology enables easy availability of portable devices. This can defeat traditional physical screenings of individuals. With more solutions and techniques becoming available in the market, physical security concepts are also evolving, establishing it as an important discipline for protecting information security. While it focuses more on restriction to physical intrusion, technological solutions provide means to raise alarms by detecting anomalies and patterns of information being accessed which help in detection and containment of information security incidents

10.1.3.4. **Application security:** The primary objective of application security is to secure information as it is processed, transferred or stored during the lifecycle of an application. The

characteristics of applications vary from basic versions, to context aware, and Internet rich usage of apps. These variations at various fronts expose the information processed, stored, accessed, transacted through these applications to a larger threat landscape

10.1.3.5. **Data security:** Each data item collected, stored, processed, transmitted and accessed by an organization has to be protected against cyber-attacks especially that are sensitive or critical for internal and national security as stated in classification of information. The entire focus and effort is to secure data. It is this which has led to the evolution of the discipline of data security - the ultimate goal of an organization's security

10.1.3.6. **Personnel security:** Risks due to insider threat and internal security breach undermines all security measures taken to fortify information systems and data from the outside world. The personnel security focuses on both the aspects of employee as well as third party security and focuses on sourcing patterns of an organization which requires specifics checks from a security viewpoint

10.1.3.7. **Threat & vulnerability management:** There is an ever increasing rise of security threats with enhanced capabilities, varieties and scales; exploring new ways to find vulnerabilities and exploits in an organization's infrastructure to cause maximum possible damage. Threat and Vulnerability Management (TVM) ensures that an organization's resources are protected against the perennial as well as evolving threats, and provides assurance over the management of its resources in a way that the relevance of new vulnerabilities, exploits or malware is immediately tested and that the organization responds swiftly to them. TVM adds critical value to an organization's security initiatives, which not only delivers protection capabilities but also provides means to manage IT infrastructure securely

10.1.3.8. **Security monitoring & incident management:** Security Monitoring and incident response management is a key component of an organization's information security program, as it demonstrates its ability to respond to an information breach which might emanate from external or internal sources

10.1.3.9. **Security audit and testing**: Security audit, testing and reviews should be conducted on a continuous basis to check for conformance of security measures deployed by the organization with security policies, standards and requirements. Specific requirements are implicit in all disciplines. Moreover, general best practices have been provided as part of this document

10.1.3.10. **Business continuity**: Business continuity of the operations has to be planned by the respective government departments and is kept outside the scope of this policy. However, this document covers areas which are important from the perspective of ensuring availability of critical operations and classified information

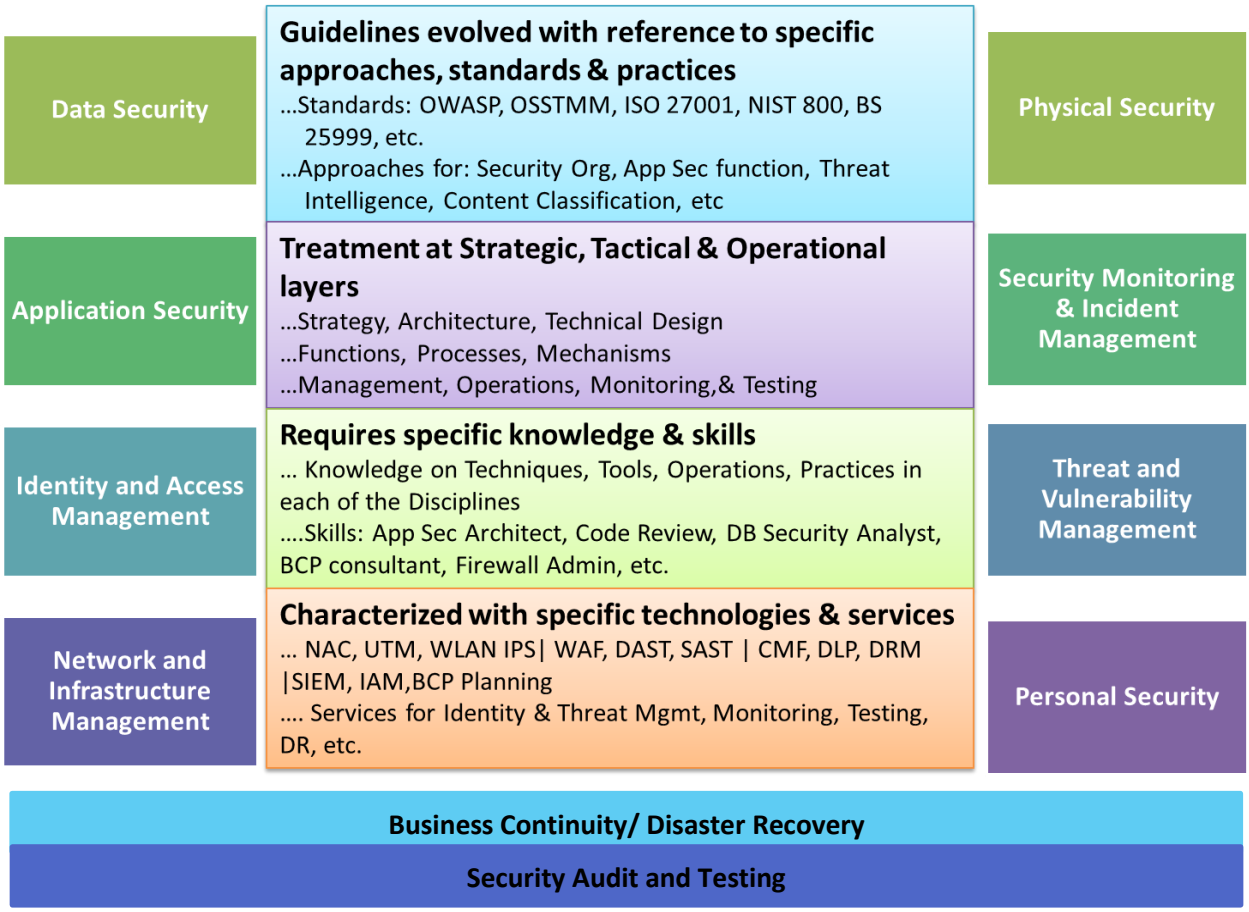


Figure 3: Information security domains

11. Guidelines structure and components

11.1. **Structure:** Each domain in the National Information Security Policy & Guidelines consists of five parts, as follows:

11.1.1. **Section X.1: Background** – This section provides an overview and the coverage of each domain and states the important evolutions and developments in each area. This section provides an overview of each domain for the reader to understand the importance and significance of achieving maturity in each area.

11.1.2. **Section X.2: Relevance of domain to information security** – This section establishes role and scope of a domain in context of Information Security. It provides insights into the impact of compromise of information due to the current and emerging threats and vulnerabilities of the said domain.

11.1.3. **Section X.3: Management guidelines**– This section provides domain specific recommendations in the form of guidelines and objectives. These guidelines will help the senior management in an organization to institute security processes, procedures and governance mechanisms. The management guidelines section provides a high level view of each domain, focusing on areas which are of significant importance in order to establish practices in each domain.

This section also provides intent to senior management in order to pursue further action in design, development, implementation and governance of security domain. The management guidelines can also be used to derive assurance from operating divisions and will help in the high level performance evaluation of the security function. Each guideline is mapped with a number of security controls which provide clarity on the diverse elements contained in a management guideline.

These are denoted by the nomenclature "G" followed by the guideline number. For example, G1, G2, G3 … G112

11.1.4. **Section X.4: Security controls**– Provides control statements which are administrative, technical, operational or procedural and need to be diligently followed. Security controls provide insight into multiple areas which need to be implemented/ addressed in order to achieve the objectives laid out in the management guidelines section. Security controls provide exact direction and articulate expectations needed to develop adequate protection.

Each control statement is further complimented by implementation guidelines, which provide specific information with respect to area covered in each security control.

These are denoted by the nomenclature "C" followed by the control number. For example, C1, C2, C3… C135

11.1.5. **Section X.5**: **Implementation guidelines** – This section provides specific recommendations to aid implementation of management guidelines and security controls. Implementation guidelines offer granular detail on the expectations from each organization, for implementation of controls and management guidelines. This section provides practical guidance considering the depth of implementation of various controls, while considering the value of information based on its classification.

These are denoted by the nomenclature "IG" followed the implementation guideline number. For example, IG1, IG2, IG3 …IG181

12. Network and infrastructure security

12.1. Background

12.1.1. The increased adoption of information technologies has created immense opportunities to connect, expand and integrate different entities. This led to the expansion of the network capabilities and adoption of emerging connectivity techniques

12.1.2. The network infrastructure itself has evolved with various options of network topologies, types of routing and switching devices and different connectivity options. Networks are playing important role in providing access to information and information systems; providing new ways for executing transactions and helping organizations leverage fruits of globalization and hyper specialization. The diversity of these topologies, devices and connections contributes to creating immense possibilities, however; it also introduces several new security issues and concerns

12.1.3. The organizational ecosystem is undergoing transformation, extending its boundaries by increasingly providing access to third parties and vendors, integrating external interfaces, adopting innovations in endpoint, mobility and wireless technologies, while relaxing norms of standardization and ownership of connecting devices. Enterprise architectures are becoming more complex, multiple new system components are under deployment, and their capabilities are extensively utilized through virtualization. This provides multiple opportunities by which security can be compromised

12.2. Relevance of domain to Information Security

12.2.1. Network plays an important role as it binds all the information assets together and provides a means for operational transaction where different entities can participate, exchange information and carry operations over the information by making use of specific ports, protocols and services provided by the network. This may create the possibilities of exposure of information

12.2.2. Network plays a role in provisioning users and devices access to data as it is the first point of connects. Users seek flexibility in accessing data across different devices and access paths. This may expose organization's information through these devices and the way users access information

12.2.3. Network infrastructure typically spreads across geographies, providing access, facilitating exchange of information and executing a variety of transactions. A combination of network solutions and devices are required in order for these transactions to be successful. They may create possibilities of compromising security of information at various levels

12.2.4. Traffic flow, connections, devices and traffic patterns introduce significant vulnerabilities and weaknesses. These vulnerabilities and weaknesses may lead to serious security threats to information

12.2.5. Insiders have easy access information and IT systems. Network aids their access to the information and IT systems. They may be source or reason for compromise of security of information

12.2.6. The new components and architectural elements incorporated as a part of the plan for infrastructure transition may introduce serious security issues. Adoption of trends such as mobility and usage of personally owned devices exposes the network to a new set of threats

12.3. Network and infrastructure security management guidelines

12.3.1. **Inventory of assets and infrastructure:** The organization should ensure that a network diagram illustrating all network devices and other significant devices is available. Since this contains classified information, such documentation should be appropriately protected and its distribution should be limited. The organization must maintain and update a map/inventory of authorized devices such as: **G 1**

a. **Infrastructure components** spread across the organization and connected to the network endpoints, server systems, applications, databases and data files, and messaging systems

b. **Connectivity and access** to users, endpoints, devices, server systems, applications, databases and messaging systems should be recorded and maintained

c. **The spread of the organizational assets** across the operational functions and geographies and their access requirements should also be recorded

12.3.2. **Security testing of network & infrastructure devices:** All infrastructure and network hardware may be procured, from manufacturers or resellers who are authorized by manufacturers, with reasonable demonstration of compliance with global security best practices **G 2**

12.3.3. **Network perimeter security:** The government organization must secure the network perimeter by deploying competent security solutions **G 3**

12.3.4. **Network zones:** The organization must divide their networks into multiple functional zones according to the sensitivity or criticality of information or services in that zone. Wherever possible, physical isolation must be performed **G 4**

a. **Access from external environment:** Sensitive IT assets must not be directly accessible from the external environment

b. **Network segmentation technologies:** The organization must ensure that appropriate network segmentation technologies are enforced to logically and physically isolate the network and protect classified information and critical services (such as user authentication and user directory information)

c. **Operating zones for users:** Environment that allow internal users access to information assets and systems should be separated from the environment created for external users

12.3.5. **LAN security:** The organization must develop, document and periodically update security policies and procedures related to Local Area Networks (LAN) **G 5**

a. The organization must evaluate risks associated with transmission of

classified information over LAN on a periodic basis

b. The organization must clearly define roles and responsibility of personnel for supporting planning and implementing of LAN security, through appropriate job functions

c. The organization must ensure that appropriate security measures, tools and methodologies are implemented to protect transmission of classified information over LAN. Traffic over LAN should be protected with use of appropriate encryption methodologies

12.3.6. **Wireless architecture:** The organization must ensure that Wireless LAN (WLAN) planning and implementation incorporates security best practices **G 6**

a. **Confidentiality and integrity**: The organization must implement appropriate encryption for transmission of classified information over WLAN

b. **Administration of access points:** The access to WLAN key distribution program should be controlled and limited to the administrators only

c. **Logging of device activities and audit trails**: Network traffic and access to the WLAN should be logged by using suitable methodologies

12.3.7. **Network security management:** Network security management processes should be created and documented. These processes should define the governing procedures for any security mechanism, changes or modification to the network configuration, the approval matrix, backup mechanisms, guidelines for testing and failover switching amongst others. The organization should ensure that all network security management tasks are approved and performed under the aegis of a single authority or team **G 7**

12.3.8. **Unauthorized device connection:** Organizations should implement stringent measures to minimize the risk of unauthorized devices from accessing the network. The necessary countermeasures must be deployed to deter the attempts of unauthorized access **G 8**

12.3.9. **Extending connectivity to third parties:** The government organizations must integrate the infrastructure security with other security solutions such as identity & access management, security monitoring & incident management for integrated defense and response against the threats **G 9**

12.4. Network and infrastructure security controls

12.4.1. **Identification & classification:** The organization must ensure that all infrastructure devices are grouped and classified in accordance to the criticality of the information that they contain/ process **C 1**

12.4.2. **Network diagram:** The organization must ensure that the network diagram is updated as changes are made to the network. The date of last modification should be clearly stated **C 2**

12.4.3. **Network configuration:** The organization should regularly review their network configuration to ensure that it conforms to the documented network configuration **C 3**

12.4.4. **Testing and certification of network & infrastructure device:** Network and Infrastructure devices should be tested basis globally accepted security standards, in appropriate test labs prior to their purchase. A secure and stable configuration of the device and product may only be procured for deployment **C 4**

12.4.5. **Network security measures:** The organization must ensure the competent security countermeasures for network security are established, such as: **C 5**

a. Perimeter defense

b. Traffic inspection and detection of anomalies and threats

c. Detection and prevention of intrusion

d. Filter, block and prevent the malicious traffic

e. Restrict insecure ports, protocols and services

f. Protection against the denial of service and distributed denial of service attacks

g. Restriction on connections to the external world and the internet

h. Malicious code detection and filtering

i. Restrict, change and segment users access

12.4.6. **Security of IPv6 device:** The organization must ensure that all dual-stack network devices, equipment and operating systems that support IPv6 must disable the functionality unless it is being used and appropriate security measure have been deployed for their protection. All future networks should be IPv6 compatible **C 6**

12.4.7. **Segmentation:** The organization must create appropriate network segmentation and maintain updated network access control lists **C 7**

12.4.8. **Security zones:** The organization must create separate zones for and apply additional security protections to network zones that contain classified information from the environment where their users access the Internet and external email. **C 8**

12.4.9.	**Network traffic segregation :** The organization must implement network access controls to limit traffic within and between network segments to only those that are required for operations	**C 9**
12.4.10.	**LAN security:** The organization must implement relevant controls to ensure security of information traversing the organizations Local Area Network (LAN)	**C 10**
12.4.11.	**Wireless LAN security:** The organization should implement appropriate controls to protect the confidentiality and integrity of information traversing over WLAN.	**C 11**
12.4.12.	**Disabling unused ports:** The organization must disable unused physical ports on network devices such as switches, routers and wireless access points	**C 12**
12.4.13.	**Personal devices usage policy:** The organization must ensure that incase personally owned devices are permitted to be connected to the organizations network, a prior security validation must be performed on such devices at each log-in instance to check for basic system health requirements. Devices which are non-compliant with health requirements should be quarantined	**C 13**
12.4.14.	**Restricting access to public network:** The organization must ensure that devices are prevented from simultaneously connecting to an organization controlled network and to a public data network.	**C 14**
12.4.15.	**Network access control:** The organization must implement network access controls on all networks	**C 15**
12.4.16.	**Firmware upgrade:** The organization must ensure that firmware for network devices is kept up to date	**C 16**
12.4.17.	**Network change management:** All changes to the network configuration, in the form of upgrades of software and firmware or in the form of addition or removal of hardware devices and systems should be undertaken post approval from competent authority. All changes to the network configuration should be documented and approved through a formal change control process	**C 17**
12.4.18.	**Securing transmission media:** All cables and encompassing cabinets must be secured from unauthorized access, physical damage and tampering	**C 18**
12.4.19.	**Default device credentials:** The organization must ensure that default usernames and passwords are changed before network devices are deployed	**C 19**
12.4.20.	**Connecting devices:** The organization must deploy appropriate monitoring and network scanning methodologies to detect systems connecting to the network and portable devices connected to workstations via USB ports	**C 20**
12.4.21.	**Audit and review:** The organization must conduct periodic audits of network devices which are being added or removed from networks and create an inventory of authorized network devices	**C 21**

a. **Network logs:** The organization must set up logging of access and activity of network devices. Depending on the scale of the network components,

organisation may be also evolving to have automated alert systems wherever there is a deviation in the acceptable log parameters

12.4.22. **Extending connectivity to third parties:** The connectivity to third party must be securely managed **C 22**

12.5. Network and Infrastructure security implementation guidelines

12.5.1. **Identification and classification:** The organization must ensure that classified information is mapped with the infrastructure elements through which it will be transmitted, processed or stored. **IG 1**

a. All infrastructure devices should be categorized as per classification of information that they manage

12.5.2. **Network diagram:** The organization must develop an accurate mapping of the core components, connections and information of the network to build organization's network diagram including network components such as routers, switches, firewall and computer systems, IP addresses, data flow routes, blacklisted or white listed systems/IP addresses, open/entry ports, subnet mask, administrative interface, zones, access control lists, network name amongst others **IG 2**

a. All amendments to network diagram should be documented with reason of change, nature of change, person responsible

b. All previous configuration diagram must also be retained for reference

12.5.3. **Network configuration:** Organization must review network configuration periodically by using configuration audit and configuration comparison tools **IG 3**

a. The organization must establish a mechanism that compares the running configuration of network devices against the documented configuration

b. There must be documented standards/procedures for configuring network devices (e.g. routers, hubs, bridges, concentrators, switches, firewalls, IPS, IDS etc.), which cover - security architecture, device configuration, access control to network devices, vulnerability and patch management, changes to routing tables and settings in network devices and regular review of network device configuration and set-up.

c. Security controls applied to network devices must incorporate security architecture principles (e.g. 'secure by design', 'defense in depth', 'secure by default', 'default deny', 'fail secure', 'secure in deployment' and 'usability and manageability').

12.5.4. **Testing and certification of network & infrastructure device:** Devices deployed must be tested and certified prior to their implementation in the organization's environment **IG 4**

b. Network and infrastructure devices must be self-certified by the manufacturer

c. Network and infrastructure devices must be tested and certified in any globally recognised lab

d. The organization must ensure comprehensive network and infrastructure device testing from established testing labs of STQC, DRDO or other designated government test labs

12.5.5. **Network security measures:** For perimeter defense, organization must use appropriate security capability, such as **IG 5**

a. For traffic inspection and detection of anomalies and threats organization should implement Security Information and Event Management (SIEM) capability

b. Organization should deploy Intrusion Detection System (IDS) capabilities to monitor network or system activities for malicious activities or policy violations

c. Organization should deploy Intrusion Prevention System (IPS) capabilities to identify malicious activities in the network, log information and attempts to block them

d. For protection against the distributed denial of service (DDoS) and denial of service (DoS) attacks appropriate protection must be incorporated in-house such as on premise traffic filtering equipment or from service providers for services such as traffic-routing service through Border Gateway Protocol, DNS change to traffic snubbing centers, cloud based mitigation etc.

e. The organization should conduct or participate in mock drill exercises to test network security measure

12.5.6. **Security of IPv6 device:** The organization should have security measures specific to IPv6 security **IG 6**

a. Disable IPv6 functionality at the gateway level until and unless required for use by organization with additional DoS security measures. Block all IPv6 traffic on IPv4-only networks

b. Use standard, non-obvious static addresses for critical systems

c. Firewall, IDS/IPS must be able to scan IPv6 traffic and enforce policies on the same

d. The event and transaction logging mechanism must be capable of capturing activity of IPv6 devices

e. All future networks should be IPv6 compatible

12.5.7. **Segmentation:** To restrict, segment and modify user access, organization should deploy tools such as Active Directory to limit or grant permissions to a user **IG 7**

a. The organizations must ensure segmentation of the network to create

security zones for isolating sensitive traffic and secure critical IT systems. This is typically done by using means such as establishing Demilitarized Zone (DMZ) and configuring virtual LANs

b. Organization should limit and segment user rights for access by implementing proper Access Control Lists in the network. Access control lists should be configured on devices such as routers and/or switches

12.5.8. **Security zones:** Virtual LAN should be used by an organization to logically separate zones which deal with confidential information from the rest of the network **IG 8**

a. VLANs should not be used between classified networks and any other sensitive networks

b. VLANs between classified networks and any other network of a lower classification must not be used

c. VLANs between a sensitive or classified network and public network infrastructure must not be used

d. VLAN trunking must not be used on network devices managing VLANs of differing security classifications

e. Administrative access for network devices using VLANs must only be permitted from the most trusted network

12.5.9. **Network traffic segregation:** Organization should enforce rule set to minimize methods and level of access to classified information in order to limit access to authorized personnel **IG 9**

a. Implementation of traffic flow filters, VLANs, network and host based firewalls,

b. Implementation of application level filtering, proxies, content-based filtering etc.

c. Wherever possible physical segregation must be preferred over logical segregation

12.5.10. **LAN security:** The organization must implement the following to ensure LAN security: **IG 10**

a. **Securing LAN devices**: Ensure that all default passwords of routers and switches are changed prior to deployment

b. **Strong device passwords:** Use strong passwords such using a minimum of 12 characters or more (combination of alphanumeric and special characters)

c. **Using secure protocols**: Disable all non-IP-based access protocols such as TELNET, and use secure protocols such as SSH, SSL, or IP Security (IPSec)

encryption for all remote connections to the router/switch/server

d. **Traffic monitoring**: Deploy traffic management capabilities which continuously monitors and controls IP network

e. **Allocating IP address**: Ensure that IP addresses allocated to each network appliance/system/server is associated with their respective MAC address and is not user modifiable

12.5.11. **Wireless LAN security:** The organization must implement the following for wireless LAN security: **IG 11**

a. **Limiting coverage of access points:** Organization must evaluate physical perimeter to define positioning of wireless device thereby limiting radio transmission and coverage, inside the physical premises or intended coverage area

b. **Device configuration:** Organization owned systems with ability to connect wireless network should be preconfigured with relevant and appropriate drivers by the relevant ICT personnel. Configuration of wireless access including Wi-Fi/Bluetooth and similar technologies should not be user configurable

c. **Wireless encryption:** Organization must ensure that communication between user system and wireless AP are secured using highest graded encryption (WPA-2 or higher) for data confidentiality and integrity. Under no circumstances, should open APs be deployed in the network

d. **Using secure protocols:** Organization must ensure that all available measures are applied on Access Points (APs) or WLAN switches to secure them from unauthorized access, use of plaintext protocols such as SNMP, Telnet or HTTP for access management services should not be done. Restrict systems from which management access is permitted

e. **Wireless security gateway:** Organization should place firewalls or application proxies between client and server subnets and before network admission of any new devices proper security scanning should be done.

f. **Visitor access to WLAN**: If the organization sets up external WLANs primarily to provide Internet access to visitors; such WLANs should be architected so that their traffic does not traverse the organization's internal trusted networks such as configuring a guest WLAN access with a second SSID for limiting guest access to Internet only. Organization should further ensure use of guest accounts and require login (guest authentication)

g. **Perform a WLAN security audit to identify vulnerabilities:** Organization with WLANs should conduct regular periodic security audit to see if organization's WLAN networks are vulnerable to attacks resulting from configuration errors; if equipment or software used have critical flaws that attackers can exploit to penetrate the network; if network is vulnerable to

denial of service; impersonation (rogue AP, DHCP, or other spoofing) attacks, and more

h. **Logging and monitoring:** Organization must have a logging mechanism in place to record and maintain unauthorized attempts and authorized user activity

i. **Prevent simultaneous connections:** Organization must implement appropriate technical security controls to separate Wi-Fi network and wired network, if any. Devices used for connecting the Wi-Fi network should not be allowed to connect simultaneously to the wired network such as by explicitly disabling or enabling wireless adapters

j. **Physical isolation:** Organization should ensure that there is proper physical isolation of sensitive and wireless networks. All the terminals or computers dealing with sensitive/classified information should not have any wireless equipment including Internet and Bluetooth

k. Disable SSID broadcasting to prevent the access points from broadcasting the SSID to enable only authorized users with preconfigured configured SSID to access the network

l. Disable DHCP and assign static IP addresses to all wireless users

12.5.12. **Disabling unused ports:** The organization must identify ports, protocols and services required to carry out daily operations and block all others, including all non-IP based and unencrypted protocols, by establishing policies in routers and wireless access points **IG 12**

12.5.13. **Personal devices usage policy:** Use of personal devices must be authorized by concerned personnel of the organization, with documented forms maintained to reflect approvals and rejections. This documentation should include fields such as employee name, employee ID, device approved/rejected status, date and time, device identity and type etc. *(refer section 20.2)* **IG 13**

a. The organization must perform security check of the personal device prior to authorization for use in official premises. A comprehensive security evaluation of the device must be performed to ensure no security loophole is induced in the network due to introduction of such devices. These checks should include at a minimum checking for malwares, open ports, installed firewall, antivirus, latest system patches installed amongst others

b. The organization must create a secure data container on the personal device

c. Classified information marked secret and top secret must be prohibited from storage, transaction or processing on personal devices

12.5.14. **Restricting access to public network:** The organization must disable unused network adapters in systems and restrict internet connection sharing and adhoc network creation. **IG 14**

a. Organization owned information assets should be configured to connect to organization owned/ operated networks only

b. Organization must disable Internet connection sharing, Ad hoc networks, Routing between virtual private network interfaces and other network interfaces on all organization owned devices

12.5.15. **Network access control:** The organization must implement network access control mechanism across the network **IG 15**

a. Verify identity of device upon request to connect to the network

b. Perform health scan of device post access to network resources

c. Authorize access to information sources post validation of policy implementation and update in device

d. There must be documented standards/procedures for managing external network access to the organization's information systems and networks, which specify: List of external connections must be maintained, access control must be implemented, allow only authorized remote device, external connection must be removed when no longer required

e. Information systems and networks accessible by external connections must restrict external network traffic to only specified parts of information systems and networks as per the business requirements, provide access to defined entry points, verify the source of external connections, log all security-related activity, record details relating to external connections established

f. Access to the network must be restricted to devices that meet minimum security configuration requirements, which includes verifying that devices which are authorized, are running up-to-date malware protection, have the latest systems and software patches installed, are connecting over an encrypted network

g. There should be policy for use of firewalls, remote access, VOIP and Telephony and Conferencing

12.5.16. **Firmware upgrade:** Organization must regularly check for updated firmware for network appliances. All upgrades must be installed post appropriate validation and testing **IG 16**

12.5.17. **Network change management:** Organization must test/simulate the changes required for the network in the network simulator tools before implementing in live environment **IG 17**

a. Ensure that appropriate test and simulation facility/ lab is available

b. Select and download appropriate patches/ upgrades and prepare them for test and simulation in facility/ lab

c. Examine test results to ensure there are no conflicts with existing patches/

upgrades

d. Appropriate permissions should be obtained from the concerned department

e. Significant changes to network configuration must be approved by the ISSC

12.5.18. **Securing transmission media:** All cables and encompassing cabinets must be secured from unauthorized access, physical damage and tampering **IG 18**

a. Ensure proper mapping and labeling of transmission media

b. Physical access to cables must be restricted

c. All connectivity points must be secured inside a cabinet

12.5.19. **Default device credentials:** The organization must ensure that default credentials of network devices and information systems such as usernames, passwords, tokens are changed prior to their deployment or first use **IG 19**

12.5.20. **Connecting devices:** The organization must identify active hosts connected to its network using tools and techniques such as IP scanners, network security scanners etc. **IG 20**

a. Deploy client-side digital certificates for devices to authorize access to network or information resources

12.5.21. **Audit & review:** *Refer section 21.2* **IG 21**

12.5.22. **Extending connectivity to third parties:** **IG 22**

a. The organization must restrict the use of ports, service, protocols etc. used for extending access of organizations network to third parties

b. The organization must limit the access granted to third parties to the purpose of granting such access and to the time duration specified for completion of defined tasks

c. The organization must ensure that network documentation provided to a third party, such as to a commercial provider, must only contain information necessary for them to undertake their contractual services and functions. Detailed network configuration information must not be published in documentation

d. All traffic emanating from third partied must be monitored

13. Identity, access and privilege management

13.1. Background

13.1.1. Users have a diverse set of access requirements based on their roles and privileges that lead to complex authentication, access, role & privilege management scenarios in respect of access to information and information systems

13.1.2. The access requirements vary widely from providing access to endpoints to network, server systems, applications, data and databases, messaging systems, and so on. Organization's information is stored, processed and shared over these components of infrastructure. Access to these systems may expose the users to the information

13.1.3. Further, users and user groups, with their respective operational roles, seek access to different information assets for diverse purposes and through various platforms and means. Changing operational ecosystem introduces significant level of dynamism in access requirements in the life cycle of information and information systems

13.2. Relevance of domain to information security

13.2.1. Identity breach is one of the most common threats for organization: intruders try and defeat the organizations authentication scheme; or might steal a critical element of their identity; or might misuse an attribute of their identity to engage in fraud

13.2.2. As there is significant complexity of user identities, privileges and access patterns, the organization may struggle to comprehend the exposure of information and exposure of information to unintended persons may get unnoticed

13.2.3. Without specific attention on identification, access and privilege management of employees of external service providers and vendors, information may be exposed outside the boundaries of an organization

13.3. Identity, access and privilege management guidelines

13.3.1. **Governance procedures for access rights, identity & privileges:** The organization must establish appropriate procedures to govern access rights to information systems and assets; establish a process for creation of identities; establish a process for defining user privileges and a devise a mechanism to understand how access to information is provided. **G 10**

a. Each information assets must have an appointed custodian or owner, who should be responsible for classification of data and approving access to the same

b. Information about the user identities, privileges, access patterns must be managed in secure manner

c. The management oversight must be enforced through the process of approval, monitoring and review to manage identity, users and privileges through their life cycles- identity request, creation, assignment, operations and revocation

d. The changes should be approved by a designated authority

e. The changes should be recorded for any future analysis

13.3.2. **Authentication & authorization for access:** The organizations must establish processes for authenticating each user accessing information systems or assets. The access requests should be authorized based on predetermined rules that consider type of information, access types, access requirements, users roles and security requirements *(Refer section 7.2)* **G 11**

a. Instances that authenticate users and authorize their access to critical information must be recorded

b. Inactive accounts must be disabled as per the organization's policy

13.3.3. **Password management:** The organizations must have standardized, reliable and secure way of managing passwords of users **G 12**

a. A standard for password must be defined length, type of characters permitted

b. Password history, password change duration etc. should be determined depending on the sensitivity of information and transactions

c. Password reset requests must be handled carefully and securely

d. Password of privileged user accounts should be handled with additional care

e. Shared passwords with vendors must be changed regularly

13.3.4. **Credential monitoring:** The organization must ensure that instances of user access provisioning, identification, authentication, access authorization, credential changes and deprovisioning are logged **G 13**

a. The access instances should be monitored and reviewed for identifying discrepancies

b. Malicious attempts of authentication should be prevented, recorded and reviewed

13.3.5. **Provisioning personal devices and remote access:** The organizations must ensure that provisioning of access to employees of external service providers and vendors is managed in a standardized and secure manner **G 14**

13.3.6. **Segregation of duties:** The organization must ensure that user roles are appropriately segregated for performing operations. It should be ensured that user levels and their designated actions are segregated based on the criticality of information and transactions **G 15**

a. Each user action must be distinguished from other users. Any discrepancies must be identified, reviewed and corrected

13.3.7. **Access record documentation:** The organization must ensure that it maintains an updated record of all personnel granted access to a system, reason for **G 16**

access, duration for which access was granted.

13.3.8. **Linkage of logical and physical access:** The organizations must correlate logical access instances with physical access rules for areas where sensitive information is processed and stored **G 17**

13.3.9. **Disciplinary actions:** The organizations must incorporate provisions for managing discrepancies and non-conformance in the disciplinary processes **G 18**

13.4. Identity, access and privilege management controls

13.4.1. **Operational requirement mapping:** The organization must ensure that operational requirements are carefully studied to translate them into access requirements **C 23**

13.4.2. **Unique identity of each user:** The organization must ensure that each user identity (User-ID) is uniquely attributable to only one unique user **C 24**

13.4.3. **User access management:** The organization must document procedures for approving, granting and managing user access including user registration/de-registration, password delivery and password reset. The procedures must be updated in a periodic manner as per policy **C 25**

a. **Authorization for access:** The organization must not allow access to information unless authorized by the relevant information or information system owners

13.4.4. **Access control policies:** The organization must define access control policies which are integrate-able with existing architecture and technological, administrative and physical controls **C 26**

13.4.5. **Need – to – know access:** Access rights to information and information systems must only be granted to users based on a need-to-know basis **C 27**

13.4.6. **Review of user privileges:** The organization must enforce a process to review user privileges periodically **C 28**

13.4.7. **Special privileges:** The organization must ensure that the use of special privileges shall be restricted, controlled and monitored as per organization's policy **C 29**

13.4.8. **Authentication mechanism for access:** The organization must enforce appropriate authentication mechanism to allow access to information and information systems which is commensurate with the sensitivity of the information being accessed. **C 30**

13.4.9. **Inactive accounts:** Inactive accounts must be disabled as per organizations policy **C 31**

13.4.10. **Acceptable usage of Information assets & systems:** The organization must define an acceptable usage policy and procedures specifying the security requirements and user responsibility for ensuring only organization mandated **C 32**

use of user account privileges

13.4.11. **Password policy:** The organization must define a password policy **C 33**

a. Password standards- such as minimum password length, restricted words and format, password life cycle, and include guidelines on user password selection

b. Password reset process must be set in order to secure the credential in the process

13.4.12. **Default device credentials:** The organization must ensure that all vendor-supplied default passwords for equipment and information systems are changed before any information system is put into operation **C 34**

13.4.13. **Monitoring and retention of logs:** The organization must monitor and retain records for all activity related to granting access to users **C 35**

13.4.14. **Unsuccessful log-in attempts:** The organization must monitor all log-in attempts to information systems and block access to users with consecutive unsuccessful log-in attempts **C 36**

a. The organization must ensure appropriate monitoring mechanism is available to identify fraudulent or malicious activity. The authorization credentials of user accounts suspected of being compromised must be reset immediately

13.4.15. **Ad-hoc access to systems:** The organization must ensure that prior approval from the head of the department is obtained in-case it is required to connect a departmental information system with another information system under the control of another organization. The security level of the information system being connected shall not be downgraded upon any such interconnect of systems **C 37**

a. Under any circumstances the authorization level should not allow vendors to access sensitive information / database of the organization. If needed proper supervision mechanism may be evolved to watch the activities of the vendors

13.4.16. **Remote access:** The organization must ensure that security measures are in place to govern the remote access to information systems **C 38**

a. Appropriate security technologies must be implemented to protect information or information systems being accessed via remote access. These may include use of protocols such as SSL, TLS, SSH and IPsec

13.4.17. **Provisioning of personal devices:** The organization must govern provisioning of access to personal computing devices such as smartphones, tablets, and memory devices to its internal network as per its security policy **C 39**

13.4.18. **Segregation of duties:** The organization must ensure that duties, roles, responsibilities and functions of individual users are segregated, considering **C 40**

factors such as conflict of privileges

13.4.19. **User awareness & liability:** The organization must ensure that all users are made aware of their responsibilities towards secure access to and usage of the organizations information and information systems. All users shall be accountable and responsible for all activities performed with their User-IDs **C 41**

13.5. Identity, access and privilege implementation guidelines

13.5.1. **Operational requirement mapping:** The organization must develop a formal procedure to govern allocation of user identification and access mechanism. All privileges associated with a user-ID must also be governed as per standard procedure **IG 23**

a. Operational roles must be mapped to corresponding IT roles

b. IT roles must be grouped for performing particular operations

c. Credential requirements of the roles must be mapped carefully

d. Operational rules for granting and revoking access must be studied and an inventory should be created of the same

13.5.2. **Unique identity of each user**: All employees including temporary and contract workers must be allotted a unique ID. The system for managing user IDs must function directly under the head of the department or his authorized representative **IG 24**

a. User identity schemes must be defined and enforced

b. Identity provisioning workflow must be defined with proper checks and balances

c. Identity provisioning process must be audited at periodic interval

d. Any sharing of user ID's should be restricted to special instances, which are duly approved by the information or information system owner

e. The shared ID's passwords must be changed promptly when the need no longer exists and should be changed frequently if sharing is required on a regular basis

f. There must be clear ownership established for shared accounts

g. There must be a log maintained as to whom the shared ID was assigned at any given point of time. Multiple parallel sessions of the same ID must be strictly prohibited

13.5.3. **User access management:** The organization must establish a process to manage user access across the lifecycle of the user from the initial registration of new users, password delivery, password reset to the final de-registration of users who no longer require access to information systems and services in the organization **IG 25**

a. Details of users authorized by the head of the department to access

information systems and devices must be communicated as per standard user access request form containing details such as name of person, location, designation, department, access level authorization, access requirement for applications, databases, files, information repositories etc.

b. Any changes or update to user access level must be made only post approval from head of department

c. User access deactivation request must be submitted immediately upon termination of employment, instances of non-compliance, suspicious activity and incase required as part of disciplinary action etc.

d. The organization must ensure that all user access requests are well documented with details including, but not restricted to, reason for access, user details, type or user – admin, super user, contractor, visitor etc., period of access, HOD approval, information asset/ system owner approval

13.5.4. **Access control policies:** The organization must enforce, govern and measure compliance with access control policy. **IG 26**

a. **Enforcement of access control policies:** Access control policies must be defined to be enforced on ICT infrastructure components such as network, endpoints, servers systems, applications, messaging, databases and security devices

b. **Governance of access control policies:** Access to the systems, network resources and information must be governed as per organization's policies

c. **Compliance with access control policies:** Non-conformance to policy must be monitored and dealt with as per standard practice defined by organization

d. **Correlation of logical and physical access**: The organization must implement a mechanism to correlate instances of physical access and logical access using IP enabled physical security devices, collection and correlation of logs and rules written to correlate physical and logical instances

13.5.5. **Need – to – know access:** Access privileges to users must be based on operational role and requirements **IG 27**

a. Access to higher category of classified information must not be granted unless authorized by information owner

b. Access to systems containing higher category of classified information must be restricted by logical access control

c. Access security matrix must be prepared which contains the access rights mapped to different roles. This must be done to achieve the objective of role based access control (RBAC)

d. Access to system must be granted based on access security matrix

13.5.6. **Review of user privileges:** All user accounts must be reviewed periodically by concerned authority by use of system activity logs, log-in attempts to access non-authorized resources, abuse of system privileges, frequent deletion of data by user etc. **IG 28**

13.5.7. **Special privileges:** The organization must ensure that the use of special privileges for users to access additional information systems, resources, devices are granted only post documented approval from information owner **IG 29**

a. All such additional privileges must be issued for a pre-notified duration and should lapse post the specified period.

b. Allocation of special privileges must be strictly controlled and restricted to urgent operational cases

c. All activity conducted with the use of special privileges must be monitored and logged as per organization's policy

13.5.8. **Authentication mechanism for access**: The organization must have various levels of authentication mechanisms **IG 30**

a. Depending on the sensitivity of information and transactions, authentication type must vary

b. For access to sensitive information system, authentication such as 2-factor authentication should be implemented. Authentication levels must be defined to include a combination of any two of the following authentication mechanisms:

   Level 1: PIN number or password authentication against a user-ID

   Level 2: Smart card or USB token or One-time password

   Level 3: Biometric identification

c. Credential sharing must be performed on an encrypted channel which is separate from the message relay channel

d. Use directory services such as LDAP and X500

13.5.9. **Inactive accounts:** The organization must ensure the following: **IG 31**

a. All user accounts which are inactive for 45 days should be disabled

b. The authentication credentials of all disabled accounts must also be reset upon deactivation

c. All disabled accounts must be reactivated only post verification of the user by concerned security administrator

d. All accounts in disabled state for 30 days must be deleted

13.5.10. **Acceptable usage of Information assets & systems:** The organization must ensure that users are made aware of their responsibility to use their account privileges only for organization mandated use **IG 32**

a. The organization must clearly state that it provides computer devices, networks, and other electronic information systems to meet its missions, goals, and initiatives and users must manage them responsibly to maintain the confidentiality, integrity, and availability of the organizations information

b. This needs to be elaborate across areas such as email, internet, desktops, information, clear desk policy, password policy etc.

c. The organization must obtain user sign-off on acceptable usage policy

13.5.11. **Password policy:** The organization must define its password policy, with specific focus on password issuance and activation methods along with standard process for governance and communicate the same to user upon creation of user account **IG 33**

a. All active sessions of a user must be terminated post 15 minutes of inactivity and must be activated only post re-authentication by specified mechanism such as re-entering password etc.

b. Passwords must be encrypted when transmitting over an un-trusted communication network

c. Issue guidelines to end user to help in selection of strong alphanumeric password comprising of a minimum of 12 characters

d. Prevent users from using passwords shorter than a pre-defined length, or re-using previously used passwords

e. Passwords must be automatically reset if user accounts are revoked or disabled upon inactivity beyond 30 days of inactivity

f. Password communication must on verified alternate channel such as SMS, email, etc.

13.5.12. **Default device credentials:** The organization must ensure that default login credentials of devices such as routers, firewall, storage equipment etc, are changed prior to the deployment of such devices in the operational environment **IG 34**

13.5.13. **Monitoring and retention of logs:** The organization must retain information pertaining to requests for user ID creation, user rights allocation, user rights modification, user password reset request and other instances of change or modification to user profile, as per audit and governance requirements **IG 35**

13.5.14. **Unsuccessful login attempts:** The organization must monitor unsuccessful log-in attempts from each of the authentication mechanisms, to track for consecutive unsuccessful log-in attempts **IG 36**

a. The user account must be disabled for a pre-defined limit post five unsuccessful log-in attempts

b. A random alpha numeric text CAPTCHA should be introduced post second unsuccessful log-in attempt

13.5.15. **Ad-hoc access to systems:** The organization must ensure that authentication credentials of information systems which are disclosed to vendors for maintenance and support are reset on a periodic basis or upon termination of maintenance activity, as defined under the organization's policy **IG 37**

13.5.16. **Remote access:** Appropriate device configuration must be maintained and security capability must be deployed, to prevent remote access to information systems and data from outside the organizations boundary, unless approved by the head of the department. **IG 38**

a. Implement appropriate security technologies to protect information or information systems being accessed via remote access, such as using VPN based on SSL/TLS, SSTP or IPsec

b. Enable capture of logs of all activity conducted via remote access

c. Audit logs of all activity conducted via remote access

13.5.17. **Provisioning of personal devices:** *Refer section 20.3* **IG 39**

13.5.18. **Segregation of duties:** The organization must ensure the following: **IG 40**

a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion

b. Documents separation of duties

c. Implements separation of duties through assigned information system access authorizations

d. Restricts mission functions and creates distinct information system support functions are divided among different individuals/roles

e. Prevent different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security)

f. Separate security personnel who administer access control functions from performing administer audit functions

g. Create different administrator accounts for different roles

13.5.19. **User awareness & liability:** *Refer section 17.4* **IG 41**

14. Physical and environmental security

14.1. Background

14.1.1. Organizations generally have multiple touch points, which may be spread across different geographic regions, from where information can be accessed physically. Thus geographies, locations and facilities play an important role in the security posture of information and information systems

14.1.2. Physical aspects have a role in determining how information and information systems are housed in a facility, who can possibly reach physical systems, which way one can enter or exit from the facility, what can human elements physically do with the system housed in a facility and what will be impact of regional physical events on the particular facilities

14.1.3. Physical security in an important component of information security and requires a careful attention in planning, selecting countermeasures, deploying controls, ensuring secure operations and respond in case of an event

14.1.4. Physical security is not only restricted to barriers or locks but have evolved with the use of access control measures, risk based or multifactor authentications, monitoring cameras, alarms, intrusion detectors, etc.

14.2. Relevance of domain to information security

14.2.1. Lack of due consideration to the area and to the choice of the building may expose information and IT systems to threats. Choice of the area, building architecture and plan have a significant impact on security posture of information and information systems

14.2.2. Insufficient entry controls may give access to unintended persons. It may allow entry of unauthorized assets or easy passage of sensitive assets from premises

14.2.3. Without adequate interior physical control, unauthorized personnel may gain access to sensitive areas. Instances such as theft of information may remain undetected

14.2.4. Without processes for physical access provisioning and deprovisioning, governing access to the sensitive physical locations will remain a challenging task. This will have serious impact on security of information and information during their life cycle in a particular physical facility

14.3. Physical and environmental security guidelines

14.3.1.	**Map and characteristics of physical facilities:** The organization must create an map of access point and information assets and systems housed within	**G 19**
14.3.2.	**Protection from hazard:** The organization must ensure that all facilities housing information systems and assets are provided with adequate physical security measures, which include protection from natural and man-made hazard	**G 20**
14.3.3.	**Physical boundary protection:** The organization must deploy an adequate level of perimeter security measures such as barriers, fencing, protective lighting, etc.	**G 21**
14.3.4.	**Restricting entry:** The organization must deploy an adequate level of countermeasures for restricting the entry to the facilities only to authorized persons	**G 22**

14.3.5. **Interior security:** The organization must ensure that all information systems and assets are accessed by only authorized staff and protected by adequate interior security measures **G 23**

14.3.6. **Security zones:** The organization must ensure that appropriate zones are created to separate areas accessed by visitors from areas housing classified information assets and systems **G 24**

a. **Basis information classification:** Appropriate security zones must be created inside the premises/ building based on the location of information assets and systems, commensurate with the classification of information

b. **Marking of zones:** Zones must be clearly marked to indicate type of personnel allowed access to the said zone within the premise

c. **Security and monitoring of zones:** Strict security measures in addition to round the clock monitoring of such areas must be done

14.3.7. **Access to restricted area:** Access of people and equipment movement and disposal from the restricted area should be regulated and governed. A special care must be taken for wearable devices. Such clearances should be done by the concerned head of the department. The organization must establish a methodology to ensure coordination between internal functions and staff for the same **G 25**

14.3.8. **Physical activity monitoring and review:** All physical access to information assets and systems should be monitored and tracked. User should not be allowed to carry external devices such as laptops; USB drives etc. without prior approval and authorization, into areas which house critical information infrastructure such as data centers etc. **G 26**

14.4. Physical and environmental security controls

14.4.1. **Map and characteristics of physical facilities:** The organization must obtain visibility over physical facilities and information systems housed within **C 42**

a. A list of persons who are authorized to gain access to information assets and systems housed in data centers or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and should be reviewed periodically

14.4.2. **Hazard assessment:** The facility housing information assets and systems must be protected from natural hazard and man-made hazard. All facilities located in geographically vulnerable areas must undergo annual assessment to check structural strength **C 43**

14.4.3. **Hazard protection:** All facilities must be equipped with adequate equipment to counter man-made disasters or accidents such as fire. The facility should have a combination of hazard detection and control measures such as smoke sensors, sprinklers, fire extinguishers etc. Other sensors and alarms should also be installed for early warning **C 44**

14.4.4. **Securing gateways:** All entry and exit points to facilities housing information assets and systems must be secured by deploying manpower and appropriate technological solutions **C 45**

14.4.5.	**Identity badges:** The entry to a facility is restricted to only those users who provide proof of their organizational identity. Users must be aware of the importance of carrying their identity proof with them	**C 46**
14.4.6.	**Entry of visitors & external service providers:** the organization must define process for allowing and revoking access to visitors, partners, third-party service providers and support services	**C 47**
14.4.7.	**Visitor verification:** All visitors to the facility must only be permitted to enter post validation from concerned employee. Visitor must be instructed to record their identity credentials into the visitor register prior to permitting them inside the facility	**C 48**
14.4.8.	**Infrastructure protection:** Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage	**C 49**
14.4.9.	**Guarding facility:** The organization must ensure that an adequate number of security guards are deployed at the facilities	**C 50**
14.4.10.	**Vehicle entry:** Ensure that an adequate level of security measures are implemented for vehicle entry & exit, vehicle parking areas, loading/unloading docks, storage areas, manholes, and any other area that may provide passage for physical intrusion	**C 51**
14.4.11.	**Correlation between physical and logical security:** The instances of physical access should be analyzed with logical access instances. Restrictions should be imposed for on premise access of information systems to unauthorized personnel.	**C 52**
14.4.12.	**Monitoring & surveillance:** All entry and exit points should be under surveillance round the clock to look for suspicious activity. Further, all security zones inside the facility/ building must be secured by deploying manpower and appropriate security technologies	**C 53**
14.4.13.	**Disposal of equipment:** Physical disposal of computer or electronic office equipment containing non-volatile data storage capabilities must be checked and examined to ensure all information has been removed. Destruction, overwriting or reformatting of media must be approved and performed with appropriate facilities or techniques such as degaussing of hard drives, secure delete technologies etc. *(Refer Annexure 7.2)*	**C 54**
14.4.14.	**Protection of information assets and systems:** All information assets and systems must be protected with appropriate access control methodologies such as authorized log-in and password control, smart cards or biometric access	**C 55**
14.4.15.	**Authorization for change:** Ensure that security authorization is performed for all changes pertaining to physical security, instances that may introduce security vulnerabilities and exception to the policy	**C 56**

14.4.16. **Inactivity timeout:** All information systems must be configured to time-out a user's activity post inactivity for a designated period of time **C 57**

14.4.17. **Protection of access keys and methodology:** All access keys, cards, passwords, etc. for entry to any of the information systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures **C 58**

14.4.18. **Shoulder surfing:** The display screen of an information system on which classified information can be viewed shall be carefully positioned so that unauthorized persons cannot readily view it **C 59**

14.4.19. **Categorization of zones:** The facilities in the organization must be categorized based on parameters such as the sensitivity of information in the facility, roles of employees in facilities, operational nature of facility, influx of visitors etc. **C 60**

14.4.20. **Access to restricted areas:** Visitors requiring access to restricted areas, in – order to perform maintenance tasks or activities must be accompanied by authorized personnel from the concerned department at all times. A record of all equipment being carried inside the facility must be maintained along with equipment identification details. Similarly a record of all equipment being carried outside the facility must be recorded and allowed post validation and written consent from employee concerned **C 61**

14.4.21. **Visitor device management:** Visitors must be instructed to avoid carrying any personal computing devices or storage devices inside facilities housing classified information, unless written permission is obtained from the head of the department **C 62**

14.4.22. **Physical access auditing and review:** All attempts of physical access must be audited on a periodic basis **C 63**

14.5. Physical security implementation guidelines

14.5.1. **Map and characteristics of physical facilities:** The organization must appropriately position security and monitoring measures commensurate with criticality of Physical facilities, information and IT systems housed within these facilities **IG 42**

a. Create map of facilities, their entry & exit points, deployment of IT systems and people

b. Create list of authorized personnel, permitted to access areas/ facility housing sensitive information systems/ devices, should be maintained at all entry points

c. Physical access to such areas/facility must be granted only post verification of person as well as by user authentication by use of smart cards, etc.

14.5.2. **Hazard assessment:** The organization must undergo hazard assessment at regular intervals to counter disasters or accidents such as fire safety risk assessment, seismic safety assessment, flood control assessment and other **IG 43**

natural calamities amongst others

14.5.3. **Hazard protection:** The organization must deploy sufficient tools, techniques, equipment etc., to deal with hazard. Capability for detection, prevention and control measures such as fire alarms, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings must be available in each facility housing classified information **IG 44**

14.5.4. **Securing gateways:** All entry and exit points to facilities/areas housing classified information in an organization must have biometric access controls such as fingerprint scanners or other similar gateway access control mechanisms **IG 45**

14.5.5. **Identity badges:** The organization must issue photo identity cards with additional security features such as smart chips to employees for identification and entry to facilities **IG 46**

a. Appropriate measures must be undertaken to prevent tailgating inside the organizations facility

14.5.6. **Entry of visitors & external service providers:** The organization should maintain records for visitor entry such as name of visitor, time of visit, concerned person for visit, purpose of visit, address of the visitor, phone number of the visitor, ID proof presented, devices on-person etc. **IG 47**

a. Entry by visitors such as vendor support staff, maintenance staff, project teams or other external parties, must not be allowed unless accompanied by authorized staff

b. Authorized personnel permitted to enter the data center or computer room must display their identification cards at all instances

c. Visitor access record shall be kept and properly maintained for audit purpose. The access records may include details such as name and organisation of the person visiting, signature of the visitor, date of access, time of entry and departure, purpose of visit, etc.

d. The passage between the data center/computer room and the data control office, if any, should not be publicly accessible in order to avoid the taking away of material from the data center/computer room without being noticed

14.5.7. **Visitor verification:** Visitor entry must be permitted only if prior notification has been shared via email from the concerned personnel. **IG 48**

a. Visitors must present a valid photo identification card, preferably issued by the Government of India at the reception, for verification

b. Visitors must always be escorted by the concerned person into the designated meeting area in the facility

c. Visitors should be issued a temporary identity card that identifies them as

a visitor and must be returned to issuing authority while leaving the premises after marking out time in the visitor's record

14.5.8. **Infrastructure protection:** **IG 49**

a. Power and telecommunication lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection

b. Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas

c. Power cables and switching centers should be segregated from communication cables to prevent interference

14.5.9. **Guarding facility:** Background checks of all private guards manning the facility should be conducted prior to employment/ deployment. Details such as address verification, criminal records, past experience, references, family details, medical records must be maintained as a minimum **IG 50**

a. Ensure that background checks and credibility is established prior to recruitment of guards. In- case guards are hired from a third party organization a stringent process to verify and establish credibility of the third-party organization must also be undertaken

b. The organization must conduct regular trainings for security guards to handle routine security operations as well as security incidents, physical intrusions, awareness about new storage devices, etc.

14.5.10. **Vehicle entry:** Adequate security measures should be adopted at vehicle entry, exit and parking areas such as deploying physical barriers, manual inspection of vehicles, security lighting, video surveillance, deploying adequate security guards etc. **IG 51**

14.5.11. **Correlation between physical and logical security:** Physical security and logical security linkages must be created **IG 52**

a. Only approved personnel should have physical access to facility housing systems or devices which enable physical or logical access to sensitive data and systems. This includes areas within the facility which house backup tapes, servers, cables and communication systems etc.

b. Access controls should encompass areas containing system hardware, network wiring, backup media, and any other elements required for the system's operation

14.5.12. **Monitoring & surveillance:** The organization must establish mechanism for 24/7 surveillance of all areas inside the physical perimeter by use of technology such as security cameras (or closed-circuit TV) **IG 53**

a. The organization must monitor the areas such as hosting critical/sensitive systems and have video images recorded. The recording of the camera

should be retained for at least a month for future review

b. Intruder detection systems can be considered to be installed for areas hosting critical/sensitive systems

14.5.13. **Disposal of equipment:** Destruction and disposal of hard drives/ memory devices should be performed by techniques such as removing magnets, hammering, burning, degaussing, shredding, secure deletion etc. **IG 54**

a. Any equipment, being carried out of the facility for disposal, must be authorized by the head of the department, under whom the equipment was deployed as well as the concerned representative of the information security team

14.5.14. **Protection of information assets and systems:** Physical access to information assets and systems must be governed by employing techniques such as biometric access, smart cards, passwords etc. **IG 55**

14.5.15. **Authorization for change:** Any modification or changes to the physical security layout/ established procedure must be done post documented approval of concerned authority in the security team/ Head of the department **IG 56**

14.5.16. **Inactivity timeout:** All information systems should be configured to automatically lock the computer system after 10 minutes of inactivity **IG 57**

14.5.17. **Protection of access keys: :** All access keys, cards, passwords, etc. for entry to any of the information systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures **IG 58**

a. Maintain a record of all physical access keys by capturing details such as serial number, card ID

b. Create a mapping of physical cards issued with details of person authorized to use the same

c. Establish governance and audit procedures to manage issue of all physical access cards and eventual return to concerned authority on employee departure or revocation of access rights of individual authorized to access using physical cards

14.5.18. **Shoulder surfing:** Information systems containing classified information should be secured, to avoid shoulder surfing, by deploying privacy filter, positioning the systems to reduce chances of unauthorized viewing **IG 59**

14.5.19. **Categorization of zones:** The facility should be categorized as follows: **IG 60**

a. **Public zone:** where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples: the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings

b. **Reception zone**: where the transition from a public zone to a restricted-access area is demarcated and controlled. It is typically located at the entry

to the facility where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons

c. **Operations zone:** an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously. Examples: typical open office space, or typical electrical room

d. **Security zone:** area to which access is limited to authorized personnel, and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously. Example: an area where secret information is processed or stored

e. **High security zone**: an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications, monitored continuously and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel

14.5.20. **Access to restricted areas:** Visitors requiring access to restricted areas must be accompanied by authorized personnel. Visitor details such as name of the visitor, time of visit, purpose of visit, serial number of the equipment (if being carried), name of authorized person, signature of authorized person etc. must be maintained by the security personnel responsible for the area/facility **IG 61**

a. In case, any equipment is being carried out by the visitor, appropriate written authorization granted by the head of the department/ concerned official must be presented to security personnel

b. An inventory of all equipment taken out of the facility should be maintained. Details such as equipment name, serial number, model number, department/ owner, name of approver etc. must be maintained

c. The information security team must co-authorize the removal of equipment from its deployment site

14.5.21. **Visitor device management:** Visitors must not be allowed to carry personal computing or storage devices such as USB, laptop, hard drive, CD/DVD etc. unless written permission is obtained from head of department. **IG 62**

a. Wearable devices: Visitors must be prohibited from carrying any wearable computing and processing devices such as smart watch's, glass or similar equipment

b. All visitors and Third parties authorized to carry information processing equipment (like Laptops, Ultra books, PDAs) or Media (like Mobile phones with cameras, DVD/CDs, Tapes, Removable storage), shall be asked to declare such assets. They will be issued a returnable gate pass

containing the date, time of entry and departure along the type of equipment and its serial number, if applicable. The same shall also be recorded in a register at the security gate.

c. Equipment like laptops, hard disks, tape drives, camera mobile phones, etc. shall not be allowed inside the restricted areas, shared services area, etc. unless authorized by the concerned authority

14.5.22. **Physical access auditing and review:** All attempts of physical access must be captured in logs and audited for illegal access attempts, number of access attempts, period of access, facilities visited etc. The following steps should be undertaken **IG 63**

a. Enabling and collecting logs physical devices

b. Writing rules to correlate logs to identify physical security incidents

c. Integrating physical security logs with logical security logs

d. Integrating physical security with SIEM solutions

e. Real time monitoring of physical security logs for classified information

15. Application security

15.1. Background

15.1.1. Application portfolios of organizations are becoming increasingly complex with a mix of legacy applications, addition of new applications, deployment of enterprise packaged applications and adoption of externally provisioned applications. Each of these applications and their modules provide means of achieving a certain set of organizations objectives. These variations at various fronts expose information to a larger threat landscape

15.1.2. Protecting applications against attacks simply by defending the perimeter with firewalls and network traffic encryption has proven to be insufficient. To address the risks at application layer, several technology and tactical measures have emerged that have helped the evolution of 'application security' as an important discipline in itself. The application itself should build in additional security measures, depending on the vulnerability of the system and the sensitivity of the data it is dealing with

15.2. Relevance of discipline to information security

15.2.1. As most information, both for operational and governance operations, is processed and transacted through applications, it becomes important to secure applications throughout their lifecycle

15.2.2. Information of the organization may be compromised or exposed if applications are not securely designed, developed, tested, configured and deployed

15.2.3. Inadequate visibility over how applications handle information; inadequate effort and resources deployed for application security; and lack of key application security capabilities endanger security of information

15.2.4. Applications liberate access to information and information systems, providing multiple avenues for internal as well as external users to connect and perform their respective tasks. However, they provide opportunities to attackers or introduce security threats which may help attackers penetrate into information systems

15.2.5. Applications are undergoing continuous innovation, several architectural ideas and platforms are under evolution and numerous have already been deployed. New ways of managing and setting up sessions are being implemented and transaction processing is undergoing change with respect to the way information is handled. This makes applications vulnerable to many new types of attacks

15.3. Application security guidelines

15.3.1.	**Application security process:** The organization must establish application security processes to ensure all tasks performed for securing applications are done in a standardized manner	**G 27**
15.3.2.	**Application design**: The organization must ensure that the system specification and design phase should incorporate necessary and relevant practices for application security	**G 28**
15.3.3.	**Application threat management:** The organization must ensure a threat model is built, and threat mitigation measures are present in all design and	**G 29**

functional specifications by analyzing high-risk entry points and data in the application

15.3.4. **Application security testing:** The organization must have a plan for testing applications for identifying vulnerabilities and weaknesses **G 30**

15.3.5. **Data management:** Information owners must evaluate the sensitivity of their data and define associated parameters for securing information **G 31**

15.3.6. **Application lifecycle management:** The organization must ensure that appropriate security measures such as version control mechanism and separation of environments for development, system testing, acceptance testing, and live operation are adhered with **G 32**

15.3.7. **Application vulnerability intelligence:** The organization must ensure that it compiles information around application vulnerabilities, exposures and weaknesses. The information should be compiled from both internal and external sources **G 33**

15.3.8. **Application security governance:** The organization must deploy a governance mechanism to ensure that the security issues of applications are timely identified, analyzed and remediated **G 34**

15.4. Application security controls

15.4.1. **Application security process:** The organization must ensure that documentation and listing of applications is properly maintained and relevant personnel are tasked with dedicated responsibilities for application security **C 64**

15.4.2. **Application security architecture:** The organization must ensure that application security is considered during the design of application **C 65**

a. Application security controls should be planned in early stages of the development rather than post deployment

15.4.3. **Application user authentication:** User authentication by the application must be managed in a standardized manner **C 66**

15.4.4. **Secure configuration:** Ensure that the application and system are properly and securely configured, including turning off all unused services and setting security configurations as per policy **C 67**

a. **Installation audit and control:** The organization must audit and control the installation of all computer equipment and software

15.4.5. **Ports & services:** Ensure that unused or less commonly used services, protocols, ports, and functions are disabled to reduce the surface area of attack **C 68**

15.4.6. **Session management:** The organization must ensure that applications have proper and secure session management to protect the sessions from unauthorized access, modification or hijacking **C 69**

15.4.7. **Input validation:** The organization must ensure that strict validation is applied to all input of the application such that any unexpected input, e.g. overly long input, incorrect data type are handled properly and would not introduce a exploitable vulnerability into the application **C 70**

a. Ensure that security mechanisms are designed to reject further code execution if application failure occurs

15.4.8. **Error handling:** The organization must ensure that error handling by applications should not provide system information or become reason for denying service, impairing system or leading to a system crash **C 71**

15.4.9. **Application security testing:** The organization must test applications to know their strength against contemporary security threats **C 72**

a. Security testing schedule for the applications must be defined considering their criticality and sensitivity

b. Testing requirements, testing types, and frequency of testing should be defined for the applications

15.4.10. **Code review:** For sensitive applications, the source code must be reviewed for evaluating vulnerabilities. Code review should be done while new application is being developed or any significant changes are under progress **C 73**

15.4.11. **Black box testing:** Application security testing, vulnerability assessment and penetration testing, should be performed at a frequency determined by sensitivity of the information handled by applications **C 74**

15.4.12. **Data handling:** The organization must ensure that applications handle data in a secure manner **C 75**

15.4.13. **Least privileges:** The organization must ensure that applications are designed to run with least amount of system privileges necessary to perform their tasks **C 76**

15.4.14. **Segregation of duties:** The organization must ensure that the practice of segregation of duties is followed in such a way that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process **C 77**

15.4.15. **Secure Software Development Life-Cycle (SDLC) processes**: The organization must ensure that security is considered at different stages of application development ,deployment and maintenance such as application conceptualization, requirement definition, architecture planning, development, testing, deployment, operation and continuous improvement **C 78**

15.4.16. **Application change control:** The organization must develop a change control procedure for requesting and approving application/system changes. All change activity must be documented **C 79**

15.4.17. **Application vulnerability intelligence:** Ensure that application threat management incorporates knowledge about vulnerabilities from both internal as well as external intelligence sources **C 80**

15.4.18. **Application logs & monitoring:** Ensure that applications have the capability of generating logs of exceptions, error or other instances which impact security **C 81**

15.5. Application security implementation guidelines

15.5.1. **Application security process:** The organization must maintain an updated document containing the list of authorized applications, their usage, custodian(s) assigned to each application, level of criticality, version implemented, Number of installed instances, application license details etc. **IG 64**

a. Specific personnel must be entrusted with the task of application security, who should be accountable for defining and enforcing enterprise level standards and guidelines for application security

b. The application security process should specify tasks and activities required to be performed for application security

c. The process should drive and guide other organizational functions such as operations, application development and maintenance and infrastructure management for the purpose of application security

15.5.2. **Application security architecture:** For applications developed in-house or sourced from a third party vendor, the organization must ensure that secure coding principles are adhered to. **IG 65**

a. The web software applications must be developed as per secure coding guidelines such as the Open Web Application Security Project (OWASP) guidelines

b. Methods such as threat modeling, data flow, risk assessment etc. should be deployed to understand the threat exposure of an application

c. Application interactions, data handling, session management, processing of transactions, authentication, authorizations, etc. should be planned in early stages

d. The applications must not have hardcoded passwords to connect to other databases and start services

e. There must be application security standards developed and all applications must be subjected to those during the time of induction or during any major change release

15.5.3. **Application user authentication:** Ensure applications integrate with central authentication systems to authenticate users **IG 66**

a. Authorization of users should be based on centralized system rather than at an individual application level. Application may be integrated with central authentication system such as active directory

b. Authorization and access to resources should be based role, affiliation and membership of group rather than individual basis

c. Periodic review of authorization should be performed

15.5.4. **Secure configuration:** Ensure that applications are securely configured through use of secure protocols and services and measures such as implementing encrypted storage of data, using strong password for administrative access of application amongst others **IG 67**

a. Perform installation security audit prior to production launch and post major changes to the system

15.5.5. **Ports & services:** The organization must identify ports, protocols and services required to carry out daily operations of application and restrict or block all others, including all non-IP based and unencrypted protocols, in addition to removing unnecessary content such as server banners, help databases, online software manuals, default or sample files etc. **IG 68**

15.5.6. **Session management:** Ensure that applications have secure session management to protect the sessions from unauthorized access, modification or hijacking **IG 69**

a. Protection measures include generating unpredictable session identifiers,

limiting the session lifetime, applying appropriate logout function and idle session timeout, and filtering invalid sessions

b. Ensure that sessions established by applications are secured by using appropriate encryption technologies, especially when sensitive information is transferred using HTTPS/TLS protocols

c. Ensuring encrypting sensitive session contents using protocols such as S/MIME

15.5.7. **Input validation:** Ensure applications validate input properly and restrictively, allowing only those types of input that are known to be correct. Examples include, but are not limited to, cross-site scripting, buffer overflow errors, and injection flaws amongst others **IG 70**

a. Organization should ensure that applications validate the data on the server-side and not on client-side

15.5.8. **Error handling:** Ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system **IG 71**

a. Ensure that the application will provide meaningful error message that is helpful to the user or the support staff

b. Ensure that errors are detected, reported, and handled properly

c. Error messages shouldn't reveal much information

d. No debug message for errors, no debugging in application itself

e. Application safe mode for occurrence of unexpected instance

15.5.9. **Application security testing:** Ensure comprehensive security testing of applications in its lifecycle. The testing may be performed either in-house or in government approved labs : **IG 72**

a. Applications should be subjected to rigorous application security testing and risk assessment since the beginning of design phase

b. Application security testing process must be coordinated with and approved by authorized individuals in an organization

c. Vulnerability scans should be performed whenever there are developer changes to application code or configuration

d. Daily vulnerability scanning for sensitive applications

e. All security flaws should be prioritized, and fixed prior to the release of the application

f. Flaws discovered in applications that are already released must be assessed to determine whether there is a low/medium/high level of exposure due to the following factors:

i. The likelihood that the security flaw would be exposed

ii. The impact on information security, integrity and application availability

iii. The level of access that would be required to exploit the security flaw

g. Automated escalation workflow of resolving application security flaws

h. Emergency procedures for addressing security flaws must be defined and

documented prior to production deployment. Methods such as limiting application use, blocking access, temporarily blocking some parts of applications must be used amongst others

15.5.10. **Code review:** The organization must conduct code-level security reviews with professionally trained personnel for all applications along with document details of actions performed **IG 73**

a. Perform source code review to identify security bugs overlooked during development stage. It may focus on input validation, information leakage, improper error handling, object reference, resource usages, and weak session management

b. Organization should consider reviewing the source code of the application for vulnerabilities with the help of government approved labs or organizations such as DRDO

c. Code review by automated code review tools

d. Combination of automated tool and manual skills for code review

15.5.11. **Black-Box Testing:** Ensure specification based testing is performed, to assure that defined input will produce actual results that agree with required results documented in the application development specifications **IG 74**

a. Periodic application penetration testing must be performed

b. Quarterly for sensitive application

c. Vulnerabilities identified should be resolved on priority based on the criticality of the underlying information impacted

d. For sensitive applications, critical vulnerability must be resolved within 3 days of detection

15.5.12. **Data handling:** The organization must ensure that applications handle data securely, by use of: **IG 75**

a. Security measures based on classification of data

b. AES 128 bit encryption for the classification level of secret

c. AES 256 bit encryption for storage for the classification level of top secret

d. Auditing of each instance of data access

15.5.13. **Least privileges:** User privileges and rights to use an application must be configured using the principle of least functionality with all unnecessary services or components removed or restricted **IG 76**

a. Ensure that end-user account only has the least privilege to access those functions that they are authorized, and the account has restricted access to backend database, or to run SQL or other OS commands

b. Restrict access to application and web server system or configuration files

15.5.14. **Segregation of duties:** The organization must ensure that no employee handles more than one critical function and avoid execution of all security functions of an information system by a single individual. Functions such as custody of assets, record keeping, authorization, reconciliation etc. should be allocated to different individuals **IG 77**

a. The access rights shall be kept to the minimum and authorized by the

application owner

b. Ensure that proper access control is implemented to enforce the privileges and access rights of the users

15.5.15. **Secure Software Development Life-Cycle (SDLC) processes:** The organization must incorporate security at each level of software development lifecycle such as during development, deployment and maintenance of application etc. to limit inclusion of threats or vulnerabilities **IG 78**

a. SDLC processes such as change management, release management, test management, backlog management should incorporate security

b. Security responsibility of SDLC roles such as change manager, release management, engineering support, platform manager must be defined

c. SDLC infrastructure such as development, test, build, integration and pilot environments must be segregated

d. Security testing must be incorporated in each stage of SDLC

15.5.16. **Application change control:** The organizations must implement and maintain a change management process to track and monitor activity related with changes to existing software applications **IG 79**

a. Activity such as application maintenance, installation of critical changes, review of changes and post testing, responsibility of changes, documenting change requests amongst others must be documented with relevant details

b. Each significant change in application must be approved ISSC

15.5.17. **Application vulnerability intelligence:** Ensure that a mechanism exists to manage the application security specific information **IG 80**

a. Sources of information

   i. Internal sources: historical vulnerability trend of application, vulnerability scans and penetration testing results

   ii. External sources: vulnerability databases, exploit & threat databases, vendor alerts and third party penetration testers

b. Diligent integration of intelligence in application threat management process

15.5.18. **Application logs & monitoring:** Exceptions which are thrown by the application such as a warning or as a validation error should be logged for monitoring and incident management **IG 81**

a. The log generation should adhere to the standard process so that it can be integrated with monitoring and incident management mechanism
b. Enable web server log and transactions log
c. Ensure implementation of web application firewalls
d. Log monitoring at periodic interval
e. Daily log monitoring for application processing secret information
f. Real time monitoring for application processing top secret information
g. Integration of application log monitoring with SIEM solution
h. Application security dashboard

16. Data security

16.1. Background

16.1.1. Increasing complexity of data access due to multiplicity of platforms leads to multiple leakage scenarios while data is being created, accessed and utilized

16.1.2. Network, server systems, endpoints, applications, physical environments, and communication channels are involved in the execution of a data transaction. These elements contribute to the security posture of data

16.1.3. Value associated with data collected by an organization is increasing phenomenally, attracting attention of adversaries and attackers

16.1.4. Security threats are becoming more organized and targeted, reaping immense benefits out of data compromises. This has led to the increasing concentration of these threats at the data layer

16.2. Relevance of domain to information security

16.2.1. Without classification of information, it will be difficult to sensitize services, processes and functions towards importance of information

16.2.2. Secondly, it will misalign measures planned for security. Critical information may not get the desired level of protection

16.2.3. Without labeling of information, criticality of information may not be recognized and may not invoke the corresponding actions for protection

16.2.4. Lack of prior knowledge about potential data leakage scenarios will lead to inadequate threat mitigation measures

16.2.5. There have been increasing instances of cyber espionage, where there have been concentrated and targeted efforts on attacking the data resulting in data breaches, which attracts a high level of media attentions. Organization should ensure that the weaknesses leading to data leakages are addressed in a timely manner

16.3. Data security guidelines

16.3.1. **Information discovery, identification & classification:** The organization must continually ascertain the information being created, accessed, received, processed, stored and shared **G 35**

Identification & classification: Prior to determining security measures, the information to be protected needs to be identified and classified. For information classification norms, refer section 7.1

16.3.2. **Cryptography & encryption:** Ensure that proportionate encryption protection is applied to protect sensitive information **G 36**

16.3.3. **Key management:** The organization must retain control over the encryption keys while allowing efficient and effective encryption operations **G 37**

16.3.4. **Information leakage prevention:** The organization must establish procedures to protect classified information from unauthorized access or unintended disclosure, by identifying possibilities of data breach. Appropriate data backup **G 38**

and data leakage prevention methodologies, to monitor and protect classified information while at rest in storage, in use at endpoint, or in transit with external communications must be implemented

16.3.5. **Information access rights:** The organization must establish appropriate procedures to govern access rights of users to access information systems and assets; establish process for creation of identities; establish process for defining user privileges and devise mechanisms to understand how access to information is provided **G 39**

16.3.6. **Third party access:** The organizations must set up norms for third parties, which will be involved in the processing of information and seek the desired level of assurance from third-parties, for security of information available with them **G 40**

16.3.7. **Monitoring & review:** The organizations must monitor the instances of access of information. Activity logs must be enabled to help in review of information usage and handling **G 41**

16.3.8. **Breach management & corrective action:** The organizations must have proactive measures to identify, notify, remediate and manage breach of information *(refer section 19)* **G 42**

a. Any breach of classified information should be reported to relevant agencies such as CERT-In , NCIIPC and any such agency duly notified by the Government of India

16.4. Data Security Controls

16.4.1. **Data discovery:** The organization must establish a process of discovering information that is created, received, accessed and shared **C 82**

16.4.2. **Data classification:** The organization must enforce the information classification across all processes, functions and operations **C 83**

a. Establish easily accessible data classification guidelines, with proactive contextual help to bring data consciousness in the organization's operations

b. Information labeling should be strictly adhered

c. Integrate information identification and classification in the organization's operational life cycle

d. Automated tool for classification and labeling information

16.4.3. **Cryptography & encryption:** The organization must use encryption techniques to protect the data and enforce confidentiality during transmission and storage. Several methods exist for encryption of files such as encryption feature on external hardware device, secret key encryption, and public key encryption **C 84**

a. SAG (Scientific Analysis Group) approved encryption should be used for secret and top secret classification levels.

16.4.4. **Key management:** Encryption key must be managed securely and governed by a documented key management process. For sensitive networks, Cryptographic keys for the systems must be obtained from Joint Cipher Bureau (JCB) **C 85**

16.4.5. **Data-at-rest:** The organization must implement appropriate capability to protect all data storage including backup files **C 86**

16.4.6. **Data-masking:** The organization must use data masking techniques while provisioning access to application interfaces and providing data for testing **C 87**

16.4.7. **Database management:** The organization must incorporate security considerations in database management and administration. Access to database management should be governed as per organizations policy **C 88**

16.4.8. **Public mail and collaboration tools:** The organization must ensure that access to public mail and collaboration tools such as instant messaging should be restricted **C 89**

16.4.9. **External media and printing devices:** The organization should prohibit use of external media such as USB memory, external HD, mobile storage where classified information is handled **C 90**

a. The organization must enable security feature on printing devices

16.4.10. **Preventing loss of information:** The organization must ensure that the loss of information is prevented **C 91**

16.4.11. **Backup:** The organization must ensure that backup copies should be maintained for all operational data to enable reconstruction should they be inadvertently destroyed or lost **C 92**

16.4.12. **Data retention and disposal:** The organization must implement data retention and disposal policy, considering laws, regulations and guidelines regarding the storage of data: **C 93**

a. Limit data storage for the time required as per applicable policy, law or regulation etc.

b. Deploy/ devise system to delete and purge data beyond that its storage date

c. Classified and personal data must be erased before any ICT asset such as media, computer system and electronic office equipment etc. are to be transferred or disposed

d. Standard Operating Procedure (SOP) regarding transfer and disposal of Information media should be maintained

e. Encryption modules / memory modules / chips having cipher related data in the embedded device, if any, should be removed and destroyed beyond recovery

16.4.13. **Third party access:** Access to third parties systems and persons must be granted and governed by predestinated policies and procedures **C 94**

16.4.14. **Monitoring & review:** The organization must have mechanism to monitor and review access, use and share of information at the predetermined level **C 95**

16.4.15. **Breach management:** The organization must respond to security compromises, incidents and breaches in predicable and responsive manner. **C 96**

16.5. Data security implementation guidelines

16.5.1. **Data discovery:** The organization must deploy a process and techniques for discovering data generated, received, accessed and shared **IG 82**

a. Scanning all projects, processes and functions

b. Scanning all applications, endpoint systems, servers and network storages

c. Scanning connections, emails, and collaboration tools

d. Deployment of data discovery tools

16.5.2. **Data classification:** Ensure classification of data based on its level of criticality and the impact to the organization and on internal and national security of the nation, should that data be disclosed, altered or destroyed without authorization. The organization must enforce the information classification as per Section 7, across all processes, functions and operations. **IG 83**

a. Implement a mechanism that helps identify the information, classify and report it

b. Information without any security classification should also be protected at-least on par with restricted information

16.5.3. **Cryptography and encryption:** The organization must use encryption techniques to protect the data and enforce confidentiality during transmission and storage **IG 84**

a. For data at rest, the organization should use secure encryption methodologies such as AES (128 bits or higher)

b. To avoid data tampering during transmission and to establish authenticity of source or origin of data, cryptographic and hashing algorithms such as SHA -2 should be applied while using digital signature. Passwords that are used for authentication or administration should be hashed or encrypted in storage

c. Passwords that are used for authentication or administration should be hashed or encrypted in storage

d. In cases where the information asset or system is reachable via web interface, web traffic must be transmitted over Secure Sockets Layer (SSL), using only strong security protocols, such as SSLv3, Transport Layer Security (TLS 1.2 or higher)

e. SAG (Scientific Analysis Group) approved encryption algorithms must be used for secret and top secret classification

16.5.4. **Key management:** Ensure key management process is documented and includes key distribution plan which must describe circumstances under which key management components are encrypted or decrypted, their physical form such as electronic, optical disk, paper etc. **IG 85**

a. Central key management function, however the execution should be distributed to ensure to avoid single point of failure

b. It should support multiple encryption standards

c. Centralize user profiles for authentication and access keys. Users must be assigned and issued credentials to provide access to encryption resources

d. Ensure extensive logging of operational instances of key management function Restrict access to cryptographic keys to the fewest number of custodians

e. Keys should be distributed securely

f. Periodic key changes should be implemented at the end of their crypto-period

g. Ensure one key management solution for field, file and database management

h. For sensitive networks, Cryptographic keys for the systems must be obtained from Joint Cipher Bureau (JCB)

i. Ensure to support to third party integration should be restricted for Secret and Top Secret unless it is required

j. Ensure that keys must be stored securely inside cryptographic hardware and encrypted using master key etc.

k. Proper SOP must be placed for outlining Key Management during:

- Day-to-day operations
- Emergency circumstance

l. In the event of key compromise

16.5.5. **Data-at-rest:** The organization must: **IG 86**

a. Implement segmentation to secure access paths to storage containing classified data

b. Enforce strict access control on the file systems of the storage devices in the storage network

c. Data should be protected as it is in active use as well as when it is archived to external storage devices/ media by use of encrypted storage

d. For sensitive data, a suitable a full-disk encryption may be deployed

16.5.6. **Data masking:** Ensure use of data masking techniques such as randomization, blurring, nulling, shuffling, substitution amongst others while provisioning access to data **IG 87**

16.5.7. **Database Management:** The following must be implemented for database management **IG 88**

a. Access to database must be restricted to authorized users

b. Sensitive fields must be encrypted in databases

c. Instances of database accesses must be logged and activities of database administrator must be recorded

d. Database administration credentials must be protected from unauthorized access

e. A mechanism for real time monitoring of databases

16.5.8. **Public mail and collaboration tools:** The following must be implemented for securing public mail and collaboration tools **IG 89**

a. Information systems containing classified information marked top secret

should not be connected with the Internet

b. Public mail such as gmail, yahoo etc. should strictly not be used for official purposes or official communication. Access to public mails from official systems should be prohibited, unless approved the head of the department, for limited personal use.

c. Files and messages transferred from public mails should be monitored using capabilities such as Data Loss Prevention (DLP)

d. Official collaboration tools such as inter office chat facility should prohibit transfer of classified files and data, using such services. Public chat applications/ web portals should be strictly prohibited on official information systems or assets

16.5.9. **External media & printing devices:** **IG 90**

a. External storage media (e.g., USB memory devices/readers, removable hard drives, SD, CompactFlash, flash drives, key drives, rewritable DVDs, and floppy disks) should not be allowed to be connected with official information systems or assets.

b. The organization must implement appropriate detection capability and take necessary corrective action to thwart instances of unauthorized attempts to use such media.

c. All endpoint devices allocated to users must have their USB ports disabled, unless authorized for use by head of department due to operational requirements

d. User authentication such as PIN, smart card, user password for printing information

e. The printing devices must be configured to remove spooled files and other temporary data using a secure overwrite, or device storage for data processing must be encrypted

f. All printing devices must be allocated a static IP address

g. Enable secure network protocols and services (e.g. IPsec or Secure Internet Printing Protocol (IPP)) to prevent unauthorized network interception

16.5.10. **Preventing loss of information**: External storage media used for official purposes should be encrypted prior to use **IG 91**

a. Classified information shall not be stored in privately-owned information processing equipment, mobile devices or removable media, unless authorized by head of department. Top secret or secret information must not be processed in privately-owned computers or mobile devices in any case

b. External connections from information systems and assets should be restricted for information exchange and transmission

c. External connections from information systems and assets should be restricted & monitored for information exchange and transmission

d. Email exchanges should be evaluated to build visibility over what information is leaving the organization

e. Activity on information systems should be monitored for information

exchange and transmission

f. Classified information meant for internal use only, should be prevented from transmission

16.5.11. **Backup:** The backup copies should be taken at regular intervals such that recovery to the most up-to-date state is possible **IG 92**

a. Backup activities must be reviewed and tested for integrity on a periodic basis. Hash signature of the backup data must be maintained to verify the integrity of data at the time of restoration

b. Backup should be properly labelled as per the classification of data stored. Backup labels should also indicate the exact date and time of backup creation as well as the name/type of system from which backup has been created

c. Copies of backup media and records should be stored at safe and secure location where they may be recovered/ reconstructed in case of disaster at the original location

d. Adequate and strong encryption methodology such as AES (256 bit) must be deployed for backup of data at the operations and recovery center

e. Backup media disposal should be in accordance with asset destruction controls

f. Backup may be extracted as per daily schedule, weekly schedule, monthly schedule, quarterly schedule etc. Backup data of atleast the last 5 cycles should be maintained at a minimum

16.5.12. **Data retention & disposal:** Data erasure from storage devices must be done prior to its transfer or destruction from storage devices using secure technologies such as degaussing or overwriting disks and tapes etc. obsolete storage devices must be physically destroyed **IG 93**

a. All media must be checked to ensure secure deletion of information and data prior to transfer or destruction

b. The organizations must ensure that all ICT assets are securely disposed of by authorized users when they are no longer required by physically destroying the ICT assets, to ensure that no information can be retrieved

c. Asset transfer or destruction decisions, and the reasons for taking them, must be documented. Record of all ICT assets transferred or destroyed must be maintained with an officer of appropriate level of authority

d. Periodic audit should be in place to verify the storage media disposal process

e. Obsolete ICT equipment such as laptops, desktops and other computing devices must only be allowed outside the organizations premises post secure deletion of data

f. 2 years retention of data from the levels of top secret to restricted after active use. The retention period is subject to respective regulatory requirements

16.5.13. **Third party access:** Ensure that third party access to information is restricted and governed **IG 94**

a. Block access to third party systems and persona unless it is required

b. Ensure the security provisions are incorporated into the contract

c. Ensure background verification and security clearance of external people before providing the access

d. Establish a mechanism for seeking assurance from third party organizations

e. Restrict access to public emails, writing material and mobile phone in the premises of third party accessing information

16.5.14. Monitoring & review: The organization must deploy a process for monitoring use and access of information **IG 95**

a. Each instance of access to information is logged

b. Access of fields, files and databases is recorded and logged

c. Activity of database monitored

d. Behavior of people and systems access data is closely tracked

e. Logs are reviewed frequently

f. Logs of reviewed on real time basis for sensitive information

g. Integration with SIEM solution

h. Dashboard of data security

16.5.15. **Breach management**: The organization must ensure that each security, incident or breach generates desired level of attention to resolve in a timely manner **IG 96**

a. Mechanism to identify or recognize security incident

b. Define type of incidents and their respective severity

c. Escalation matrix for each type of incident

d. Establish remediation workflow

e. Automated tool and technology for incident management like SIEM

f. Process to notify the breaches to authorities like CERT-In, NCIIPC, etc

17.Personnel security

17.1. Background

17.1.1. Insider threat has been a large contributor towards a number of security incidents faced by organizations. Additionally, the sourcing patterns of an organization are increasingly dependent on external service providers, for bridging gaps in their skills and competence, saving costs, augmenting capabilities to improve scalability and for making operations lean and efficient

17.1.2. However, granting access to organizations information assets and systems to third-party service providers (TPSP's) increases the security risk. As employees and third parties have access to confidential information during their tenure of employment it is crucial that greater emphasis be given to securing threats originating from human resources

17.1.3. The organization may have robust security framework; however, the third party may not have a similar framework, thus placing the information at risk of compromise or theft. The third party may become the weakest link in the security ecosystem of the organization

17.2. Relevance of domain to information security

17.2.1. Personnel are owners, custodian or users of information assets and systems. Lack of data about these personnel, who may be either employees or third parties, will lead to inadequate protection of these assets and systems from a security standpoint

17.2.2. As processes and sub processes continue to be outsourced or managed by third party personnel, it is important to keep track of information and data they have access to. All vendors, third parties, consultants etc. should be contractually liable to implement and follow security best practices for personnel security, understanding the applicable legal and regulatory compliances, assessment of the sensitivity of information and formulation of robust contractual agreements

17.2.3. Without the knowledge over how and what employees access, it will be difficult to assess risk posed to information and IT systems by employee actions

17.2.4. Without training and awareness, employees may not be aware of the security implications of their actions, resulting in unintentional loss

17.2.5. Third party environment and employees may not be sensitive to the specific security requirements of the organization. If coverage of the personnel security does not extend to them, it will be difficult to get the desired level of assurance

17.3. Personnel security guidelines

17.3.1.	**Awareness & training:** The organization must develop an appropriate information security awareness and training program for all personnel. All adequate tools and systems to support such training programs should be made available by the organization	**G 43**
17.3.2.	**Employee verification**: The organization must conduct background checks or security clearance as part of its employee hiring process	**G 44**
17.3.3.	**Authorizing access to third parties:** The organization must develop and document a process for authorizing physical and logical access to third parties	**G 45**

for organization owned information assets and systems

17.3.4. **Record of authorized users:** The organization should maintain an updated record of all users granted access to each information asset and system **G 46**

17.3.5. **Acceptable usage policy:** The organization must develop an acceptable usage policy for all information assets and systems including Web and email resources provided to employees, amongst others **G 47**

17.3.6. **Monitoring and review:** The organization must implement appropriate monitoring tools and technology to track compliance of personnel with organization's policies **G 48**

17.3.7. **Limiting exposure of information:** The organizations must ensure that coverage of personnel security program limits the exposure of information to unintended recipients, parties or organizations **G 49**

17.4. Personnel security controls

17.4.1. **Training and Awareness:** The organization must ensure that role based training is provided to all personnel within the organization to familiarize them with their roles and responsibilities in order to support security requirements. The organization must ensure that information security awareness and training includes the following: **C 97**

a. Purpose of the training or awareness program

b. Reporting any suspected compromises or anomalies

c. Escalation matrix for reporting security incidents

d. Fair usage policy for organizations assets and systems

e. Best practices for the security of accounts

f. Authorization requirements for applications, databases and data

g. Classifying, marking, controlling, storing and sanitizing media

h. Best practices and regulations governing the secure operation and authorized use of systems

17.4.2. **Employee verification:** The organization must ensure appropriate verification such as background checks are performed for employees and personnel of TPSP(s) before providing access to classified information **C 98**

a. The organization must conduct pre-employment verification through authorized/competent agency

17.4.3. **Authorizing access to third parties:** The organization must identify individuals representing third party organizations such as consultants, contractors, or any other individuals who require authorized access to the organizational information and information system **C 99**

a. Access to information and information systems by employees of external / Third Party Service Provider(s) (TPSP) should only be allowed after due verification (which should be repeated after specific intervals), and such access should occur under supervision of relevant authority

b. Under no circumstances shall third party vendors or partner be allowed unmonitored access to the organizations information or information

systems

17.4.4.	**Acceptable use policies:** Ensure that the policies for acceptable use are established for secure usage of organization's resources such as email, internet, systems, networks, applications and files amongst others	**C 100**
17.4.5.	**Disciplinary processes**: Ensure that a mechanism and supporting disciplinary processes are established to resolve non-compliance issues and other variances in a timely manner	**C 101**
17.4.6.	**Record of authorized users:** The organization must prepare and continuously update records of access granted to all users such as employees and third party personnel The record management must be performed in an automated manner to ensure access authorization granted by different functions are maintained in a central repository/ system	**C 102**
17.4.7.	**Monitoring and review:** The organization must define processes to monitor and review access granted to personnel including temporary or emergency access to any information asset or system	**C 103**
17.4.8.	**Non- disclosure agreements:** The organization must incorporate considerations such as signing non-disclosure contracts and agreements in the HR process, both for employees and third parties allowed to access information assets and systems	**C 104**
17.4.9.	**Legal and contractual obligations:** The organization must ensure that employees and third parties are aware of legal and contractual obligations with respect to security of information a. The organization must ensure that users are aware of policies, procedures and guidelines issued with respect to Information Security	**C 105**
17.4.10.	**Communication practices:** The organization must prohibit its employees and external parties from disseminating/ communicating classified information for any other purpose expect its authorized and intended use a. Information regarding security incidents must only be communicated by designated personnel	**C 106**

17.5. Personnel security implementation guidelines

17.5.1. **Training and awareness:** Organization must undertake the development, implementation and evaluation of role-based training for all personnel **IG 97**

a. Impart role-based training to all personnel through specially designed training courses or modules, on a regular basis

b. Emphasize on role of the employees towards information security while designing training courses or modules

c. Organization should work with an IT/cyber security subject matter expert when developing role-based training material and courses

d. Organization must measure effectiveness of role-based training material by means of internal evaluation of attendees

e. Organization must ensure that role-based training material is reviewed periodically and updated when necessary

f. Organization should provide an effective mechanism for feedback on role-based training security material and its presentation

g. Employee awareness on information security: Organization must provide information security awareness training as part of the employee induction process and at regular intervals during the employee's tenure. This must be extended to all third party employees working from the organizations facility

h. Awareness training program should aim to increase user understanding and sensitivity to threats, vulnerabilities

i. Awareness training should focus on the need to protect organization's and personal information

j. Awareness training must cover topics such as security procedures, security policies, incident reporting amongst others

17.5.2. **Employee verification:** Organization must conduct employee verification by using methods such as **IG 98**

a. Perform identity verification through authorized/ competent agency

b. Conduct background checks of all personnel including third party personnel, prior to allowing access to classified information

c. Background verification check should include details such as address verification, criminal records, past experience, medical records, family details amongst others

17.5.3. **Authorizing access to third parties:** The organization must restrict the level of access provided to authorized individuals from third parties based on their role; function performed and associated need for access **IG 99**

a. Prior to granting physical and logical access to third party personnel, the organization must seek sufficient proof of identity of personnel from the third party employer such as recent background check and verification by competent authority

b. Authorization for access to third party personnel must be supported by documented request from head of department, where third party

personnel will be deployed

c. Organization must strictly monitor all activity conducted by third party personnel

d. Organization must strictly monitor physical movement of third party personnel within its facility

e. Organization should permit authorized individuals to use an external information system to access or to process, store, or transmit organization-controlled information only post verification of the implementation of required security controls on the external system as specified in the organization's information security policy

f. Organization must limit the use of organization-controlled portable storage media by authorized individuals on external information systems

17.5.4. **Acceptable use policies:** Organization must identify, document, and implement acceptable usage policy and incorporate the following: **IG 100**

a. All users of information systems must take responsibility for, and accept the duty to actively protect organization's information and information systems

b. The acceptable usage policy must include information about usage of organization ICT resources such as computing equipment, email, optical drives, hard drives, internet, applications, printers, fax machine, storage media amongst others

c. Ensure all employees including third party vendors/consultants/personnel are signatory to the acceptable use policy

17.5.5. **Disciplinary process:** Organization must establish disciplinary process to cater to instances of non-compliance to its security or acceptable usage policy **IG 101**

a. The organization must empower the security team to take disciplinary action whenever instances of non-compliance to the organization's security policy or procedures by any employee or third party personnel are encountered

17.5.6. **Record of authorized users:** Organization must implement a centralized automated access request and authorization capability to establish clear visibility over clearance level granted to each user – including employees and third party personnel. Details about each user must be updated in a timely manner and should include: **IG 102**

a. User details – personal details, contact details, role, function, status of employment

b. Details of background checks and verification

c. Details of HOD

d. List of authorized areas allowed to access

e. Registered/allocated devices and information systems

f. Category of classified information permitted to access

17.5.7. **Monitoring and review:** Organization must implement monitoring mechanism to track user access activity and limit the access to explicitly allowed to **IG 103**

personnel by defining areas visited, time of access, activities conducted etc.

b. The organization must periodically review the physical and logical access granted to personnel to detect instances of non-compliance

17.5.8. **Non-disclosure agreements:** Organization should include signing of non-disclosure contracts and agreements in HR process during employment **IG 104**

a. Non-disclosure agreements should restrict employees and third parties from sharing organizational information publically

17.5.9. **Legal and contractual obligations:** Organization must brief all personnel about their legal and contractual obligation to protect the organizations information and to follow all security advisories issued by competent authority so as to prevent disclosure of information, loss of sensitive data amongst and information compromise **IG 105**

a. The terms of employment must contain a copy of all relevant policies and guidelines

b. The organization must obtain a formal signoff from the employee on all such policies and guidelines such as end user policy, acceptable usage policy etc.

17.5.10. **Communication practices:** Organization must establish, documented and implemented policies, procedures and controls to restrict personnel from unintended communication, both internally and with external entities such as media **IG 106**

a. Communication messages should be circulated to state security requirements or alert employees must be sent by designated personnel only

b. Only official spokesperson/ designated person from organization must be allowed to communicate with media

c. Information/ communication shared with internal or external personnel or entities must be approved by top management

18.Threat and vulnerability management

18.1. Background

18.1.1. Organizations typically deploy security measures to guard against known threats. However, evolving threats add a different set of challenges, which require continuous vigil, monitoring and analysis. The discovery of a new vulnerability, disclosure of a new exploit or emergence of a new malware threat and the capability to incorporate protection from them on a real time basis fall under Threat and Vulnerability Management (TVM)

18.1.2. Keeping the infrastructure security posture up-to-date, scanning the infrastructure for identification of new issues or vulnerabilities that could potentially lead to a security compromise, taking corrective measures in case of a likely compromise, effectively managing infrastructure that inherently is risk prone and delivering a fast response in case of compromise are essential characteristics of the TVM function

18.2. Relevance of domain to information security

18.2.1. ICT Assets (infrastructure and application) are used for creation, processing, transaction, and retention of information. These information assets are vulnerable to attacks because of issues such as configurations gaps or newer vulnerabilities with respect to the infrastructure or unpatched systems, etc.

18.2.2. Compromise of one element of ICT infrastructure may have catastrophic effect jeopardizing security of overall infrastructure and information

18.2.3. ICT infrastructure is increasingly becoming diverse, introducing complexity of dealing with multiple entities and their independencies. This complexity makes managing threats and vulnerabilities a daunting challenge. Information that is stored, transmitted, accessed and processes by these entities will be compromised if their exposure to threats and vulnerabilities are managed effectively

18.2.4. Threat and vulnerability information is diverse in nature reflecting diversity of infrastructure in an organization on the one hand. On the other hand, each element of ICT infrastructure is made up of components sourced from around the globe. Configuration and positioning of these elements and components also contribute to exposure to threats and vulnerabilities. Security of information may be compromised due to vulnerabilities identified in the components and elements of ICT infrastructure. Insecure configuration may lead to serious security breach

18.3. Threat and vulnerability management guidelines

18.3.1. **Interdependence of systems:** The organization must create a high level map of interdependencies of ICT systems such as applications, servers, endpoints, databases, networks etc. **G 50**

18.3.2. **Standardized operating environment:** The organization should attempt to achieve a standardized operating environment **G 51**

a. The diversity in terms of hardware, application platforms, database types, operating environment and their versions must be minimized

18.3.3. **Including TVM in change management:** The change management process for **G 52**

ICT infrastructure and systems should include a stringent threat assessment prior to deployment

18.3.4. **Integration with external intelligence sources:** The organization must identify sources to gather threat and vulnerability intelligence for ICT infrastructure components including externally provisioned systems such as mobile and personally owned devices — **G 53**

18.3.5. **Intelligence gathering:** The organization must develop capability correlate information about ICT infrastructure and systems — **G 54**

a. Capability to correlate logs capturing activity of users

b. Capability to monitor and analyze traffic

c. Capability to scan anomalous behaviors of applications and systems

d. Obtain information from other industry peers

e. Obtain information from security intelligence organizations

18.3.6. **Technical policies:** The organization must define technical policies to guide configuration of ICT systems — **G 55**

18.4. Threat and vulnerability management controls

18.4.1. **Interdependence of systems:** Categorization of ICT systems should be based on lifecycle stages such as development, testing, staging, production and disaster recovery — **C 107**

a. Compatibility of various ICT systems must be analyzed, understood and documented

18.4.2. **Standard operating environment:** — **C 108**

a. The organization must aim to establish standard operating environments for server and endpoint systems

b. The organization must ensure that infrastructure is standardized and homogenous

18.4.3. **Threat assessment:** The organization must conduct periodic assessment of ICT infrastructure for identifying exposure to threats — **C 109**

b. All changes to ICT infrastructure and information systems must be made post thorough threat assessment

c. Changes to ICT infrastructure and information systems

18.4.4. **Integration with external intelligence:** The organization must ensure that vulnerabilities and threat exposures are managed through appropriate agreements, obligations and service level requirements established with all vendors, TPSP(s) and partners — **C 110**

18.4.5. **Vulnerabilities knowledge management:** The organization must ensure that it maintains record of vulnerabilities in existing configurations of systems by tracking and identifying vulnerabilities present in the Operating System (OS), applications, databases, network or endpoints and their impact on information leakage — **C 111**

18.4.6.	**Changing threat ecosystem:** The organization must evaluate all information systems continually to identify exposure to new and unknown vulnerabilities and threats	**C 112**
18.4.7.	**Threats emanated from third parties:** The organization must ensure that vendors, third party providers and partners adopt equivalent threat and vulnerability protection for information transacted, processed and stored on behalf of the organization	**C 113**
18.4.8.	**System hardening**: The organization must define standard operating procedures for system hardening	**C 114**
18.4.9.	**Patch management:** The organization must ensure that the security updates and patches are applied to the information systems as per schedule	**C 115**
18.4.10.	**Malware protection:** The organization must ensure that all information systems are protected with adequate measures to ward off threats from malware	**C 116**
18.4.11.	**Perimeter protection:** Ensure that perimeter security protects the organization from possible exploitation of vulnerabilities	**C 117**
18.4.12.	**Threat protection**: The organization must deploy appropriate capability to protect against attempts to penetrate into systems and traffic scanning	**C 118**
18.4.13.	**Configuration:** The organization must ensure that all the unnecessary services, ports and interfaces in systems, network equipment and endpoints are blocked	**C 119**
18.4.14.	**Remediation:** The organization must establish processes to ensure remediation of threats and vulnerabilities in the least possible time a. Threat and vulnerability management system should integrate with ICT infrastructure management systems for triggering remediation tasks	**C 120**

18.5. Threat and vulnerability management implementation guidelines

18.5.1.	**Interdependence of systems:** a. Replacement of ICT assets with newer/upgraded version must be done keeping in view their backward and forward compatibility with existing infrastructure devices b. Ensure that addition of ICT infrastructure components is made post compatibility analysis of the additional components with existing ICT infrastructure	**IG 107**
18.5.2.	**Standard operating environment:** The organization must ensure standardization of operating environment across the organization. This should include, but not limited to, the following: a. Operating systems b. Servers and platforms c. Limit diversity of endpoints d. Uniform and homogenous network devices e. Application platforms and installed versions	**IG 108**

f. Database types should be uniform

g. Depending the size of the IT assets and to have standard, secure and smooth operating environment, organizations may create Network Operation Center (NOC) and Security Operations Center (SOC)

18.5.3. **Threat assessment:** The organization must identify the possible threat vectors' paths, exploitation points, tools and techniques which can compromise the security of the organization. The organization must also analyze the impact of compromise of security of a device or components to its operations: **IG 109**

a. Perform vulnerability assessment to identify vulnerabilities and weaknesses as a result of specific way of configuring devices and systems; vulnerabilities and threats associated with the use of specific ports, protocols and services; vulnerabilities introduced due to changes in ICT infrastructure

b. Vulnerabilities and threats associated with specific types of infrastructure components

c. Vulnerabilities associated with specific versions of infrastructure components

d. Whenever there is a change in ICT system, new configuration should take care of established identification, authorization and authentication policies

18.5.4. **Integration with external intelligence:** The organization must establish a formal relationship with external entities for receiving timely notification **IG 110**

a. Relevant feeds, information about emerging threats, vulnerabilities, bugs and exploits must be obtained

b. Relevant sources should include a mix of different vendors, trusted third parties, product developers, open source communities, industry bodies and other relevant organizations

c. The organizations risk management function must incorporate inputs received from such external sources and entities

18.5.5. **Vulnerabilities knowledge management:** The organization must document and maintain list of vulnerabilities present in installed instances of operating system, applications, databases, network device, endpoints **IG 111**

a. Specify the level of severity associated with each known vulnerability

b. Ensure availability of security capabilities to protect against all known threats and vulnerabilities

c. Maintain and update vulnerability information and integrate with change management process

d. Integrate information from external intelligence sources

18.5.6. **Changing threat ecosystem:** The organization must evaluate all ICT systems and devices on regular basis to uncover new vulnerabilities **IG 112**

a. Conduct periodic security testing for all ICT systems and devices

b. Conduct ad-hoc security testing for all ICT systems and devices

18.5.7. **Threats emanated from third parties:** The organization must ensure that all third party vendors, agencies, partners with access to the organizations information implement capability to counter emerging threats and address vulnerabilities, as per the organizations requirements **IG 113**

18.5.8. **System hardening:** The organization must aim to establish standard operating environments covering hardware, software and the process of IT assets without comprising the security aspects of the IT assets. The organization must develop a standard procedure for system hardening which includes, but is not limited to the following: **IG 114**

a. Developing standard hardened configuration for implementation across the organization by modification of default security controls, tailored to organizations requirements, eliminating known risks and vulnerabilities

b. Keeping security patches and hot fixes updated Implement encryption on all information systems

c. Establish hardening security policies, such as local policies relating to how often a password should be changed

d. Shut down unused physical interfaces on network devices

e. Use secure protocols when transmitting over the network

f. Implement access lists that allow only those protocols, ports and IP addresses that are required by network users and services, and then deny everything else

g. Restrict remote management connectivity to only controlled machines that are on a separate security domain with robust protection

h. Monitor security bulletins that are applicable to a system's operating system and applications

i. Removal of unnecessary software,

j. Enable system security scanning and activity and event logging mechanism

18.5.9. **Patch management:** The organization must ensure that patch management is carried out at regular intervals or as soon as critical patches for ICT systems or software are available **IG 115**

a. Integrate patch management with operational cycle of ICT infrastructure management such as such as asset management, capacity management, change management, configuration management, problem management and service management

b. The organization must regularly be in touch with vendors and service providers to ensure latest patches are installed on priority basis

18.5.10. **Malware protection:** The organization must ensure that each information system is protected by installation of antivirus software and regular updates are made available to the same **IG 116**

a. Capabilities to protect against specific malware which attempt information theft should be available

18.5.11. **Perimeter threat protection:** The organization must ensure perimeter threat protection of its network infrastructure through implementation of **IG 117**

capabilities such as a firewall

18.5.12. **Protection from fraudulent activity:** The organization must deploy techniques for protection from fraudulent applications such as key loggers, phishing, Identity theft and other rogue applications **IG 118**

18.5.13. **Configuration of endpoints:** The organization must block all unnecessary services and system level administrator privileges through methods such as active directory, group policies on endpoint devices and systems **IG 119**

18.5.14. **Remediation:** The organization must ensure that ICT systems and devices are updated with the latest security patches and virus signature to reduce the chance of being affected by, malicious code or vulnerabilities **IG 120**

a. The organization must prioritize the order of the vulnerabilities identified and treat them based on their impact and severity

b. The organization must pre-test the security updates and patches of the identified vulnerabilities. The organization must apply appropriate patches and perform post-test to confirm the return to desired secure state

c. The organization should deploy patches to the target machines and make sure that patches are only installed on machines where they are required

d. The organization must perform security risk assessment regularly by using capabilities such as vulnerability scanning tools (host-based or network-based) to identify patch inadequacy or potential system misconfiguration

19. Security monitoring and incident management

19.1. Background

19.1.1. Organizations face significant risks of information loss through inappropriate account access and malicious transaction activity etc. which have implication such as information leakage resulting in misuse, financial loss and loss of reputation

19.1.2. Security monitoring and incident response management is a key component of an organization's information security program as it helps build organizational capability to detect, analyze and respond appropriately to an information breach which might emanate from external or internal sources

19.2. Relevance of domain to information security

19.2.1. The success of a security program and the value being delivered by security initiatives lies in the organization's responsiveness to an external attack and its ability to sense and manage an internal data breach

19.2.2. In the operating cycle of an organization, information is exchanged, processed, stored, accessed and shared. There are multiple ways through which the information may be exposed to unintended persons, it may be intentionally or unintentionally lost or external attackers may able to steal information. This requires continuous monitoring of operations to identify likely instances of information loss

19.2.3. Information loss instances lead to serious consequences. An organization has some window of opportunity to curb the losses and reduce the impact. This requires a predictable and responsive incident management

19.2.4. The logs generated by information systems, servers, operating systems, security devices, networks and application systems provide useful information for detection of incidents pertaining to security of information

19.2.5. Disruptive and destructive information security incidents demand a competent monitoring and incident management

19.3. Security monitoring & incident management guidelines

19.3.1. **Incident response coverage:** The organization must develop the monitoring and incident response program such that it addresses the requirements of its extended ecosystem **G 56**

a. The organization must ensure that the scope of security monitoring and incident management is extended to all information emerging from internal as well as external sources such as threats emerging from vendors, partner or third parties

19.3.2. **Breach information:** The organization must build 'incident matrix', particular to its own threat environment, helping it identify possible breach scenarios that can expose or leak information whilst listing down appropriate response procedure **G 57**

a. The incident scenarios should be based on criticality and sensitivity of information, threat ecosystem around the organization

19.3.3.	**Security intelligence information:** The organization must establish capability to monitor and record specific information about vulnerabilities (existing and new) that could affect information, systems & assets	**G 58**
19.3.4.	**Enterprise log management:** The organization must ensure that logs are collected, stored, retained and analyzed for the purpose of identifying compromise or breach	**G 59**
19.3.5.	**Deployment of skilled resources:** The organization must deploy adequate resources and skills for investigation of information security incidents such as building competencies in digital forensics	**G 60**
19.3.6.	**Disciplinary action:** The organization must establish procedures in dealing with individuals involved in or being party to the incidents	**G 61**
19.3.7.	**Structure & responsibility:** The organizations should define and establish roles and responsibilities of all the stakeholders of incident management team, including reporting measures, escalation metrics, SLAs and their contact information	**G 62**
19.3.8.	**Incident management awareness and training:** The organization must conduct educational, awareness and training programs as well as establish mechanism by virtue of which users can play an active role in the discovery and reporting of information security breaches	**G 63**
19.3.9.	**Communication of incidents:** The organization must establish measures for effective communication of incidents along with its impact, steps taken for containment and response measures to all stakeholders including clients and regulators	**G 64**

19.4. Security monitoring & incident management controls

19.4.1.	**Security incident monitoring:** The organization must build capability to monitor activity over information assets and systems that are being used across its ecosystems	**C 121**
19.4.2.	**Incident management:** The organization must define an information security incident management plan which includes process elements such as incident reporting, incident identification and notification, incident metrics based on the type of incidents, procedural aspects and remediation measures, mechanisms for root cause analysis, communication procedures to internal as well as external stakeholders a. The organization must deploy security measures for incident monitoring and protect the system during normal operation as well as to monitor potential security incidents. The level and extent of measures to be deployed should be commensurate with the sensitivity and criticality of the system and the information it contains or processes	**C 122**
19.4.3.	**Incident identification:** Ensure that a set of rules exists that helps to detect, identify, analyze and declare incidents from the information collected from different sources	**C 123**
19.4.4.	**Incident evaluation:** The organization must define polices and processes for logging, monitoring and auditing of all activity logs a. The organization must deploy relevant forensic capability to aid in incident evaluation	**C 124**

19.4.5. **Escalation process:** The organization must create and periodically update an escalation process to address different types of incidents and facilitate coordination amongst various functions and personnel during the lifecycle of the incident **C 125**

19.4.6. **Breach information:** Ensure that knowledge of incidents, and corrective action taken should be compiled in a structured manner. The organizations must record, at a minimum, the following information: **C 126**

a. The time information security incident was discovered

b. The time when incident occurred

c. A description of incident, including the information, asset & system, personnel and locations involved

d. Action taken, resolution imparted and corresponding update in knowledge base

19.4.7. **Configuring devices for logging:** The organization must configure the devices to generate log information required to identify security compromise or breach **C 127**

19.4.8. **Activity logging:** The organization must define a process for collection, management and retention of log information from all information sources **C 128**

a. The scope of generating logs should be extended to all critical systems

19.4.9. **Log information:** Logs must contain, at a minimum the following information: unauthorized update/access, starting/ending date and time of activity, user identification, sign-on and sign-off activity, connection session or terminal, file services such as file copying, search, log successful and unsuccessful log-in attempts, activities of privileged user-IDs, changes to user access rights, details of password changes, modification to software etc. **C 129**

a. The organization must ensure that time consistency is maintained between all log sources through mechanisms such as time stamping and synchronization of servers

19.4.10. **Log information correlation:** Organization should ensure that a process is established for regular review and analysis of logs and log reports **C 130**

19.4.11. **Protecting log information:** Periodic validation of log records, especially on system/application where classified information is processed/stored, must be performed, to check for integrity and completeness of the log records. **C 131**

a. Any irregularities or system/application errors which are suspected to be triggered as a result of security breaches, shall be logged, reported and investigated

b. For sensitive network, all logs should be stored in encrypted form or place tamper proof mechanism for during creation / storing / processing logs

19.4.12. **Deployment of skilled resources:** The organization must deploy personnel with requisite technical skills for timely addressing and managing incidents **C 132**

19.4.13. **Incident reporting:** The organization must ensure that a mechanism exists for employees, partners and other third parties to report incidents **C 133**

a. Incident management should support information breach notification

requirements as well as formal reporting mechanisms

b. Ensure that a significant level of efforts are dedicated towards spreading awareness about incident response process throughout the organization and to partners and other third parties

19.4.14. **Sharing of log information with law enforcement agencies:** The organization must make provisions for sharing log information with law enforcement bodies in a secure manner, through a formal documented process **C 134**

19.4.15. **Communication of incidents:** The organization must ensure that timely communication is done to report the incident to relevant stakeholders such as the Information Security Steering Committee (ISSC), sectorial CERT teams and CERT- In etc. **C 135**

19.5. Security monitoring and incident management implementation guidelines

19.5.1. **Security incident monitoring:** The roles and responsibilities for incident management must be defined by the organization. Necessary tools and capability to enable monitoring must be made available. The following groups, entities form an essential part of the coverage of the organizations monitoring capability: **IG 121**

a. **Users** – their roles, associations and activities over multiple systems and applications, disgruntled employee

b. **Assets** – ownerships, dependency on related applications or business processes and what information is accessed

c. **Applications** – usage of applications, transactions, access points, file systems which holds sensitive information

d. **Networks** – traffic patterns, sessions and protocol management which are used to access the information

e. **Databases** – access patterns, read & updates activity, database queries on information

f. **Data** – access and transactions on the amount of unstructured/ structured data, sensitivity of data such as PII, PHI, financial Information etc

19.5.2. **Incident management:** The organization must establish a security incident response procedure with necessary guidance on the security incident response and handling process. The procedure must be communicated to all employees, management and third party staff located at the organizations facility **IG 122**

a. Organization should establish guidelines for prioritization of information security incidents based on - criticality of information on affected resources (e.g. servers, networks, applications etc.) and potential technical effects of such incidents (e.g. denial of service, information stealing etc.) on usage and access to information

b. Organization should assign a category to each type of information security incident based on its sensitivity for prioritization of incidents, arranging proportionate resources, and defining SLAs for remediation services

c. Organization must define disciplinary action and consequences in-case

employee or authorized third party personnel are responsible for breach or triggering security incident by deliberate action

d. Organization must define liability of third party entity in-case breach or incident originates due to deliberate action of such parties

19.5.3. **Incident identification:** The organization must continuously monitor users, applications, access mechanisms, devices, physical perimeter, and other aspects of its operations to check for disruption in their normal functioning **IG 123**

a. Security capability should seek to detect and/or "prevent" attacks through monitoring activity

b. Establish processes to identify and report intruders leveraging unauthorized access

c. Monitor downloading and installing activity

d. Monitor hosts, network traffic, logs, and access to sensitive data to identify abnormal behavior

e. Detect, seek establishment of unauthorized peer-to-peer networks, or intruder-operated botnet servers

f. The organization must develop guidelines to classify incident based on certain parameters such as identity theft, unauthorized access, and malicious code execution etc. This will aid in classification of incidents and help in identification of most frequent types of incidents

g. Direct all users to report suspicious activity or abnormal system performance

h. Conduct periodic training of all users to acquaint with incident reporting processes

19.5.4. **Incident evaluation:** The organization must focus on developing procedures for incident evaluation such as type of incident, loss of information, access of information, IP address, time, and possible reason for incident, origin of threat etc. **IG 124**

a. Obtain snapshot of the compromised system as soon as suspicious activity is detected. The snapshot of the system may include system log files such as server log, network log, firewall/router log, access log etc., information of active system login or network connection, and corresponding process status

b. Conduct impact assessment of the incident on data and information system involved

c. Segregate and isolate critical information to other media (or other systems) which are separated from the compromised system or network

d. Keep a record of all actions taken during this stage

e. Check any systems associated with the compromised system through shared network-based services or through any trust relationship

f. Isolate the compromised computer or system temporarily to prevent further damage to other interconnected systems, or to prevent the compromised system from being used to launch attack on other

connected systems

g. Remove user access or login to the system

h. Ensure that incidents are reported in timely manner so that fastest possible remedial measures can be taken to reduce further damage to the IT assets

19.5.5. **Escalation processes:** The organization must create and periodically update an escalation process to address different types of incidents and facilitate coordination amongst various functions and personnel during the lifecycle of the incident **IG 125**

a. The escalation procedure must identify and establish points of contact, at various levels of hierarchy, both within the organization and with vendors and third parties responsible for hardware/ software

b. Maintain an updated list containing details of points of contacts from all concerned departments and functions such as technical, legal, operations and maintenance staff, supporting vendors, including the system's hardware or software vendors, application developers, and security consultants etc.

c. Establish procedure for incident notification to be shared with the above identified personnel, based on the type and severity of impact caused by the incident, in a timely manner

d. Every system should have a specific escalation procedure and points of contact which meet their specific operational needs. Specific contact lists should be maintained to handle different kinds of incidents that involve different expertise or management decisions

e. Different persons may be notified at various stages, depending on the damage to or sensitivity of the system. Communication at each stage must be supported by details such as issue at hand, severity level, type of system under attack or compromise, source of incident, estimated time to resolve, resources required amongst others

19.5.6. **Breach information:** The organization must ensure adequate knowledge of incident/ breach is obtained through post incident analysis. **IG 126**

a. Recommendations to thwart similar incidents in the future, possible method of attack, system vulnerabilities or exploits used amongst other information about incidents must be recorded

b. Details such as time of occurrence, affected devices/services, remediation etc. must also be documented

c. Save image of the compromised system for forensic investigation purpose and as evidence for subsequent action

19.5.7. **Configuring devices for logging:** The organization must establish logging policies on all ICT systems and devices including security devices such as firewalls etc., by enabling syslog, event manager amongst others **IG 127**

a. The organization must capture and retain logs generated by activity on information assets and systems

b. The organization should subscribe to knowledge sources and correlate the information to generate intelligence out of various events and

instances

19.5.8. **Activity logging:** The organization must define a process for collection, management and retention of log information from all information sources **IG 128**

a. Logs should be securely managed in accordance to the organizations requirements and should focus on securing process for log generation, limiting access to log files, securing transfer of log information and securing logs in storage

b. Organization should integrate the log architecture with packaged applications or/and customized systems. There should be standardized log formats of unsupported event sources which may lead to information security incidents

c. Log archival, retention and disposal measures should be deployed as per the compliance requirements of the organization

19.5.9. **Log Information:** Ensure that system logs contain information capture including all the key events, activity, transactions such as: **IG 129**

a. Individual user accesses;

b. Rejected systems, applications, file and data accesses;

c. Attempts and other failed actions;

d. Privileged, administrative or root accesses;

e. Use of identification and authentication mechanisms;

f. Remote and wireless accesses;

g. Changes to system or application configurations;

h. Changes to access rights;

i. Use of system utilities;

j. Activation or deactivation of security systems;

k. Transfer of classified information

l. Deletion and modification of classified information

m. System crashes

n. Unexpected large deviation on system clock

o. Unusual deviation from typical network traffic flows

p. Creation or deletion of unexpected user accounts

q. Unusual time of usage

r. A suspicious last time login or usage of a user account

s. Unusual usage patterns (e.g. programs are being compiled in the account of a user who is not involved in programming)

t. Computer system becomes inaccessible without explanation

u. Unexpected modification to file size or date, especially for system executable files

v. All log generation sources such as information systems and critical

devices must be synchronized with a trusted time server periodically (at least once per month)

19.5.10. **Log information correlation:** The organization must schedule a periodic log review process for examination of any attempted system breaches, failed login attempts amongst others **IG 130**

a. The organization must undertake regular review of log records on systems/ applications where classified information is stored or processed to identify unauthorized access, modification of records, unauthorized use of information, system errors and security events, unauthorized execution of applications and programs, in addition to review of changes to standard configuration of systems storing or processing classified information

b. Appropriate capabilities must be implement to check for modification of information ownership and permission settings

c. Appropriate capabilities such as intrusion detection system (IDS) or intrusion prevention system (IPS) should be implemented to analyze log information to detect Intrusion, malicious or abusive activity inside the network, verification of integrity of classified information and important files

19.5.11. **Protecting log information:** Periodic validation of log records, especially on system/application where classified information is processed/stored, must be performed, to check for integrity and completeness of the log records **IG 131**

a. Access to system and device logs must be restricted only to ICT personnel through administrative policies and other measures

b. Logs must be retained for adequate period of time considering organizational, regulatory and audit requirements

c. Log information must be securely archived and stored in secure devices and placed under the supervision of concerned Information security personnel

d. Log information, beyond its intended period of retention, must be disposed as per standard data disposal policy

e. Log information of all administrative and privilege accounts activity must also be maintained

f. Log information must be protected from modification or unauthorized access

19.5.12. **Deployment of skilled resources:** The organization must define the resources and management support needed to effectively maintain and mature an incident response capability **IG 132**

a. Individuals conducting incident analyses must have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications

b. The organization must trains personnel in their incident response roles and responsibilities with respect to the information system

c. The organization should incorporate simulated events into incident response training to facilitate effective response by personnel in crisis

situations

d. The organization should develop competencies in cyber forensics and investigations or seek support from authorized cyber investigation agencies

19.5.13. **Incident reporting:** The organization must ensure that appropriate procedures are followed to enable reporting of incidents both by employees and partner agencies **IG 133**

a. The reporting procedure should have clearly identified point of contact, and should have easy to comprehend steps for personnel to follow

b. The reporting procedure should be published to all concerned staff for their information and reference

c. Ensure all employees and partner agencies are familiar with the reporting procedure and are capable of reporting security incident instantly

d. Prepare a standardized security incident reporting form to aid in collection of information

19.5.14. **Sharing of log information with law enforcement agencies:** The organization must make provisions to share log information with law enforcement agencies such as police on receiving formal written notice or court orders. **IG 134**

19.5.15. **Communication of Incidents:** The organization must ensure that apart from addressing an incident, the information about its occurrence should be shared with relevant stakeholders such as the Information Security Steering committee (ISSC), sectorial CERT teams and CERT- In, service providers and partner vendors and agencies etc. **IG 135**

Guidelines for technology specific ICT deployment

20. Cloud computing

20.1. Background

20.1.1. Essentially, cloud computing offers a new way of delivering traditional ICT services to an organization, by combining platforms, operating systems, storage elements, databases and other ICT equipment

20.1.2. While, the security guidelines and controls described above will be useful for the cloud service provider, to establish a security baseline, specific guidance has also been provided. Each organization has a different level of risk appetite

20.1.3. Due to the cloud deployment models and the technology currently in use to offer these services, certain risks become significant. Thus, as an organization embraces cloud services, the cloud security architecture should be aligned with the organizations security principles

20.1.4. The overall security architecture of the cloud service provider should at a minimum, follow the guidelines mentioned below. A comprehensive set of controls and advanced security measures should essentially form a part of the agreement between the cloud service customer and cloud service provider

20.1.5. The organization must also evaluate the potential impacts of storing data in different physical locations, as well as in a shared environment collocated with data from other organizations. The security measures incorporated should ensure coverage of all risks identified

20.2. Cloud computing management guidelines

20.2.1. **Security considerations in contract:** The organization must define a Service Level Agreement (SLA) with the cloud service provider incorporating aspects of data confidentiality, integrity, availability and privacy **G 65**

a. In-case any part of the cloud service is further outsourced by the contracted cloud service provider, the organization must ensure that the agreed SLA is adhered to by such vendors

20.2.2. **Alignment of security policies:** The organization must ensure that the security policy of the cloud service provider is aligned with the organizations evaluation and assessment of information security risks **G 66**

a. The organization must ensure that the cloud service provider classifies information and associated virtualized assets based on the information classification guidelines used by the organization

b. The organization must ensure that access to information over the cloud environment is restricted in accordance with its access control policy

20.2.3. **Data security in cloud environment:** The organization must ensure that security of applications in cloud environment is equivalent to or exceeds the security implemented for application in local environment **G 67**

20.2.4. **Authentication in cloud environment:** The organization should ensure that logical access authentication is performed using appropriate capabilities **G 68**

basis well defined authorization parameters

20.2.5. **Continuity of operations:** The organization must ensure that disaster recovery plan and business contingency plan is developed in consultation with the cloud service provider **G 69**

20.2.6. **Definition of roles and responsibilities:** The organization must ensure that the cloud service provider clearly defines the roles and job duties of its employees, especially if the cloud service provider provides services to multiple organizations **G 70**

20.2.7. **Security monitoring:** The organization must ensure that the cloud service provider develops appropriate mechanism to monitor; report and remediate security incidents. Security monitoring in the cloud should be integrated with existing security monitoring capabilities available with the organization **G 71**

20.2.8. **Availability of logs**: The organization must ensure that logs containing information about all operational activities, access events, modification of information, security events etc. are made available by the cloud services provider **G 72**

20.2.9. **Third party security assessments:** The organization should ensure that third party assessments are performed at least annually, or at planned intervals to measure compliance with organizations security policies, procedures, including contractual, statutory, or regulatory obligations **G 73**

20.2.10. **Data security:** The organization should implement appropriate data masking and encryption based on classification of data transferred to the cloud **G 74**

a. The organization should ensure that data is protected through appropriate encryption while in transit and at rest in cloud environment

b. The cryptographic keys must be managed in a secure manner and be available with only the least possible number of authorized personnel

c. The cryptographic keys must be stored at the least possible number of locations

20.2.11. **Use of authorized cloud services:** The organization should ensure that its personnel use services of authorized cloud service providers only **G 75**

20.3. Cloud computing implementation guidelines

20.3.1. **Security considerations in contract:** The organization must ensure that service providers are bound by contract for maintaining confidentiality, integrity, availability and privacy of the organizations data **IG 136**

a. Contract with cloud service provider must include requirements to notify the concerned organization as soon as possible in the event of an actual or suspected breach of data

b. The cloud service provider should be signatory to a stringent non-disclosure agreement

c. The organization must retain the right to conduct/ call for audits including audits from third parties, to verify the existence and effectiveness of security controls specified in the SLA

d. Logs and reports including audit logs, activity reports, system configurations reports etc. must be stored and retained as per SLA

20.3.2. **Alignment of security policies:** The organization must ensure that security policy of cloud service provider is aligned with organization's security policies and procedures **IG 137**

a. The CSP must share updated process documentation, configuration standards, training records, incident response plans, etc. with the organization

b. Compliance certificates and reports should be requested from cloud service providers for verification of security practices of the cloud service provider

20.3.3. **Data security in cloud environment:** The organization must conduct a comprehensive security assessment on applications in the cloud environment prior to production from the same **IG 138**

a. All changes in the form of upgrades, patches or enhancements must be followed by comprehensive security assessment, prior to live deployment

b. Third party assessments of CSP should be conducted on a periodic basis

c. In case of a multi-tenant cloud environment, adequate physical security measures in a cloud data center must be implemented to protect against trespassing activities to the computing resources at the physical layer

d. The organization must establish requirements to prevent sharing equipment or equipment racks with application systems of other organizations or application owners considering the sensitivity of data or other security requirements

e. An isolated area or equivalent measures should be provided by the CSP to segregate the organizations data and resources from other tenants

20.3.4. **Authentication in cloud environment:** The organization must ensure that authentication and authorization on logical access control is clearly defined, such as who should be granted with the rights to access the data, what their access rights are, and under what conditions these access rights are provided. **IG 139**

20.3.5. **Continuity of operations:** The operational contingency plan of the organization must include measures to migrate data to another service provider along with the secure deletion of data from the previous vendor, should the need arise **IG 140**

20.3.6. **Definition of roles and responsibilities:** Cloud service providers should define robust segregation of job roles and responsibilities **IG 141**

a. Employees of the cloud service provider, including all contractual staff must undergo routine role based training as well as training on security awareness

b. Employees of the CSP, including all contractual staff employed by the CSP must be signatory to a stringent non-disclosure agreement

20.3.7. **Security Monitoring:** The organization must ensure that cloud service provider performs security monitoring of the cloud environment on a continuous basis. **IG 142**

a. The CSP must communicate its incident management procedure to the organization for formal agreement

20.3.8. **Availability of logs:** The organization must define the type of activity and event logs that the CSP must provide. The organization must ensure that CSP continuously logs information about all maintenance activity, user and administrative access, critical system changes amongst others. CSP must also provide such logs to the organization as and when requested **IG 143**

(For indicative list of logs refer section 19)

20.3.9. **Third party security assessments:** The organization must ensure that CSP periodically undergoes third party security assessments to assess compliance with organization's policies, procedures, encryption standards, authentication standards etc. **IG 144**

a. The CSP must provide reports of third party security assessment to the organization on a periodic basis

20.3.10. **Data security in cloud:** Classified data should be protected through encryption both at rest and in transit in a cloud environment. The cryptographic keys should be managed and protected securely. **IG 145**

a. The organization must ensure that service provider implements strong data-level encryption such as AES (256 bit) on all classified data stored in the cloud

b. The organization should implement VPN protocols such as SSH, SSL and IPSEC to secure data in transit

20.3.11. **Use of authorized cloud services:** The organization must ensure that it procures services from authorized service providers such as those recognised by the Government of India **IG 146**

21.Mobility & BYOD

21.1. Background

21.1.1. Mobility platforms allow organizations to extend access to operational information to employees on the move and from outside the physical perimeter of the organization. Such information may be accessed by employees either on device issued by the organization of on their personal devices

21.1.2. Mobile devices such as smartphones, tablets, laptops etc. are capable of storing and processing information; however, their physical location is not fixed. They also have the ability to connect to various wired of wireless networks via technologies such as GPRS, 3G, Wi-Fi etc. and form connections with other devices via technologies such as Bluetooth, Near Field Communication (NFC), Infrared (IR) etc.

21.1.3. Data on mobile devices introduces significant risks to an organization by introducing several security risks. As mobile devices possess network connection capabilities, they can be exploited to connect to the organizations internal networks and can become a point to breach security

21.1.4. Mobile devices are inherently prone to physical security risks leading to loss of sensitive information such as disclosure of classified information. They may further be exploited for spreading computer viruses and malicious codes into the organizations internal network

21.1.5. Thus, safeguards need to be put into place to ensure the authenticity of both user and device seeking access to information from outside its physical boundary, as well as to protect information contained on devices being carried out of the physical perimeter of the organization

21.2. Mobility and BYOD management guidelines

21.2.1. **Mobile device policy:** The organization should define a mobile device policy to include, at a minimum the following parameters: **G 76**

a. Types of approved mobile devices and the approval mechanism: The organization must evaluate all existing and newer mobile devices to assess their security capabilities and vulnerabilities and notify a list of safe devices which employees are allowed to use for official purposes

b. The data classification permitted on each type of mobile device must be defined. The following classes or types of data are not suitable for BYOD and should not be permitted on personal devices - data classified as “SECRET” or above; other highly valuable or sensitive data which is likely to be classified as “SECRET” or above;

c. Device on-boarding and deprovisioning requirements must be developed to enable standardized approach for allowing and removal of devices.

d. The organization should reserve the right to control its data, including the right to backup, retrieve, modify, determine access and/or delete the organizations data without prior notice to the user. In lieu of authorization to user for provisioning of personally owned device for accessing the organizations data, the organization must obtain consent to perform the above mentioned tasks during the device on-boarding

21.2.2. **Risk evaluation of devices:** The organization must conduct a thorough risk evaluation and testing of existing and newer mobile devices and devise a program to continuously monitor and discover vulnerabilities associated with such devices **G 77**

21.2.3. **Allocation of mobile devices:** The organization should define processes for assignment of mobile devices to users, controlling inventory of devices and device de-provisioning **G 78**

a. For user owned devices, the organization should ensure that all such devices are registered

b. All user owned devices must be configured as per the organizations mobile device policy

c. All recommended security measures must be enforced on user owned devices, if they are to be used to access the organization owned information

21.2.4. **Device lifecycle management and governance:** The organization must define, enforce and monitor policies related to device on-boarding, configuration, update and governance considering the security of information contained in mobile devices. **G 79**

a. Devices must be configured with a secure password that complies with organization's password policy. This password must not be the same as any other credentials used within the organization

b. Users should be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the organization's email system

21.2.5. **Data transmission and storage**: Any authorized personal device used to access, store or process classified information must encrypt data transferred over the network by using appropriate SSL or VPN. The personal device must be configured to store the organizations data on separate encrypted storage media or partition, whatever storage technology is used (e.g. hard disk, solid-state drive, CD/DVD, USB/flash memory stick, etc.) **G 80**

21.2.6. **Awareness:** The organization should provide necessary security awareness training to employees prior to allocating mobile devices or permitting user owned devices to be used, for work related matters **G 81**

21.3. Mobility and BYOD implementation guidelines

21.3.1. **Mobile device policy:** The organization must ensure that proper documents pertaining to provisioning and de-provisioning of employee owned/ organization owned mobile devices are maintained such as employee name, department, mobile device serial number, model number, approval authority for data access on mobile device etc. **IG 147**

a. The organization must define a usage policy for mobile device to meet the business needs of the organization which includes information such as:

b. The types of approved corporate owned mobile devices and the approval mechanism for employee owned devices

c. The data classification permitted on each type of mobile device. Classified information must not be stored in employee owned mobile devices.

d. The control mechanism that would be implemented to comply with the security requirements basis data classification

e. The procedures to ensure timely sanitization of classified data stored in the mobile devices when staff posts out or ceases to provide services to the organization

f. The organization must ensure that mobile devices which are authorized to access the organizations network, use the latest, upgraded and most recent stable operating systems and platform

g. Ensure that jail-broken or devices having any customized software/firmware installed which is designed to grant access to functionality which is not intended to be exposed to the user, are not permitted into the network

h. Mobile devices must not be allowed to be connected directly to the internal corporate network and must be granted access by deploying connection authentication mechanisms

i. Devices must be kept up to date with manufacturer or network provided patches

21.3.2. **Risk evaluation of devices:** The organization must ensure that a proper security check of mobile device is performed prior to admitting them into the organization's network **IG 148**

a. The organization must perform security testing and assessment of the existing mobile devices at regular intervals to scan for any security vulnerabilities, uninstalled patches, unnecessary services etc.

21.3.3. **Device lifecycle management & governance:** The organization must enforce and monitor policies on mobile devices, through the use of mobile device management capabilities. **IG 149**

a. All mobile devices must have security controls to prevent unauthorized access. Measures such as device access password, inactivity timeout, storage encryption, device lockout on failed login attempts, secure deletion of data through remote wipe on device theft or loss etc. must be enforced on all mobile devices

b. A secure encrypted storage space/container must be created on all mobile devices. Organizations data must only be stored in this secure container. Access to the container should only be granted to applications installed by the organization. All third party application must be prevented from accessing this storage area

c. Install and manage protective software (e.g. anti-malware system or firewall) to protect the devices from malicious websites or from attacks coming over other communications channels such as Short Message Service (SMS)

d. Disable unnecessary hardware components such as the camera, Wi-Fi, Bluetooth, GPS, and restrict the use of external storage media (e.g. SD cards)

e. Ensure secure deletion of organizations data on device de-provisioning or as user completes tenure with the organization

21.3.4. **Data transmission & storage:** These may include components such as: **IG 150**

a. Mobile devices must store all user-saved passwords if any, in an encrypted password application

b. Configuring devices based on users role and access authorization, thereby limiting the privileges over modification of device configuration

c. Configuring devices to authenticate users access to applications post two factor authentication

d. Installation of security features and applications such as firewall, endpoint protection, device storage encryption etc.

e. Disabling hardware components such as the camera, Wi-Fi, Bluetooth, infrared (IR) ports, Bluetooth GPS, and restricting use of external storage media such as SD cards

f. Device network connection management to restrict access to unsecure public networks on devices containing classified information

g. Installation of capabilities to securely remove and delete organizations data contained on mobile device

h. Installation and usage of third party applications on mobile devices may be restricted. Access to third party application stores may be limited

i. Implementing storage separation to segregate official and personal data

j. Synchronization of official data contained on mobile device with organization owned backup server

k. Installation of capabilities to ensure official data is not shared/ transmitted from mobile device using unauthorized commercial/ third-party applications including online storage and cloud services

21.3.5. **Awareness:** Adequate training must be imparted to personnel using mobile devices. Training should include aspects such as usage of mobile device, maintaining confidentiality of data, identifying phishing or other fraudulent activity **IG 151**

22. Virtualization

22.1. Background

22.1.1. Virtualization allows the creation of virtual versions of an ICT asset or resource such as desktop, a server, a storage device or other network resources. Devices, applications and human users are able to interact with virtual resource as if it forms a real logical resource. One or more combination of several Virtual Machines (VMs) may be used for ICT operations. Various forms of virtualization exist such as server virtualization, desktop virtualization, application virtualization and operating system virtualization etc.

22.1.2. The virtual machines are managed by a virtual machine manager also known as the hypervisor. A hypervisor manages various VMs on a physical machine and controls the flow of instructions between a Virtual Machine and the underlying physical infrastructure such as CPU, Storage disk etc. A hypervisor may either run directly on the hardware, or as an application on top of an existing operating system referred to as the host OS. The VM running on top of the host operating system (host OS) is known as the guest operating system (guest OS)

22.1.3. Virtualization presents organizations with tremendous opportunities, as well as some significant security challenges. It provides the basis for the convergence of mobile and cloud computing, allowing organizations to consolidate resources, improve responsiveness and become agile in a cost effective manner. However, such consolidation of physical infrastructure and the creation of hybrid environments lead to the emergence of new types of risks for the organization. A virtualization platform must be able to securely segregate multiple workloads consolidated from mixed trust zones and host them from a single pool of shared system resources

22.1.4. Organizations should undertake an assessment of security risks and evaluate the risks associated with operating an ICT component in a non-virtualized environment compared with those in a virtual environment. The security of a virtualized environment largely depends on the individual security of each component, from the hypervisor and host OS to the VMs, applications and storage. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls. Organization should deploy virtualization with a complete view of its benefits and risks, and a comprehensive, defined set of effective system, application and data

22.2. Virtualization management guidelines

22.2.1. **Evaluate risks associated with virtual technologies**: Organization should carefully and thoroughly evaluate the risks associated with virtualizing system **G 82**

a. **Evaluate and address risk**: Organization must carry out risk assessment that should identify whether any additional measures are necessary to secure and protect information in a virtualized environment

22.2.2. **Strengthen physical access**: Organization should implement appropriate capabilities for safeguarding physical access to virtualized environments **G 83**

a. **Access restriction**: Organization should ensure that all unused physical interfaces are disabled, and that physical or console-level access is

restricted and monitored

b. **Secure access**: Organization should implement methods for securing administrative access

c. **Implementation of access controls**: Organization should ensure that appropriate role-based access controls are in place that prevent unnecessary access to resources and enforce separation of duties

22.2.3. **Segregation of virtual traffic:** the organization should segregate traffic generated by virtual assets from physical IT assets traffic and identify open ports in virtualized environment that can be used to establish insecure connections **G 84**

a. Appropriate capabilities should be implemented to segregate, track and monitor traffic originating from virtualized assets

22.2.4. **Implement defense in depth:** Organization should implement well-defined and documented policies, processes, and procedures that are understood and followed by concerned personnel **G 85**

a. **Enforce least privilege and separation of duties**: Organization should control access to the virtualization management console such as hypervisor

b. The organization should provision security policies and trust zones during virtual machine installation

c. The VMs processing classified information should be subjected to all security measures defined as reasonable and appropriate for classified information

d. **Segmentation**: The organization should implement appropriate segmentation scheme to limit traffic between partitions thereby preventing unwanted traffic from passing through a compromised VM to other VMs on the same host

22.2.5. **Harden the virtualization management console:** Organization should deploy hypervisor platforms in a secure manner according to industry-accepted best practices **G 86**

a. **Robust testing:** Organization should ensure that the security of the virtualization management console such as hypervisor has been thoroughly tested prior to deployment

b. **Limiting access level:** Organization should separate administrative functions such that hypervisor administrators do not have the ability to modify, delete, or disable hypervisor audit logs

c. **Separating environment:** Organization should have zones and gateways that typically include multiple independent subnets (physical or VLAN) which are isolated

d. **Malware protection:** organization should implement appropriate malware protection capabilities for virtual assets

22.2.6. **Vulnerability information:** The organization should develop capabilities to gather intelligence on reported vulnerabilities of virtual assets. Additionally, efforts must be made to liaison with agencies which can offer information **G 87**

about newly discovered vulnerabilities and risks

a. **Patching:** Organization should ensure deployment of patches and other mitigating measures as and when new security vulnerabilities are discovered

22.2.7. **Logging and monitoring:** Organization should ensure appropriate mechanism for integrating virtual environments with the organizations log management and monitoring processes **G 88**

a. **Log generation:** Organization should define procedures to generate and send logs to physically separate, secured storage in real-time

b. **Monitoring logs:** Organization should monitor logs to identify activities that could indicate a breach in the integrity of segmentation, security controls, or communication channels between workloads

c. **Time synchronization:** Virtual assets must be synchronized with the same time as physical assets using an organization wide standard time service, to aid correlation of log information for incident evaluation and forensics

22.3. Virtualization implementation guidelines

22.3.1. **Evaluate risks associated with virtual technologies**: **IG 152**

a. **Proper documentation**: Organization should accurately document flow and storage of data to ensure that all risk areas are identified and appropriately mitigated

b. The organization must conduct periodic risk assessment to determine security risks arising out of data compromise, unauthorized access, virtual machine (VM) cloning, unexpected server behavior, lack of support, lack of separation of duties, dormant virtual machines, information leakage, limited functionality amongst others

22.3.2. **Strengthen physical access:** The organization must ensure that all physical entry points to virtualized environments are continuously monitored such as by deploying guards, CCTV, biometric access etc. **IG 153**

a. Administrative access to the virtualized environments should be secured appropriately such as by implementing two step authentication or establishing dual or split-control of administrative passwords between multiple administrators

22.3.3. **Segregation of virtual traffic:** The organization must segregate traffic of virtualized environments from rest of the network traffic in the organization by using separate switches, routers, virtual LANs etc. **IG 154**

22.3.4. **Implement defense-in-depth:** The organization must implement firewalls within virtual machines operating systems or in trust zones or before each virtual Network Interface Card (NIC) etc. **IG 155**

a. The organization must implement role based access controls such as by active directory, group policy amongst others

b. The organization must segment virtualized partitions such as by using VLANs configured in a virtual switch and VLAN access control lists (VACLs)

c. The organization must segregate VM's and create security zones by type

of usage (e.g. desktop vs server), development phase (e.g. development, testing and production), and sensitivity of data (e.g. classified data vs unclassified data)

d. The organization must test patches available for new vulnerabilities in a test environment and replicate to virtual environment only if such tests are successful

22.3.5. **Harden virtualization management console:** The organization must harden the virtualization management console by following, at a minimum, the following **IG 156**

a. Use directory services for user and group authentication

b. Restrict root access via ssh

c. Prevent MAC address spoofing in virtualized environments

d. Configure NTP for time synchronization for logs

e. Maintain file system integrity for incident response and regulatory compliance by monitoring critical files that should be monitored for changes and accidental deletion or corruption

f. Disable copy/paste to remote console/location

g. Disable unnecessary devices within virtual machines

h. Prevent connection and removal of devices from virtual machines

i. Prevent use of any default self-signed certificates for SSL communication

j. Use vulnerability management tools to regularly scan the host OS and VMs for vulnerabilities

22.3.6. **Vulnerability information:** The organization must keep a track of new vulnerabilities for operating systems or applications contained in virtual environments, through trusted National Vulnerability Database, notifications from CERT-In etc. **IG 157**

22.3.7. **Logging and monitoring:** The organization must log activities for privilege accounts of hypervisor and VM. Security logs should include events such as access to VM images and snapshots, changes to user access rights, modifications of file permission **IG 158**

a. Organization should regularly analyze and monitor logs for any suspicious activity such as unauthorized access attempts, multiple failed login attempts, system lockout, critical file changes etc.

23. Social media

23.1. Background

23.1.1. Social media and networks offer users the opportunity to participate in discussions, create and follow blogs, share multimedia files etc.

23.1.2. However, such information on social media or social networks is often a source of compromise of sensitive information which may be detrimental to the Internal or national security of India.

23.1.3. Social media is often used by personnel to discuss professional issues or share information about their organization, nature of work, deployment etc. This not only leads to unnecessary disclosure of sensitive information but also exposes vital and strategic information.

23.1.4. Cyber-criminals use advanced techniques to gather intelligence from such public forums and communities. Such information enables them to mount cyberattacks by impersonation, spoofing or other social engineering attacks.

23.1.5. Additionally, attacks from malware, viruses or malicious script are easily spread across social media or social networks and similar applications

23.2. Social media management guidelines

23.2.1. **Limit exposure of official information:** All personnel including employees, contractual staff, consultants, partners, third party staff etc., who manage, operate or support information systems, facilities, communications networks and information created, accessed, stored and processed by or on behalf of the Government of India; **G 89**

a. Must be prohibited from accessing social media on all official devices, including personal devices with access to official information.

b. must be contractually bound against disclosure of official information on social media or social networking portals or applications

c. must undergo mandatory training to educate them on perils and threats in the virtual world such as phishing emails, suspicious code in page etc. and for following best practices for practicing safe online behavior

23.2.2. **Permitted official use** : Only the designated function authorized to communicate unclassified information on public forums may be permitted the use of social media or social networking portals and applications **G 90**

23.3. Social media implementation guidelines

23.3.1. **Limit exposure of official information**: The organization must use methods to restrict access to social media websites in the organization environment and on organization's devices such as by enforcing policies through administrative directory, group policy tools etc. **IG 159**

a. Third party applications must not be integrated with official websites, unless the same has undergone extensive security tested by the organization

23.3.2. **Permitted official use:** The organization must permit only authorized **IG 160**

personnel in public communication function or similar in the organization to use social media through policy enforcement in administrative directory, group policy etc.

a. **Training and awareness:** Organization should impart necessary training to all personnel on do's and don'ts of social media and threats associated such as education on phishing emails, web pages, social engineering etc

b. **Authorizing personnel for official communication:** All personnel in the organization must be bound contractually to refrain from speaking on behalf of the organization, not to share internal information, refrain from commenting on organization's performance/projects, not to cite stakeholders while posting any material on social media, blogs, applications amongst others

Guidelines for essential security practices

24. Security testing

24.1. Background

24.1.1. Security testing is the process of determining how effectively an entity being assessed meets specific security objectives. The process is intended to reveal flaws in the security mechanisms of an information system that protects data and maintain functionality as intended. Organizations conduct focused security testing with vulnerability assessment to discover and identify security vulnerabilities followed by penetration testing to simulate an attack by a malicious party and involves exploitation of found vulnerabilities to gain further access

24.1.2. Security testing uncovers the current state of security in the organization to safeguard three main objectives of confidentiality, availability and integrity. It helps organizations to strengthen the security by mitigating and addressing all the vulnerabilities and weaknesses found as a result of the exercise. This further enhances organization's defenses against the exploitation of vulnerabilities by the attackers

24.1.3. In the absence of appropriate security testing, present vulnerabilities may go unaddressed and exploitation by attackers may incur huge reputational and financial losses to the organization.

24.2. Security testing management guidelines

24.2.1. **Security evaluation**: Organization should deploy appropriate capabilities to evaluate all systems, applications, networks, policies, procedures and technology platforms such as cloud computing, mobility platforms, virtual environments etc. to identify vulnerabilities — **G 91**

24.2.2. **Testing scenarios**: Organization should perform security evaluation by constructing scenarios combining internal and external threat agents — **G 92**

24.2.3. **Overt and covert testing**: Organizations should perform both white hat and black hat testing to examine damage or estimate impact by an adversary — **G 93**

24.2.4. **Vulnerability existence**: Organization should deploy appropriate techniques which corroborate the existence of vulnerabilities — **G 94**

24.3. Security testing implementation guidelines

24.3.1. **Security evaluation**: The organization must ensure that relevant capabilities, tools and techniques are deployed for security evaluation such as use of network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security examination — **IG 161**

a. **Security compliance evaluation**: Organization should deploy appropriate capabilities to evaluate all systems, applications, networks etc. and technology platforms such as cloud computing, mobility platforms, virtual environments etc. to check for compliance with security policies

24.3.2. **Testing Scenarios:** — **IG 162**

a. **Internal testing**: The organization must conduct internal security testing assuming the identity of a trusted insider or an attacker who has

penetrated the perimeter defenses

b. **External testing**: The organization must conduct external security testing from outside the organization's security perimeter with techniques such as reconnaissance, enumeration

24.3.3. **Overt and covert testing:** **IG 163**

a. **Black hat testing:** The **o**rganization must conduct black hat testing assuming an approach followed by an adversary, by performing testing without the knowledge of the organization's IT staff but with the full knowledge and permission of CISO/ Senior management

b. **White hat testing:** The **o**rganization must perform white hat testing with the knowledge and consent of the organization's IT staff

24.3.4. **Vulnerability existence:** Security testing and assessment tools should be used to corroborate the existence of vulnerabilities which includes a list of products & affected version, technical details, typical consequences of exploitation, current exploitation status and overall measure of severity etc. **IG 164**

25. Security auditing

25.1. Background

25.1.1. The ability of an organizations security architecture to provide assurance over its security coverage is important in order understand effectiveness of measures and capabilities implemented to counter threats and risks which may jeopardize the operations of an organization

25.1.2. Security auditing is essential to test the effectiveness of design, implementation and operation of security countermeasures and adherence to compliance requirements

25.1.3. Security auditing is primarily conducted with the intent of checking conformance with established policies, procedures, standards guidelines and controls. It involves review of operational, technical, administrative, managerial controls implemented for information security

25.1.4. Recommendations and corrective actions are derived out of security audits to improve the implementation of controls and reduce security risks to an acceptable level

25.1.5. Security auditing is an on-going task and presents the overall state of existing protection at a given point in time and reveals status of implementation compared with defined security policies

25.2. Security audit management guidelines

25.2.1. **Determine security auditing requirements:** The organization should define enterprise-wide mechanism to identify requirements and considerations for conducting security audits and scope definition. Parameters, such as the ones listed below, should be used by the organization to define scope of audits: **G 95**

a. Nature of operations, risk appetite of organization, criticality of processes and operational transactions

b. Exposure of organizations information to security threats

c. Enterprise security policy, strategy and standards

d. Legal and compliance requirements

e. Historical information: previous audit reports, security incidents

25.2.2. **Periodicity and nature of audits:** The organization should conduct periodic audits of all information systems, infrastructure, facilities, third parties etc. which handle classified information at any instance in its lifecycle **G 96**

a. Define nature of audit — internal/external, ongoing/project based, enterprise wide/limited to individual area

b. Define need for audit— compliance specific (NISPG, ISO standard, PCI-DSS etc.), security certification specific

c. Allocate audit related tasks to dedicated and independent audit execution team — such as internal team, third-party audit etc.

d. Define security audit types, schedule & timeline of audits, resource requirement audit —internal stakeholders and external partners efforts required

e. Establish audit and assurance processes, and tactical mechanisms or tools to conduct the same

25.2.3. **Audit management function:** The organization should formulate a dedicated audit management function **G 97**

a. Roles & responsibilities of the function should be clearly defined

b. Identification of resources required for security audit such as automated tools, manpower, down time etc

25.2.4. **Evidence and artifacts:** The organization must define processes to manage audit sources or artifacts or evidences, such as below, in a secure manner **G 98**

a. Policy documents

b. Design/architecture

c. Flow diagrams

d. System documents

e. Process documents

f. Standards and procedures

g. Operational guidelines

h. Systems reports

i. Test reports

25.2.5. **Management reporting and actions:** The organization must devise processes which ensure that all audit observations, issues and recommendations by the audit teams are reported to the head of respective department for necessary action and review **G 99**

25.3. Security audit implementation guidelines

25.3.1. **Determine security auditing requirements:** The organization must hold meetings with all stakeholders or heads of the department to chalk out the requirements for security audits such as: **IG 165**

a. Examine the effectiveness of the existing policy, standards, guidelines and procedures

b. Compensating measures for existing vulnerabilities

c. Risks associated with category of classified information

25.3.2. **Periodicity and nature of audits:** Security audits must be conducted periodically to ensure compliance with security policy, guidelines, and procedures, and to determine the minimum set of controls required to address an organization's security. At a minimum security audit should be performed: **IG 166**

a. Prior to implementation or installation or major enhancements in the organization

b. Periodically such as quarterly either manually or automatically using tools

c. Randomly between planned cycles of quarterly audit to reflect actual practice

25.3.3. **Audit management function:** A dedicated management function must be formulated by organization to conduct security audits and associated tasks such as **IG 167**

a. Compiling audit requirements
b. Defining audit types
c. Identifying audit engagements
d. Planning and arranging audits
e. Overseeing audit execution
f. Managing engagement performance
g. Managing audit results
h. Reporting to the management

25.3.4. **Evidence and artifacts:** The organization must define how much and what type of information should be captured, during each audit cycle **IG 168**

a. Organization should filter, store, access and review the audit data and logs such as log files including system start up and shut down information, logon and logout attempts, command execution, access violations amongst others; reports such as audit trails, summaries, statistics amongst others; storage media such as optical disks, USBs etc.

25.3.5. **Management reporting and actions:** Personnel associated with security audit should analyze auditing results to reflect current security status, severity level of the vulnerabilities or anomalies present after removing false-positives and report it to the concerned departments of the organization for remediation. The results of all security audits must be shared with the ISSC and senior management **IG 169**

a. Recommendations and corrective actions for improvements

26. Business continuity

26.1. Background

26.1.1. Business continuity is a key element in organizations security initiatives. Information systems are vulnerable to a number of disruptions and threats ranging from both man-made and natural disasters. One of the major objectives of business continuity is the protection of availability of information, by timely resumption of key operational activities, in the event of a disruption

26.1.2. The identification of disruptions should essentially be part of the overall information security risk assessment. This will help identify the various types of threats to information and empower the organization to develop strategies to protect against the same. All activities and operations inherently possess risks which need to be identified, in addition to the potential of such risks cause interruptions. The response strategy to contain and manage risks in an effective manner and to reduce the likely impact of such disruptions may then be devised by organizations

26.2. Business continuity management guidelines

26.2.1. **Inventory of operational processes:** The organization should create an inventory of all operational processes and categorize each on the basis of sensitivity and criticality of information transacted in each process **G 100**

26.2.2. **Risk assessment and impact analysis:** The organization should conduct appropriate risk assessments and impact analysis to identify the associated risk, likely impact and disruption and the likelihood of occurrence of such disruption **G 101**

26.2.3. **Protection from disruption:** The organization must implement appropriate controls to prevent or reduce risk from likely disruptions **G 102**

26.2.4. **Test and management of continuity plans:** The organization should devise, implement, test and maintain business continuity response plans **G 103**

a. The organization should devise appropriate strategy to ensure continuity of operations and availability of classified information and information systems, in the event of a disruption

b. Adequate redundancies should be created to ensure alternate personnel, location and infrastructure are available to manage a disruptive event

26.2.5. **Security capability continuity:** The organization should implement measures to ensure that the security of information and information systems containing classified information is maintained to its defined level, even in the event of a disruption or adverse situation **G 104**

26.2.6. **Improvement of continuity plans:** The organization should verify and test business continuity processes and procedures on a regular basis to identify gaps and weaknesses in its implementation. Appropriate feedback mechanisms should be developed to continuously improve efficiency of business continuity processes **G 105**

26.3. Business continuity implementation guidelines

26.3.1. **Inventory of operational processes:** Responsibility for systems and resource availability and key business processes should be clearly identified in advance **IG 170**

a. Create mapping of ICT systems with operational processes

b. Continuous update of the mapping above

c. Use of automated tool to track changes and perform updates

26.3.2. **Risk assessment and business impact analysis:** **IG 171**

a. Risk assessment should be performed by personnel representing various organizational functions and support groups

b. Organization should identify and review risks that could possibly impact the business, and rate the likelihood of each, using information about known or anticipated risks

c. Risk assessments and business impact analysis must be conducted at a regular frequency

26.3.3. **Protection from disruption:** Organization should identify, document and review risks associated with business critical processes such as sales, research & development amongst others. Appropriate controls should be deployed by the organization to address the risks. **IG 172**

26.3.4. **Test and management of continuity plans:** Organization should identify resources required for resumption and recovery, such resources can include personnel, technology hardware and software, specialized equipment, identifying & backing up vital business records amongst others. **IG 173**

26.3.5. **Security capability continuity:** **IG 174**

a. Appropriate capabilities should be implemented to maintain existing information security posture during disruptions

b. Compensating controls and capabilities should be implemented in case of collapse of existing security capabilities and attempts must be made to return to most secure condition in least possible time

26.3.6. **Improvement of continuity plans:** Continuity plans should be regularly reviewed and evaluated. Reviews should occur according to a pre-determined schedule such as on yearly basis, and documentation of the review should be maintained **IG 175**

a. There must be a steering committee setup to oversee the Business Continuity strategy and implementation and a working group to review and implement the IT DR

27. Open source technology

27.1. Background

27.1.1. Open source technology is available as source code under a license agreement. It imposes very few restrictions on the use, modification and redistribution of the source code. Using open standards can support greater interoperability between systems and devices

27.1.2. The use of open source technology is particularly widespread in areas such as network infrastructure, computer servers, information security, Internet and intranet applications and network communications

27.1.3. Open source technology rarely involves any up-front purchase costs and provides more flexibility compared with commercial software contractual agreements

27.2. Open source technology management guidelines

27.2.1.	**Integration:** The organization must ensure that open source technology selections are suitable for integration with existing infrastructure	**G 106**
27.2.2.	**Licensing:** Organization must ensure that open source technology has minimum licensing and binding requirements	**G 107**
27.2.3.	**Security testing:** Organization must conduct independent security review of open source technology in addition to gathering information about security of such technology from subject matter experts etc. *(refer section 15)*	**G 108**
27.2.4.	**Installation:** Organization must make sure that open source technology to be procured contains clearly defined and easy to understand installation procedure	**G 109**
27.2.5.	**Additional requirements:** The organization must ensure that additional system components required for procurement of open source technology are adequately handled	**G 110**
27.2.6.	**Expertise:** Organization must ensure that it has capability and expertise for testing and deployment of open source technology	**G 111**
27.2.7.	**Availability of support:** Organization must ensure that vendors providing open source technology are contractually bound to provide lifetime support towards patching and up-gradation of the technology	**G 112**

27.3. Open source technology implementation guidelines

27.3.1.	**Integration:** Organization should consider various factors which make open source technology suitable for integration with existing infrastructure such as operating system, processing power, storage space, connectivity, interoperability with other technologies amongst others	**IG 176**
27.3.2.	**Licensing:** Organization should ensure that licensing agreements have minimum binding nature such as on the use of technology, time duration of use, number of systems allowed for use, permitted modifications amongst others	**IG 177**

27.3.3. **Installation:** Organization should ensure open source technology has clearly defined installation process which is understandable to ICT personnel **IG 178**

27.3.4. **Additional requirements:** Organization should ensure that additional requirements of open source technology are adequately obtained such as system components, libraries or modules amongst others. **IG 179**

27.3.5. **Expertise:** Organization must ensure that it has expertise to handle installation, migration, maintenance, changes etc. in the open source technology either in-house or through external parties. **IG 180**

27.3.6. **Availability of support:** **IG 181**

a. The organization must ensure that adequate support in the form of upgrades, patches etc. is part of contractual obligation of vendor providing open source technology

b. Organization should make sure of relevant support mechanism in case of any problems with the open source technology while in use such as availability of helpdesk, troubleshooting and bug-fix services amongst others

c. Organization should ensure that open source technology receives regular patching of newly introduced vulnerabilities

d. Organization should also ensure that open source technology receives relevant up gradation to it from the vendor at regular intervals

Information handling matrix

28. Adoption matrix based on information classification

Area	Top secret	Secret	Confidential	Restricted	Unclassified
Network and infrastructure security					
Inventory of assets and infrastructure	Mapping of information to infrastructure element Categorization of devices based on information classification Comprehensive network diagram Updation to reflect each change Standard for device configuration Documentation of configuration changes Adherence to architecture principles ---------- G1 C1, C2, C3 IG1, IG1(a); IG2, IG2(a), (b); IG3, IG3 (a), (b),(c)	Mapping of information to infrastructure element Categorization of devices based on information classification Comprehensive network diagram Updation to reflect each change Standard for device configuration Documentation of configuration changes Adherence to architecture principles ---------- G1 C1, C2, C3 IG1, IG1(a); IG2, IG2(a), (b); IG3, IG3 (a), (b),(c)	Mapping of information to infrastructure element Comprehensive network diagram Updation to reflect each change Standard for device configuration Adherence to architecture principles ---------- G1 C1, C2, C3 IG1, IG2, IG2(a); IG3, IG3 (a), (c)	Comprehensive network diagram Updation to reflect each change Standard for device configuration ---------- G1 C2, C3 IG2, IG2(a); IG3,	Comprehensive network diagram Standard for device configuration ---------- G1 C2, C3 IG2, IG3,
Security testing of network & infrastructure devices	Tested and certified in any globally recognised lab Tested and certified by labs of STQC, DRDO or other designated government test labs ---------- G2, C4 IG4, IG4(b), (c)	Tested and certified in any globally recognised lab Tested and certified by labs of STQC, DRDO or other designated government test labs ---------- G2, C4 IG4, IG4(b), (c)	Self-certified by manufacturer ---------- G2, C4 IG4, IG4(a), (b)	Self-certified by manufacturer ---------- G2, C4 IG4, IG4(a)	----------
Network perimeter	Traffic inspection and detection	Traffic inspection and detection	Traffic inspection and detection	Traffic inspection and detection	Traffic inspection and detection

Area	Top secret	Secret	Confidential	Restricted	Unclassified
security	Intrusion detection system Intrusion prevention system DoS and DDoS protection SIEM capability Mock drill Disable IPv6 unless required Standard addresses for critical systems Firewall, IDS, IPS capable of IPv6 Logging for IPv6 traffic All future network should be IPv6 compatible ---------- G3, C5,C6, IG5, IG5 (a), (b), (c), (d), (e) IG6 , IG6 (a), (b), (c), (d) , (e)	Intrusion detection system Intrusion prevention system DoS and DDoS protection SIEM capability Mock drill Disable IPv6 unless required Standard addresses for critical systems Firewall, IDS, IPS capable of IPv6 Logging for IPv6 traffic All future network should be IPv6 compatible ---------- G3, C5,C6, IG5, IG5 (a), (b), (c), (d), (e) IG6 , IG6 (a), (b), (c), (d) , (e)	Intrusion detection system Intrusion prevention system DoS and DDoS protection Disable IPv6 unless required All future network should be IPv6 compatible ---------- G3, C5,C6, IG5, IG5 (a), (b), (c), (d) IG6 , IG6 (a) , (e)	DoS protection Disable IPv6 unless required All future network should be IPv6 compatible ---------- G3, C5,C6, IG5, IG5 (a), (d) IG6 , IG6 (a), (e)	Disable IPv6 unless required All future network should be IPv6 compatible ---------- G3, C5,C6, IG5, IG5 (a) IG6 , IG6 (a) , (e)
Network zones	Demilitarized Zone (DMZ) Access control list (ACL) Virtual LAN Network and host based firewalls Application & content filtering and proxies Physical segregation ---------- G4 C7, C8,C9 IG7, IG7 (a), (b) IG8, IG8 (a), (b), (c),	Demilitarized Zone (DMZ) Access control list (ACL) Virtual LAN Network and host based firewalls Application & content filtering and proxies ---------- G4 C7, C8,C9 IG7, IG7 (a), (b) IG8, IG8 (a), (b), (c), (d),(e)	Demilitarized Zone (DMZ) Access control list (ACL) Virtual LAN Network and host based firewalls ---------- G4 C7, C8,C9 IG7, IG7 (a), (b) IG8, IG8 (a), (b), (c), (d),(e) IG9, IG9 (a),	Demilitarized Zone (DMZ) Access control list (ACL) Virtual LAN ---------- G4 C7, C8, IG7, IG7 (a), (b) IG8, IG8 (a), (b), (c), (d), (e)	Demilitarized Zone (DMZ) Access control list (ACL) ---------- G4 C7, C8, IG7, IG7 (a), (b)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	(d),(e) IG9, IG9 (a), (b), (c)	IG9, IG9 (a), (b)			
LAN security	Remove default device password Use of complex 12 character password Use secure protocols - SSH, SSL, IPSec Traffic monitoring Mapping of IP addresses to MAC address --- G5 C10 IG10, IG10 (a), (b), (c), (d), (e)	Remove default device password Use of complex 12 character password Use secure protocols - SSH, SSL, IPSec Traffic monitoring Mapping of IP addresses to MAC address --- G5 C10 IG10, IG10 (a), (b), (c), (d), (e)	Remove default device password Use of complex 12 character password Use secure protocols - SSH, SSL, IPSec Traffic monitoring --- G5 C10 IG10, IG10 (a), (b), (c), (d)	Remove default device password Use of complex 12 character password Use secure protocols - SSH, SSL, IPSec --- G5 C10 IG10, IG10 (a), (b), (c)	Remove default device password Use of complex 12 character password Use secure protocols - SSH, SSL, IPSec --- G5 C10 IG10, IG10 (a), (b), (c)
Wireless architecture	Wireless network not allowed	Wireless network not allowed	Limiting coverage of access points Standard wireless network configuration Wireless encryption (WPA-2 or higher) Secure protocol for managing access points Wireless security gateway No visitor VLAN access Audit and vulnerabilities assessment Logging and monitoring No concurrent wired and wireless connection Physical isolation Disable SSID broadcasting Disable DHCP and	Limiting coverage of access points Standard wireless network configuration Wireless encryption (WPA-2 or higher) Secure protocol for managing access points Wireless security gateway Audit and vulnerabilities assessment Logging and monitoring Disable SSID broadcasting Disable DHCP and assign static IP addresses --- G6 C11 IG11, IG11 (a), (b), (c), (d), (e), (g),	Limiting coverage of access points Standard wireless network configuration Wireless encryption (WPA-2 or higher) Secure protocol for managing access points Audit and vulnerabilities assessment --- G6 C11 IG11, IG11 (a), (b), (c), (d), (g)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
			assign static IP addresses ---------- G6 C11 IG11, IG (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l)	(h), (k), (l)	
Network security management	Disable unused ports, protocols services No personal device allowed Access to public network not allowed Identification of device connecting to the network Pre-connection health scan Restricted external connections Remote access, VOIP, telephony and conferencing not allowed Maintain updated firmware In-house patch testing and change mechanism Develop process for change management Approval by Information Security Steering Committee Secure transmission cables and cabinets Quarterly security audit of all information systems, network devices, processes, governance procedures etc.	Disable unused ports, protocols services No personal device allowed Access to public network not allowed Identification of device connecting to the network Pre-connection health scan Restricted external connections Remote access, VOIP, telephony and conferencing not allowed Maintain updated firmware In-house patch testing and change mechanism Develop process for change management Approval by Information Security Steering Committee Secure transmission cables and cabinets Quarterly security audit of all information systems, network devices, processes, governance	Authorization and provisioning of personal devices Health check of personal devices Containerization of data on personal devices Monitored external connections Strict governance of remote access, VOIP, telephony and conferencing Maintain updated firmware Bi-annual security audit of all information systems, network devices, processes, governance procedures etc. ---------- G7 C12,C13,C14,C15, C16, C17,C18, , C21 IG12 IG13, IG13 (a), (b), (c), (d) IG14 (a), (b), IG15, IG15 (a), (b), (c), (d), (e), (f), (g) IG17, IG17 (a), (b), (c), (d), (e)	Maintain updated firmware Use of personal device allowed Yearly security audit of all information systems, network devices, processes, governance procedures etc. ---------- G7 C12,C13, C16, C18, , C21 IG12 IG13 IG16 IG18	Maintain updated firmware Use of personal device allowed Yearly security audit of all information systems, network devices, processes, governance procedures etc. ---------- G7 C12,C13, C16, C18, , C21 IG12 IG13 IG16 IG18

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	--- G7 C12,C14,C15, C16, C17,C18, C21 IG12 IG14, IG14 (a), (b), IG15, IG15 (a), (b), (c), (d), (e), (f), (g) IG16 IG17, IG17 (a), (b), (c), (d), (e) IG18 IG21	procedures etc. --- G7 C12,C14,C15, C16, C17,C18, , C21 IG12 IG14, IG14 (a), (b), IG15, IG15 (a), (b), (c), (d), (e), (f), (g) IG16 IG17, IG17 (a), (b), (c), (d), (e) IG18 IG21			
Unauthorized access	Changed device default credentials Network active host scanning mechanism IP scanners Client-side digital certificates --- G8 C19, C20 IG19 IG20, IG20 (a)	Changed device default credentials Network active host scanning mechanism IP scanners Client-side digital certificates --- G8 C19, C20 IG19 IG20, IG20 (a)	Changed device default credentials Network active host scanning mechanism --- G8 C19 IG19	Changed device default credentials --- G8 C19 IG19	Changed device default credentials --- G8 C19 IG19
Extending connectivity to third parties	Access only to limited ports, services, protocols Limit access to defined purpose and time duration No sharing of network configuration, device credentials Strict monitoring of third party traffic to and from network --- G9	Access only to limited ports, services, protocols Limit access to defined purpose and time duration No sharing of network configuration, device credentials Strict monitoring of third party traffic to and from network --- G9	Access only to limited ports, services, protocols Limit access to defined purpose and time duration No sharing of network configuration, device credentials Strict monitoring of third party traffic to and from network --- G9	Access only to limited ports, services, protocols Limit access to defined purpose and time duration No sharing of network configuration, device credentials --- G9 C22 IG22, IG22 (a), (b), (c),	Access only to limited ports, services, protocols No sharing of network configuration, device credentials --- G9 C22 IG22, IG22 (a), (b),

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	C22 IG22, IG22 (a), (b), (c), (d)	C22 IG22, IG22 (a), (b), (c), (d)	C22 IG22, IG22 (a), (b), (c), (d)		
Identity, access and privilege management					
Governance procedures for access rights, identity & privileges	Mapping and grouping of business roles with IT roles Rules for granting and revoking access Unique identity of each user Identity provisioning process and workflow Sharing of user ID not allowed Designated process of user access authorization Strict enforcement of access policies across infrastructure components Correlation between physical and logical access Role based access control Authorization as per security access matrix Logging, monitoring and review of user privileges Strict control of special privileges – duration, purpose, monitoring --- G10 C23, C24, C25, C26, C27, C28, C29, IG23, IG23 (a), (b), (c), (d) IG24, IG24 (a), (b),	Mapping and grouping of business roles with IT roles Rules for granting and revoking access Unique identity of each user Identity provisioning process and workflow Sharing of user ID not allowed Designated process of user access authorization Strict enforcement of access policies across infrastructure components Correlation between physical and logical access Role based access control Authorization as per security access matrix Logging, monitoring and review of user privileges Strict control of special privileges – duration, purpose, monitoring --- G10 C23, C24, C25, C26, C27, C28, C29, IG23, IG23 (a), (b),	Mapping and grouping of business roles with IT roles Rules for granting and revoking access Unique identity of each user Identity provisioning process and workflow Sharing of user ID allowed on approval Logging of activity from shared user ID Designated process of user access authorization Strict enforcement of access policies across infrastructure components Role based access control Logging, monitoring and review of user privileges --- G10 C23, C24, C25, C26, C27, C28, C29, IG23, IG23 (a), (b), (c), (d) IG24, IG24 (a), (b), (c), (d), (e), (f), (g) IG25, IG25 (a), (b),	Mapping and grouping of business roles with IT roles Unique identity of each user Sharing of user ID allowed on approval Logging of activity from shared user ID Designated process of user access authorization Need to know access --- G10 C23, C24, C25, C26, C27, C28, C29, IG23, IG23 (a), (b) IG24, IG24 (a), (c), (d), (e), (f), (g) IG25, IG25 (a), (b), (c), (d), IG26, IG26 (a), (b), (c), IG27, IG27 (a), (b) IG28 IG29, IG29 (a), (b), (c)	Unique identity of each user Sharing of user ID allowed on approval Logging of activity from shared user ID Designated process of user access authorization Need to know access --- G10 C23, C24, C25, C26, C27, C28, C29, IG23, IG23 (a), (b) IG24, IG24 (a), (d), (f) IG25, IG25 (a), (b), (c), (d), IG26, IG26 (a) IG27, IG27 (a), (b) IG28 IG29, IG29

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	(c) IG25, IG25 (a), (b), (c), (d), IG26, IG26 (a), (b), (c), (d), IG27, IG27 (a), (b), (c), (d), IG28 IG29, IG29 (a), (b), (c)	(c), (d) IG24, IG24 (a), (b), (c), IG25, IG25 (a), (b), (c), (d), IG26, IG26 (a), (b), (c), (d), IG27, IG27 (a), (b), (c), (d), IG28 IG29, IG29 (a), (b), (c)	(c), (d), IG26, IG26 (a), (b), (c), IG27, IG27 (a), (b), (c) IG28 IG29, IG29 (a), (b), (c)		
Authentication & authorization for access	User ID/ password Multifactor authentication (including biometrics) Directory services Identity proofing One time password PKI authentication Encrypted channel for credential sharing Disable account on inactivity of 30 days Elaborate access use policy User signoff on acceptable use policy ---------- G11 C30, C31, C32 IG30 , IG30 (a), (b), (c), (d) IG31, IG31 (a), (b), (c), (d), IG32, IG32 (a), (b), (c)	User ID/ password Multifactor authentication (including biometrics) Directory services Identity proofing One time password PKI authentication Encrypted channel for credential sharing Disable account on inactivity of 30 days Elaborate access use policy User signoff on acceptable use policy ---------- G11 C30, C31, C32 IG30 , IG30 (a), (b), (c), (d) IG31, IG31 (a), (b), (c), (d), IG32, IG32 (a), (b), (c)	User ID/ password Multifactor authentication Directory services Encrypted channel for credential sharing Disable account on inactivity of 45 days Elaborate access use policy ---------- G11 C30, C31, C32 IG30 , IG30 (a), (b), (c), (d) IG31, IG31 (a), (b), (c), (d), IG32, IG32 (a), (b), (c)	User ID/ password Directory services Encrypted channel for credential sharing Disable account on inactivity of 60 days Elaborate access use policy ---------- G11 C30, C31, C32 IG30 , IG30 (a), IG31, IG31 (a) IG32, IG32 (a), (b), (c)	User ID/ password Encrypted channel for credential sharing Disable account on inactivity of 60 days Elaborate access use policy ---------- G11 C30, C31, C32 IG30 , IG30 (a), IG31, IG31 (a) IG32, IG32 (a)
Password management	Password activation process 12 character complex	Password activation process 12 character complex	Password activation process 12 character complex	Password activation process 12 character complex	Password activation process 12 character complex

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	alphanumeric password Password encryption Strict adherence to password standards Revocation post 30 days inactivity Change default password prior to use Password communication through alternate channel ---------- G12 C33 IG33, IG33 (a), (b), (c), (d), (e), (f) IG34	alphanumeric password Password encryption Strict adherence to password standards Revocation post 30 days inactivity Change default password prior to use Password communication through alternate channel ---------- G12 C33 IG33, IG33 (a), (b), (c), (d), (e), (f) IG34	alphanumeric password Password encryption Strict adherence to password standards Revocation post 45 days inactivity Change default password prior to use Password communication through alternate channel ---------- G12 C33 IG33, IG33 (a), (b), (c), (d), (e), (f) IG34	alphanumeric password Password encryption Strict adherence to password standards Revocation post 60 days inactivity Change default password prior to use ---------- G12 C33 IG33, IG33 (a), (b), (c), (d), (e) IG34	alphanumeric password Password encryption Strict adherence to password standards Revocation post 60 days inactivity Change default password prior to use ---------- G12 C33 IG33, IG33 (a), (b), (c), (d), (e) IG34
Credential monitoring	Log generation and retention of all user account related activity Monitoring of all instances of authentication, authorization of access Deny access to system post 3 unsuccessful login attempts ---------- G13 C35, C36 IG35 IG36, IG36 (a), (b)	Log generation and retention of all user account related activity Monitoring of all instances of authentication, authorization of access Deny access to system post 3 unsuccessful login attempts ---------- G13 C35, C36 IG35 IG36, IG36 (a), (b)	Log generation and retention of all user account related activity Deny access to system post 5 unsuccessful login attempts ---------- G13 C35, C36 IG35 IG36, IG36 (a), (b)	Deny access to system post 5 unsuccessful login attempts ---------- G13 C35, C36 IG36, IG36 (a), (b)	Random CAPTCHA post 3 unsuccessful login attempts ---------- G13 C35, C36 IG36, IG36 (a), (b)
Provisioning personal devices and remote access	Strict monitoring of maintenance and support activity Log of all maintenance activity No remote access	Strict monitoring of maintenance and support activity Log of all maintenance activity	Authorization for remote access Remote access via VPN based on SSL/TLS, SSTP or IPsec Log of remote	Authorization for remote access Remote access via VPN based on SSL/TLS, SSTP or IPsec Log of remote	Authorization for remote access Remote access via VPN based on SSL/TLS, SSTP or IPsec ----------

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	--- G14 C37, C38, C39 IG37 IG38, IG38 (a), (b), (c), IG39	No remote access --- G14 C37, C38, C39 IG37 IG38, IG38 (a), (b), (c), IG39	access --- G14 C37, C38, C39 IG37 IG38, IG38 (a), (b), (c), IG39	access --- G14 C37, C38, C39 IG37 IG38, IG38 (a), (b), (c), IG39	G14 C37, C38, C39 IG37 IG38, IG38 (a), (b), (c), IG39
Segregation of duties	Segregation of duties --- G15 C40 IG40, IG40 (a), (b), (c), (d), (e), (f), (g)	Segregation of duties --- G15 C40 IG40, IG40 (a), (b), (c), (d), (e), (f), (g)	Segregation of duties --- G15 C40 IG40, IG40 (a), (b), (c), (d), (e), (f), (g)	Segregation of duties --- G15 C40 IG40, IG40 (a)	Segregation of duties --- G15 C40 IG40, IG40 (a)
Access record documentation	Maintain record of user access request --- G16 C25 IG25, IG25 (a)	Maintain record of user access request --- G16 C25 IG25, IG25 (a)	Maintain record of user access request --- G16 C25 IG25, IG25 (a)		
Linkage of logical and physical access	Mechanism to correlate between logical and physical access --- G17 C26 IG26 (d)	Mechanism to correlate between logical and physical access --- G17 C26 IG26 (d)			
Disciplinary actions	Non – compliance will invoke disciplinary actions --- G18 C41 IG41	Non – compliance will invoke disciplinary actions --- G18 C41 IG41	Non – compliance will invoke disciplinary actions --- G18 C41 IG41	Non – compliance will invoke disciplinary actions --- G18 C41 IG41	Non – compliance will invoke disciplinary actions --- G18 C41 IG41
Physical and environmental security					
Map and characteristics of physical	Comprehensive map and characterization of physical facilities	Comprehensive map and characterization of physical facilities	Comprehensive map and characterization of physical facilities	Comprehensive map and characterization of physical facilities	

Area	Top secret	Secret	Confidential	Restricted	Unclassified
facilities	Map of deployed information systems and resources in each physical facility Maintain list of authorized personnel Verification of user ---------------- G19 C42 IG42 (a), (b), (c)	Map of deployed information systems and resources in each physical facility Maintain list of authorized personnel Verification of user ---------------- G19 C42 IG42 (a), (b), (c)	Map of deployed information systems and resources in each physical facility Maintain list of authorized personnel Verification of user ---------------- G19 C42 IG42 (a), (b), (c)	Map of deployed information systems and resources in each physical facility Maintain list of authorized personnel Verification of user ---------------- G19 C42 IG42 (a), (b), (c)	
Protection from hazard	Regular assessment of hazard Deployment of fire alarm, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings ---------------- G20 C43, C44 IG43 IG44	Regular assessment of hazard Deployment of fire alarm, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings ---------------- G20 C43, C44 IG43 IG44	Regular assessment of hazard Deployment of fire alarm, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings ---------------- G20 C43, C44 IG43 IG44	Regular assessment of hazard Deployment of fire alarm, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings ---------------- G20 C43, C44 IG43 IG44	Regular assessment of hazard Deployment of fire alarm, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings ---------------- G20 C43, C44 IG43 IG44
Physical boundary protection	Biometric access Access control gateway Photo-ID badges with smart chips Visitor escort by authorized person Visitor identity proof Log of visitor activity, purpose, devices, time, photo capture Issue of temp ID to visitor – clear mention of area allowed to visit Restriction on external media Additional access barriers for	Biometric access Access control gateway Photo-ID badges with smart chips Visitor escort by authorized person Visitor identity proof Log of visitor activity, purpose, devices, time, photo capture Issue of temp ID to visitor – clear mention of area allowed to visit Restriction on external media Additional access barriers for	Access control gateway Photo-ID badges Protection of power, telecommunication, network or other transmission cables from unauthorized access of damage Visitor identity proof Log of visitor activity, purpose, devices, time, photo capture Issue of temp ID to visitor – clear mention of area allowed to visit Restriction on	Access control gateway Photo-ID badges Protection of power, telecommunication, network or other transmission cables from unauthorized access of damage Visitor identity proof Log of visitor activity, purpose, devices, time, photo capture Issue of temp ID to visitor – clear mention of area allowed to visit SOP's and training	Photo-ID badges Protection of power, telecommunication, network or other transmission cables from unauthorized access of damage Log of visitor activity, purpose, devices, time, photo capture Issue of temp ID to visitor – clear mention of area allowed to visit Perform manual inspection of vehicles ----------------

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	sensitive areas such as data center Protection of power, telecommunication, network or other transmission cables from unauthorized access of damage Background check of security personnel SOP's and training for physical security instances Deploy physical barriers, manual inspection of vehicles, security lighting, video surveillance ---------- G21 C45, C46, C47, C48, C49, C50, C51 IG45 IG46, IG 46 (a) IG47, IG47 (a), (b), (c), (d) IG48, IG48 (a), (b), (c) IG49, IG 49 (a), (b), (c) IG50, IG50 (a), (b) IG51	sensitive areas such as data center Protection of power, telecommunication, network or other transmission cables from unauthorized access of damage Background check of security personnel SOP's and training for physical security instances Deploy physical barriers, manual inspection of vehicles, security lighting, video surveillance ---------- G21 C45, C46, C47, C48, C49, C50, C51 IG45 IG46, IG 46 (a) IG47, IG47 (a), (b), (c), (d) IG48, IG48 (a), (b), (c) IG49, IG 49 (a), (b), (c) IG50, IG50 (a), (b) IG51	external media Background check of security personnel SOP's and training for physical security instances Perform manual inspection of vehicles, video surveillance ---------- G21 C45, C46, C47, C48, C49, C50, C51 IG45 IG46, IG 46 (a) IG47, IG47 (a), (b), (c) IG48, IG48 (a), (b), (c) IG49, IG 49 (a), (b), (c) IG50, IG50 (a) IG51	for physical security instances Perform manual inspection of vehicles ---------- G21 C45, C46, C47, C48, C49, C50, C51 IG45 IG46 IG47 IG48, IG48 (a), (b), (c) IG49, IG 49 (a), (b), (c) IG51	G21 C45, C46, C47, C49 IG45 IG46 IG49, IG 49 (a), (b), (c)
Restricting entry	Correlation between physical and logical security ---------- G22 C45, C46, C52 IG45 IG46, IG46 (a) IG52, IG52 (a), (b)	Correlation between physical and logical security ---------- G22 C45, C46, C52 IG45 IG46, IG46 (a) IG52, IG52 (a), (b)	Correlation between physical and logical security ---------- G22 C45, C46, C52 IG45 IG46, IG46 (a) IG52, IG52 (a), (b)		
Interior security	24/7 video surveillance	24/7 video surveillance	24/7 video surveillance	Privacy filters for all devices	Privacy filters for all devices

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	Secure retention of video records for 60 days Physical destruction of storage media, equipment Significant change in physical security approved by ISSC System lock-out post 5 minutes of inactivity Restricted issue and updated record of physical access keys, cards, password issued Periodic audit of access measures ---------- G23 C53, C54, C55, C56, C57, C58, C59 IG53, IG53 (a), (b) IG54, IG54 (a) IG55 IG56 IG57 IG58, IG58 (a), (b), (c) IG59	Secure retention of video records for 60 days Physical destruction of storage media, equipment Significant change in physical security approved by ISSC System lock-out post 5 minutes of inactivity Restricted issue and updated record of physical access keys, cards, password issued Periodic audit of access measures ---------- G23 C53, C54, C55, C56, C57, C58, C59 IG53, IG53 (a), (b) IG54, IG54 (a) IG55 IG56 IG57 IG58, IG58 (a), (b), (c) IG59	Secure retention of video records for 60 days Physical destruction of storage media, equipment Significant change in physical security approved by ISSC System lock-out post 5 minutes of inactivity Restricted issue and updated record of physical access keys, cards, password issued Periodic audit of access measures ---------- G23 C53, C54, C55, C56, C57, C58, C59 IG53, IG53 (a), (b) IG54, IG54 (a) IG55 IG56 IG57 IG58, IG58 (c) IG59	Physical destruction of storage media, equipment System lock-out post 15 minutes of inactivity ---------- G23 C54, C57, C58, C59 IG54, IG54 (a) IG57 IG59	System lock-out post 15 minutes of inactivity ---------- G23 C57, C59 IG57 IG59
Security zones	Housing only in high security zone Authorization to security cleared only Perimeter monitoring Access recorded & audited ---------- G24 C60 IG60, IG60 (e)	Housing only in security zone Authorization to limited people Perimeter monitoring Access recorded & audited ---------- G24 C60 IG60, IG60 (d)	Housing only in security zone Authorization to limited people Perimeter monitoring ---------- G24 C60 IG60, IG60 (d)	Housing only in operation zone Authorization to limited people ---------- G24 C60 IG60, IG60 (c)	Housing only in operation zone Authorization to limited people ---------- G24 C60 IG60, IG60 (c)
Access to	Visitor entry	Visitor entry	Wearable	Wearable	Wearable

Area	Top secret	Secret	Confidential	Restricted	Unclassified
restricted area	banned unless required Wearable computing devices should not be allowed Record of entry and exit of visitors Authorization of movement of equipment Inventory of equipment in the facility Record and verification of visitor devices External media should not be allowed to enter ---------- G25 C61, C62 IG61, IG61 (a), (b), (c) IG62, IG62 (a), (b), (c)	banned unless required Wearable computing devices should not be allowed Record of entry and exit of visitors Authorization of movement of equipment Inventory of equipment in the facility Record and verification of visitor devices External media should not be allowed to enter ---------- G25 C61, C62 IG61, IG61 (a), (b), (c) IG62, IG62 (a), (b), (c)	computing devices should not be allowed Record of entry and exit of visitors Authorization of movement of equipment Inventory of equipment in the facility Record and verification of visitor devices External media should not be allowed to enter ---------- G25 C61, C62 IG61, IG61 (a), (b), (c) IG62, IG62 (a), (b)	computing devices should not be allowed Record of entry and exit of visitors Authorization of movement of equipment Inventory of equipment in the facility Record and verification of visitor devices External media should not be allowed to enter ---------- G25 C61, C62 IG61 IG62, IG62 (a), (b)	computing devices should not be allowed Record of entry and exit of visitors Authorization of movement of equipment Inventory of equipment in the facility ---------- G25 C61, C62 IG61
Physical activity monitoring and review	Physical device log enablement & collection Rules to correlate logs for physical security incidents Integration of physical & logical security SIEM implementation of physical security Real time monitoring of physical security logs ---------- G26 C63 IG63, IG63 (a), (b), (c), (d), (e)	Physical device log enablement & collection Rules to correlate logs for physical security incidents Integration of physical & logical security SIEM implementation of physical security Real time monitoring of physical security logs ---------- G26 C63 IG63, IG63 (a), (b), (c), (d), (e)	Physical device log enablement & collection Rules to correlate logs for physical security incidents ---------- G26 C63 IG63, IG63 (a), (b)	Physical device log enablement & collection Rules to correlate logs for physical security incidents ---------- G26 C63 IG63, IG63 (a), (b)	

Area	Top secret	Secret	Confidential	Restricted	Unclassified
Application Security					
Application security process	Detailed application records Application security processes Function accountable for application security --- G27 C64 IG64 (a), (b), (c)	Detailed application records Application security processes Function accountable for application security --- G27 C64 IG64 (a), (b), (c)	Detailed application records Application security processes --- G27 C64 IG64 (a), (b)	Detailed application records Application security processes --- G27 C64 IG64 (a), (b)	Application records --- G27 C64 IG64
Application security design	Secure coding adhering to OWASP guidelines Threat modeling, data flow analysis & risk assessment Planned interactions, data handling, authentication & authorization No hardcoded password Adherence to application security standards --- G28 C65 IG65 (a), (b), (c), (d), (e)	Secure coding adhering to OWASP guidelines Threat modeling, data flow analysis & risk assessment Planned interactions, data handling, authentication & authorization No hardcoded password Adherence to application security standards --- G28 C65 IG65 (a), (b), (c), (d), (e)	Secure coding adhering to OWASP guidelines Planned interactions, data handling, authentication & authorization No hardcoded password Adherence to application security standards --- G28 C65 IG65 (a), (c), (d), (e)	Secure coding adhering to OWASP guidelines Planned interactions, data handling, authentication & authorization No hardcoded password Adherence to application security standards --- G28 C65 IG65 (a), (c), (d), (e)	Secure coding adhering to OWASP guidelines Planned interactions, data handling, authentication & authorization No hardcoded password Adherence to application security standards --- G28 C65 IG65 (a), (c), (d), (e)
Application threat management	Centralized user authentication using directory services Role base access control Review of authorization Secure configuration of ports, services, data handling,	Centralized user authentication using directory services Role base access control Review of authorization Secure configuration of ports, services, data handling,	Centralized user authentication using directory services Review of authorization Secure configuration of ports, services, data handling, password & admin access	Review of authorization Secure configuration of ports, services, data handling, password & admin access Block unused ports, services and services Unpredictable	Secure configuration of ports, services, data handling, password & admin access Block unused ports, services and services Unpredictable session identifiers, secure

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	password & admin access Block unused ports, services and services Installation audit prior to production launch or major change Unpredictable session identifiers, secure communication channels, message security, session timeouts Session encryption using HTTPS/TLS Message security S/MIME Strict input validation at server side No revelation of information by error messages No debugging feature in application Application safe mode feature ---------- G29 C66, C67, C68, C69, C70, C71 IG66, IG66 (a), (b), (c) IG67, IG67 (a) IG68, IG69, IG69 (a), (b), (c) IG70, IG70 (a) IG71, IG71 (a), (b), (c), (d), (e)	password & admin access Block unused ports, services and services Installation audit prior to production launch or major change Unpredictable session identifiers, secure communication channels, session timeouts Session encryption using HTTPS/TLS Message security S/MIME Strict input validation at server side No revelation of information by error messages No debugging feature in application Application safe mode feature ---------- G29 C66, C67, C68, C69, C70, C71 IG66, IG66 (a), (b), (c) IG67, IG67 (a) IG68, IG69, IG69 (a), (b), (c) IG70, IG70 (a) IG71, IG71 (a), (b), (c), (d), (e)	Block unused ports, services and services Installation audit prior to production launch or major change Unpredictable session identifiers, secure communication channels, session timeouts Session encryption using HTTPS/TLS Strict input validation at server side No revelation of information by error messages No debugging feature in application ---------- G29 C66, C67, C68, C69, C70, C71 IG66, IG66 (a), (c) IG67, IG67 (a) IG68 IG69, IG69 (a), (b) IG70, IG70 (a) IG71, IG71 (a), (b), (c), (d)	session identifiers, secure communication channels, session timeouts Session encryption using HTTPS/TLS Strict input validation at server side No revelation of information by error messages No debugging feature in application ---------- G29 C66, C67, C68, C69, C70, C71 IG66, IG66 (c) IG67, IG67 (a) IG68, IG69, IG69 (a), (b) IG70, IG70 (a) IG71, IG71 (a), (b), (c), (d)	communication channels, session timeouts Strict input validation at server side No revelation of information by error messages ---------- C67, C68, C69, C70, C71 IG67, IG67 (a) IG68, IG69, IG69 (a) IG70, IG70 (a) IG71, IG71 (a), (b), (c)
Application security testing	Rigorous testing of applications Daily vulnerability scanning of	Rigorous testing of applications Daily vulnerability scanning of	Testing of applications Quarterly vulnerability	Testing of applications Quarterly vulnerability	Testing of applications Quarterly vulnerability

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	application Prioritization of security issues & flaws Automated workflow for resolution of issues Emergency procedures for security flaws Security code review using government approved labs Code review using automated & manual method Quarterly penetration testing of application Resolution of vulnerabilities within 3 days ---------- G30 C72, C73, C74 IG72, IG72 (a), (b), (c), (d), (e), (f), (g), (h) IG73, IG73 (a), (b), (c), (d) IG74, IG74 (a), (b), (c), (d)	application Prioritization of security issues & flaws Automated workflow for resolution of issues Emergency procedures for security flaws Code review using automated & manual method Half yearly penetration testing of application ---------- G30 C72, C73, C74 IG72, IG72 (a), (b), (c), (d), (e), (f), (g), (h) IG73, IG73 (a), (c), (d) IG74, IG74 (a), (b), (c)	scanning of application Prioritization of security issues & flaws Emergency procedures for security flaws Half yearly penetration testing of application ---------- G30 C72, C73, C74 IG72, IG72 (a), (b), (c), (f), (h) IG74, IG74 (a), (b)	scanning of application Prioritization of security issues & flaws Half yearly penetration testing of application ---------- G30 C72, C74 IG72, IG72 (a), (b), (c), (f) IG74, IG74 (a)	scanning of application Yearly penetration testing of application ---------- G30 C72, C74 IG72, IG72 (a), (b), (c), (f) IG74, IG74 (a)
Data Management	AES 256 bit or higher encryption Audit of each instance of data access Strict enforcement of least privilege principle Access control mechanism ---------- G31 C75, C76, C77 IG75, IG75 (a), (b), (c), (d)	AES 128 bit encryption Audit of each instance of data access Strict enforcement of least privilege principle Access control mechanism ---------- G31 C75, C76, C77 IG75, IG75 (a), (b), (c), (d)	AES 128 bit encryption Audit of each instance of data access Strict enforcement of least privilege principle Access control mechanism ---------- G31 C75, C76, C77 IG75, IG75 (a), (b), (c), (d)	Audit of each instance of data access Strict enforcement of least privilege principle Access control mechanism ---------- G31 C75, C76, C77 IG75, IG75 (a) IG76, IG76 (a), (b) IG77, IG77 (a), (b)	Enforcement of least privilege principle Access control mechanism ---------- G31 C75, C77 IG75, IG75 (a) IG77, IG77 (a), (b

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	IG76, IG76 (a), (b) IG77, IG77 (a), (b)	IG76, IG76 (a), (b) IG77, IG77 (a), (b)	IG76, IG76 (a), (b) IG77, IG77 (a), (b)		
Secure Software Development Life-Cycle (SDLC)	Strict adherence to SDLC processes Responsibility distribution for security for each stage of SDLC Segregation of test, development & production environments Security testing at each stage of SDLC environment Strict adherence to change management process Significant change approval by ISSC --- G32 C78, C79 IG78, IG78 (a), (b), (c), (d) IG79, IG79 (a), (b)	Strict adherence to SDLC processes Responsibility distribution for security for each stage of SDLC Segregation of test, development & production environments Security testing at each stage of SDLC environment Strict adherence to change management process Significant change approval by ISSC --- G32 C78, C79 IG78, IG78 (a), (b), (c), (d) IG79, IG79 (a), (b)	Strict adherence to SDLC processes Strict segregation of test & development environments Segregation of test, development & production environments Security testing at each stage of SDLC environment Strict adherence to change management process Significant change approval by ISSC --- G32 C78, C79 IG78, IG78 (a), (b), (c), (d) IG79, IG79 (a), (b)	Security testing at each stage of SDLC environment --- G32 C78, C79 IG78, IG78 (d)	
Application vulnerability intelligence	Application security intelligence- internal & external Integration of intelligence in threat management --- G33 C80 IG80, IG80, IG80 (a), (b)	Application security intelligence- internal & external Integration of intelligence in threat management --- G33 C80 IG80, IG80, IG80 (a), (b)	Application security intelligence- internal & external --- G33 C80 IG80, IG80 (a)		
Application logs & monitoring	Log generation adheres to standards Web application firewall Real time monitoring of application	Log generation adheres to standards Web application firewall Daily monitoring of application Integration with	Log generation adheres to standards Periodic monitoring of logs --- G34	Log generation adheres to standards --- G34 C81 IG81, IG81 (a), (b),	Log generation adheres to standards --- G34 C81 IG81, IG81 (a), (b)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	Integration with SIEM solution Application security dashboard ---------- G34 C81 IG81, IG81 (a), (b), (c), (d), (f), (g), (h)	SIEM solution Application security dashboard ---------- G34 C81 IG81, IG81 (a), (b), (c), (d), (e), (g), (h)	C81 IG81, IG81 (a), (b) (c)		
Data security					
Data discovery, identification & classification	Process for discovering data Data discovery through automated tool Strict adherence to classification & labeling guidelines Integration of identification & classification with life cycle Automated tool for classification & labeling ---------- G35 C82, C83 IG82, IG82, IG82 (a), (b), (c), (d) IG83, IG83 (a), (b), (c)	Process for discovering data Data discovery through automated tool Strict adherence to classification & labeling guidelines Integration of identification & classification with life cycle Automated tool for classification & labeling ---------- G35 C82, C83 IG82, IG82, IG82 (a), (b), (c), (d) IG83, IG83 (a), (b), (c)	Process for discovering data Adherence to classification & labeling guidelines Integration of identification & classification with life cycle ---------- G35 C82, C83 IG82, IG82 (a), (b), (c) IG83, IG83 (a), (b)	Process for discovering data Adherence to classification & labeling guidelines Integration of identification & classification with life cycle G35 C82, C83 IG82, IG82 (a), (b), (c) IG83, IG83 (a), (b)	Adherence to classification & labeling guidelines G35 C83 IG83, IG83 (a), (b)
Cryptography & encryption	AES 256 bit or higher for data-at-rest User credentials (password) hashing SHA-2/ SHA-3, 256 bits or higher SSLv3, Transport Layer Security (TLS 1.2 or higher) S/MIME for message Cryptographic algorithms should be approved by SAG	AES 128 bit or higher for data-at-rest User credentials (password) hashing SHA1/ SHA-2, 160 bits or higher SSLv3, Transport Layer Security (TLS 1.2 or higher) S/MIME for message Cryptographic algorithms should be approved by SAG	AES 128 bit or higher for data-at-rest User credentials (password) hashing SHA1/ SHA-2, 160 bits or higher SSLv3, Transport Layer Security (TLS 1.2 or higher) S/MIME for message ---------- G36	User credentials (password) hashing SHA1/ SHA-2, 160 bits or higher SSLv3, Transport Layer Security (TLS 1.2 or higher) ---------- G36 C84 IG84,, IG84 (b), (c)	User credentials (password) hashing SHA1/ SHA-2, 160 bits or higher ---------- G36 C84 IG84, IG84 (b)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	---------- G36 C84 IG84, IG84, IG84 (a), (b), (c), (d), (e)	---------- G36 C84 IG84, IG84, IG84 (a), (b), (c), (d), (e)	C84 IG84, IG84, IG84 (a), (b), (c), (d)		
Key management	Central key management, distributed execution Centralize user profiles for authentication and access to keys Keys from Joint Cipher Bureau (JCB) Support to multiple encryption standards Log of each operational instances Key changed at end of crypto period Uniform solution for managing field, file & database encryptions Support to third party integration should be disables unless it is required Cryptographic hardware for the key storage SOPs for key management ---------- G37 C85 IG85, IG85, IG85 (a), (b), (c), (d), (e), (f), (g), (h)	Central key management, distributed execution Centralize user profiles for authentication and access to keys Keys from Joint Cipher Bureau (JCB) Support to multiple encryption standards Log of each operational instances Key changed at end of crypto period Uniform solution for managing field, file & database encryptions Support to third party integration should be disabled unless it is required Cryptographic hardware for the key storage ---------- G37 C85 IG85, IG85, IG85 (a), (b), (c), (d), (e), (f), (g), (h)	Central key management, distributed execution Centralize user profiles for authentication and access to keys Support to multiple encryption standards Log of each operational instances Uniform solution for managing field, file & database encryptions ---------- G37 C85 IG85, IG85, IG85 (a), (b), (c), (d), (f), (h)	Central key management, distributed execution Centralize user profiles for authentication and access to keys Support to multiple encryption standards Log of each operational instances Uniform solution for managing field, file & database encryptions ---------- G37 C85 IG85, IG85, IG85 (a), (b), (c), (d), (f), (h)	
Information leak prevention	Limit data storage at designated systems Field level protection for sensitive information Storage on	Limit data storage at designated systems Field level protection for sensitive information Storage on	Limit data storage at designated systems Field level protection for sensitive information Segmentation of	Limit data storage at designated systems Field level protection for sensitive information Segmentation of	Limit data storage at designated systems Segmentation of access path to the information Protection for data-in-use as

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	personally owned/ external media prohibited Segmentation of access path to the information Protection for data-in-use as well as archived Full disk encryption Data masking while providing access to information Restricted access to database Protection of database access credentials Encryption of fields Connection to the public network is not allowed Access to public mail is not allowed Monitoring of email inbound and outbound connections Chat, messaging and access to message/file transferring files not allowed Storage on external media not allowed Disable ports connecting to external devices (USB) Authentication, password protection, secure protocol for printing No storage on personally owned devices Restricted & monitored inbound & outbound network connections	personally owned/ external media prohibited Segmentation of access path to the information Protection for data-in-use as well as archived Full disk encryption Data masking while providing access to information Restricted access to database Protection of database access credentials Encryption of fields Connection to the public network is not allowed Access to public mail is not allowed Monitoring of email inbound and outbound connections Chat, messaging and access to message/file transferring files not allowed Storage on external media not allowed Disable ports connecting to external devices (USB) Authentication, password protection, secure protocol for printing No storage on personally owned devices Restricted & monitored inbound & outbound network connections	access path to the information Protection for data-in-use as well as archived Data masking while providing access to information Restricted access to database Protection of database access credentials Encryption of fields Monitoring of email inbound and outbound connections Disable ports connecting to external devices (USB) Authentication, password protection, secure protocol for printing Restricted & monitored inbound & outbound network connections Strict adherence to labeling for backup Integrity checks through hash signature Secure disposal of media 2 years retention of data ---------- G38, G39 C86, C87, C88, C89, C90, C91, C92, C93 IG86, IG86 (b), (c),	access path to the information Protection for data-in-use as well as archived Restricted access to database Protection of database access credentials Encryption of fields Monitoring of email inbound and outbound connections Restricted inbound & outbound network connections Strict adherence to labeling for backup Integrity checks through hash signature Secure disposal of media 2 years retention of data ---------- G38, G39 C86, C87, C88, C89, C90, C91, C92, C93 IG86, IG86 (b), (c), IG88, IG88 (a), (b), (c), (d), (e) IG91, IG91 (a), (c), (d), (e) IG92, IG92 (a), (b), (c), (f) IG93, IG93 (a), (b), (c), (d), (e), (f)	well as archived Restricted access to database Protection of database access credentials Restricted inbound & outbound network connections Strict adherence to labeling for backup Integrity checks through hash signature

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	Strict adherence to labeling for backup Integrity checks through hash signature AES 256 bit encryption of backup Secure disposal of storage devices 2 years retention of data --- G38, G39 C86, C87, C88, C89, C90, C91, C92, C93 IG86, IG86 (a), (b), (c), (d) IG87 IG88, IG88 (a), (b), (c), (d), (e) IG89, IG89 (a), (b), (d) IG90, IG90 (a), (b), (c), (d), (e), (f), (g) IG91, IG91 (a), (b), (c), (d), (e) IG92, IG92 (a), (b), (c), (e), (f) IG93, IG93 (a), (b), (c), (d), (e), (f)	Strict adherence to labeling for backup Integrity checks through hash signature AES 128 bit encryption of backup Secure disposal of media 2 years retention of data --- G38, G39 C86, C87, C88, C89, C90, C91, C92, C93 IG86, IG86 (a), (b), (c), (d) IG87 IG88, IG88 (a), (b), (c), (d), (e) IG89, IG89 (a), (b), (d) IG90, IG90 (a), (b), (c), (d), (e), (f), (g) IG91, IG91 (a), (b), (c), (d), (e) IG92, IG92 (a), (b), (c), (d), (f) IG93, IG93 (a), (b), (c), (d), (e), (f)	IG87 IG88, IG88 (a), (b), (c), (d), (e) IG89, IG89 (c), (d) IG90, IG90 (a), (b), (c), (d), (e), (f), (g) IG91, IG91 (b), (c), (d), (e) IG92, IG92 (a), (b), (c), (f) IG93, IG93 (a), (b), (c), (d), (e), (f)		
Third party access	Block access to third party unless it is required Contract incorporating security Background verification Security clearance process Mechanism for third party assurance Restricted access in third party environment	Block access to third party unless it is required Contract incorporating security Background verification & security clearance Mechanism for third party assurance Restricted access in third party environment ---	Contract incorporating security Mechanism for third party assurance Restricted access in third party environment --- G40 C94 IG94, IG94 (a), (b), (e), (f)	Contract incorporating security Mechanism for third party assurance Restricted access in third party environment --- G40 C94 IG94, IG94 (a), (b), (e), (f)	Contract incorporating security Mechanism for third party assurance --- G40 C94 IG94, IG94 (a), (b), (e)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	---------- G40 C94 IG94, IG94 (a), (b), (c), (d), (e), (f)	G40 C94 IG94, IG94 (a), (b), (c), (e), (f)			
Monitoring & review	Logging of access of fields, files & databases Tracking behavior people & systems Real time log monitoring SIEM implementation Data security dashboard ---------- G41 C95 IG95, IG95 (a), (b), (c), (d), (e), (f), (g), (h)	Logging of access of fields, files & databases Tracking behavior people & systems Daily log monitoring SIEM implementation Data security dashboard ---------- G41 C95 IG95, IG95 (a), (b), (c), (d), (e), (f), (g), (h)	Logging of access of fields, files & databases Tracking behavior people & systems Frequent log monitoring ---------- G41 C95 IG95, IG95 (a), (b), (c), (d), (e)	Logging of access of fields, files & databases Tracking behavior people & systems Frequent log monitoring ---------- G41 C95 IG95, IG95 (a), (b), (c), (d), (e)	Logging of access of fields, files & databases Tracking behavior people & systems Frequent log monitoring ---------- G41 C95 IG95, IG95 (a), (b), (c), (d), (e)
Breach management	Mechanism to identify incident or breach Categories of incident & escalation matrix Remediation workflow SIEM implementation Authority notification process ---------- G42 C96 IG96, IG96 (a), (b), (c), (d), (e), (f)	Mechanism to identify incident or breach Categories of incident & escalation matrix Remediation workflow SIEM implementation Authority notification process ---------- G42 C96 IG96, IG96 (a), (b), (c), (d), (e), (f)	Process to identify incident or breach Categories of incident & escalation matrix Authority notification process ---------- G42 C96 IG96, IG96 (a), (b), (c), (f)	Process to identify incident or breach Authority notification process ---------- G42 C96 IG96, IG96 (a),(f)	Process to identify incident or breach Authority notification process ---------- G42 C96 IG96, IG96 (a),(f)
Personnel security					
Awareness & training	Bi-annual training based on role/ function Training by subject matter experts Measure training	Bi-annual training based on role/ function Training by subject matter experts Measure training	Bi-annual training based on role/ function Measure training effectiveness Bi-annual review of training	Bi-annual awareness training Knowledge of threats, vulnerabilities Security procedures,	Bi-annual awareness training Knowledge of threats, vulnerabilities Security

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	effectiveness Bi-annual review of training courseware Quarterly awareness training Controlling, storing, managing and secure disposal of information Knowledge of threats, vulnerabilities Security procedures, policies ---------------- G43 C97 IG97, IG97 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j)	effectiveness Bi-annual review of training courseware Quarterly awareness training Controlling, storing, managing and secure disposal of information Knowledge of threats, vulnerabilities Security procedures, policies ---------------- G43 C97 IG97, IG97 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j)	courseware Quarterly awareness training Controlling, storing, managing and secure disposal of information Knowledge of threats, vulnerabilities Security procedures, policies ---------------- G43 C97, IG97, IG97 (a), (b), (d), (e), (f), (g), (h), (i), (j)	policies ---------------- G43 C97 IG97, IG97 (g), (h), (i), (j)	procedures, policies ---------------- G43 C97 IG97, IG97 (g), (h), (i), (j)
Employee verification	Authorized/ competent agency verification only Complete background check Security clearance from competent agency ---------------- G44 C98 IG98, IG98 (a), (b), (c)	Authorized/ competent agency verification only Complete background check Security clearance from competent agency ---------------- G44 C98 IG98, IG98 (a), (b), (c)	Authorized/ competent agency verification only Complete background check Security clearance from competent agency ---------------- G44 C98 IG98, IG98 (a), (b), (c)	Authorized/ competent agency verification only Complete background check Security clearance from competent agency ---------------- G44 C98 IG98, IG98 (a), (b), (c)	Authorized/ competent agency verification only Complete background check Security clearance from competent agency ---------------- G44 C98 IG98, IG98 (a), (b), (c)
Authorizing access to third parties	Role, function performed and need for third party access Recent background check and verification Documented request from head of department Strict monitoring of	Role, function performed and need for third party access Recent background check and verification Documented request from head of department Strict monitoring	Role, function performed and need for third party access Recent background check and verification Documented request from head of department Monitoring of	Role, function performed and need for third party access Recent background check and verification Documented request from head of department Monitoring of	Role, function performed and need for third party access Recent background check and verification Documented request from head of department Compliance with

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	activity Strict monitoring of physical access Compliance with security policy External media not allowed Strict disciplinary process ---------------- G45 C99, C101 IG99, IG99 (a), (b), (c), (d), (e), (f) IG101, IG101 (a),	of activity Strict monitoring of physical access Compliance with security policy External media not allowed Strict disciplinary process ---------------- G45 C99, C101 IG99, IG99 (a), (b), (c), (d), (e), (f) IG101, IG101 (a),	activity Compliance with security policy External media allowed Strict disciplinary process ---------------- G45 C99, C101 IG99, IG99 (a), (b), (c), (e), (f) IG101, IG101 (a),	activity Compliance with security policy External media allowed Strict disciplinary process ---------------- G45 C99, C101 IG98, IG98 (a), (b), (c), (e), (f) IG101, IG101 (a),	security policy External media allowed Disciplinary process ---------------- G45 C99, C101 IG99, IG99 (a), (b), (e), (f) IG101, IG101 (a),
Record of authorized users	User access authorization User details Record of background check Permitted access within office/ facility Registered/ allocated devices ---------------- G46 C102 IG102, (a), (b), (c), (d), (e), (f)	User access authorization User details Record of background check Permitted access within office/ facility Registered/ allocated devices ---------------- G46 C102 IG102, (a), (b), (c), (d), (e), (f)	User access authorization User details Record of background check Permitted access within office/ facility Registered/ allocated devices ---------------- G46 C102 IG102, (a), (b), (c), (d), (e), (f)	User access authorization User details Record of background check Permitted access within office/ facility Registered/ allocated devices ---------------- G46 C102 IG102, (a), (b), (c), (d), (e), (f)	User access authorization User details Record of background check Permitted access within office/ facility Registered/ allocated devices ---------------- G46 C102 IG102, (a), (b), (c), (d), (e), (f)
Acceptable usage policy	Limit information use to defined purpose Deploy system for intended use Protect from disclosure User acceptance ---------------- G47 C100 IG100, (a), (b), (c),	Limit information use to defined purpose Deploy system for intended use Protect from disclosure User acceptance ---------------- G47 C100 IG100, (a), (b), (c),	Limit information use to defined purpose Deploy system for intended use Protect from disclosure User acceptance ---------------- G47 C100 IG100, (a), (b), (c),	Limit information use to defined purpose Deploy system for intended use Protect from disclosure User acceptance ---------------- G47 C100 IG100, (a), (b), (c),	Limit information use to defined purpose Deploy system for intended use Protect from disclosure User acceptance ---------------- G47 C100 IG100, (a), (b), (c),
Monitoring and review	Monitoring of area visited, time of access, activity	Monitoring of area visited, time of access, activity	Monitoring of area visited, time of access, activity	Monitoring of area visited, time of access, activity	Monitoring of area visited, time of access, activity

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	performed Correlation with access privileges ---------------- G48 C103 IG103, IG103 (a)	performed Correlation with access privileges ---------------- G48 C103 IG103, IG103 (a)	performed Correlation with access privileges ---------------- G48 C103 IG103, IG103 (a)	performed Correlation with access privileges ---------------- G48 C103 IG103, IG103 (a)	performed Correlation with access privileges ---------------- G48 C103 IG103, IG103 (a)
Limiting exposure of information	Non-disclosure agreement Contractual liability of employee/ third party personnel Incident communication strictly to top management ---------------- G49 C104, C105, C106 IG104, IG104 (a) IG105, IG105 (a), (b) IG106, IG106 (a), (b), (c)	Non-disclosure agreement Contractual liability of employee/ third party personnel Incident communication strictly to top management ---------------- G49 C104, C105, C106 IG104, IG104 (a) IG105, IG105 (a), (b) IG106, IG106 (a), (b), (c)	Non-disclosure agreement Contractual liability of employee/ third party personnel Incident communication strictly to top management ---------------- G49 C104, C105, C106 IG104, IG104 (a) IG105, IG105 (a), (b) IG106, IG106 (a), (b), (c)	Non-disclosure agreement Contractual liability of employee/ third party personnel Incident communication strictly to top management ---------------- G49 C104, C105, C106 IG104, IG104 (a) IG105, IG105 (a), (b) IG106, IG106 (a), (b), (c)	Contractual liability of employee/ third party personnel Incident communication restricted within concerned parties ---------------- G49 C105, C106 IG105, IG105 (a), (b) IG106, IG106 (a), (b), (c)
Threat and vulnerability management					
Interdependence of assets & systems	Replacement with SAG tested components Addition of SAG tested components Backward and forward compatibility ---------------- G50 C107 IG107, IG107 (a), (b)	Replacement with SAG tested components Addition of SAG tested components Backward and forward compatibility ---------------- G50 C107 IG107, IG107 (a), (b)	Replacement with globally tested components Addition of globally tested components Backward and forward compatibility ---------------- G50 C107 IG107, IG107 (a), (b)	Replacement with globally tested components Addition of globally tested components Backward and forward compatibility ---------------- G50 C107 IG107, IG107 (a), (b)	Replacement with globally tested components Addition of globally tested components Backward and forward compatibility ---------------- G50 C107 IG107, IG107 (a), (b)
Standardized operating environment	Limit diversity of endpoints Secure operating system SAG tested servers	Limit diversity of endpoints Secure operating system SAG tested servers	Limit diversity of endpoints Secure operating system Globally tested	Limit diversity of endpoints Secure operating system Globally tested	Secure operating system Globally tested servers and platforms

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	and platforms SAG tested network devices Uniform database type Network Operation Center (NOC) and Security Operations Center (SOC) ---------- G51 C108 IG108, IG108 (a), (b), (c), (d), (e), (f), (g)	and platforms SAG tested network devices Uniform database type Network Operation Center (NOC) and Security Operations Center (SOC) ---------- G51 C108 IG108, IG108 (a), (b), (c), (d), (e), (f), (g)	servers and platforms Globally tested network devices Uniform database type Network Operation Center (NOC) and Security Operations Center (SOC) ---------- G51 C108 IG108, IG108 (a), (b), (c), (d), (e), (f), (g)	servers and platforms Globally tested network devices Uniform database type ---------- G51 C108 IG108, IG108 (a), (b), (c), (d), (e), (f)	Globally tested network devices Uniform database type ---------- G51 C108 IG108, IG108 (b), (c), (d), (e), (f)
Including TVM in change management	Assessment of possible threat vectors Vulnerability assessment of configuration of devices and systems Assessment of inherent vulnerability of new infrastructure Integration with established identification, authorization and authentication policies ---------- G52 C109 IG109, IG109 (a), (b), (c), (d)	Assessment of possible threat vectors Vulnerability assessment of configuration of devices and systems Assessment of inherent vulnerability of new infrastructure Integration with established identification, authorization and authentication policies ---------- G52 C109 IG109, IG109 (a), (b), (c), (d)	Assessment of possible threat vectors Integration with established identification, authorization and authentication policies ---------- G52 C109 IG109, IG109 (a), (d)	Assessment of possible threat vectors Integration with established identification, authorization and authentication policies ---------- G52 C109 IG109, IG109 (a), (d)	Assessment of possible threat vectors ---------- G52 C109 IG109, IG109 (a)
Identification of external intelligence sources	Intelligence about emerging threats, vulnerabilities, bugs and exploits Mix of various sources Integrate external intelligence with risk management	Intelligence about emerging threats, vulnerabilities, bugs and exploits Mix of various sources Integrate external intelligence with risk management	Intelligence about emerging threats, vulnerabilities, bugs and exploits ---------- G53 C110 IG110, IG110 (a),	Intelligence about emerging threats, vulnerabilities, bugs and exploits ---------- G53 C110 IG110, IG110 (a),	Intelligence about emerging threats, vulnerabilities, bugs and exploits ---------- G53 C110 IG110, IG110 (a)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	---------- G53 C110 IG110, IG110 (a), (b), (c)	---------- G53 C110 IG110, IG110 (a), (b), (c)			
Intelligence gathering	Discover vulnerability of existing systems and device Maintain repository of known vulnerabilities Protect against known vulnerabilities Quarterly vulnerability assessment of entire system Ad-hoc vulnerability assessment of key systems Vulnerability assessment prior to change Vulnerability due to third party system integration Information from third parties ---------- G54 C111, C112, C113 IG111, IG111 (a), (b), (c), (d) IG112, IG112 (a), (b) IG113	Discover vulnerability of existing systems and device Maintain repository of known vulnerabilities Protect against known vulnerabilities Quarterly vulnerability assessment of entire system Ad-hoc vulnerability assessment of key systems Vulnerability assessment prior to change Vulnerability due to third party system integration Information from third parties ---------- G54 C111, C112, C113 IG111, IG111 (a), (b), (c), (d) IG112, IG112 (a), (b) IG113	Discover vulnerability of existing systems and device Maintain repository of known vulnerabilities Protect against known vulnerabilities Bi-annual vulnerability assessment of entire system Vulnerability assessment prior to change Vulnerability due to third party system integration Information from third parties ---------- G54 C111, C112, C113 IG111, IG111 (a), (b), (c), (d) IG112, IG112 (a), IG113	Discover vulnerability of existing systems and device Maintain repository of known vulnerabilities Protect against known vulnerabilities Bi-annual vulnerability assessment of entire system Vulnerability assessment prior to change Vulnerability due to third party system integration Information from third parties ---------- G54 C111, C112, C113 IG111, IG111 (a), (b), (c), (d) IG112, IG112 (a) IG113	Discover vulnerability of existing systems and device Maintain repository of known vulnerabilities Protect against known vulnerabilities Bi-annual vulnerability assessment of entire system Vulnerability due to third party system integration ---------- G54 C111, C112, C113 IG111, IG111 (a), (b), (c) IG112, IG112 (a) IG113
Technical policies	Customization of default security profile Implement system level security policies Disable unused physical interfaces	Customization of default security profile Implement system level security policies Disable unused physical interfaces	Customization of default security profile Implement system level security policies Disable unused physical interfaces	Customization of default security profile Implement system level security policies Disable unused physical interfaces	Implement system level security policies Use SSL/TLS for transmission over the network Remote management

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	Use TLS 1.2 or above for transmission over the network Implement access control list Restrict remote management Monitor security bulletins Remove unnecessary applications Enable system scanning Enable event and activity logging Install antivirus, anti-malware, endpoint firewall Regular update of security patches Active directory Fraud protection Vulnerability scanning tools (host and network based) ---------- G55 C114, C115, C116, C117, C118, C119, C120 IG114, IG114 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j) IG115 (a), (b) IG116 (a) IG117 IG118 IG119 IG120, IG120 (a), (b), (c), (d)	Use TLS 1.2 or above for transmission over the network Implement access control list Restrict remote management Monitor security bulletins Remove unnecessary applications Enable system scanning Enable event and activity logging Install antivirus, anti-malware, endpoint firewall Regular update of security patches Active directory Fraud protection Vulnerability scanning tools (host and network based) ---------- G55 C114, C115, C116, C117, C118, C119, C120 IG114, IG114 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j) IG115 (a), (b) IG116 (a) IG117 IG118 IG119 IG120, IG120 (a), (b), (c), (d)	Use TLS 1.2 or above for transmission over the network Implement access control list Remote management allowed Remove unnecessary applications Enable event and activity logging Install antivirus, anti-malware, endpoint firewall Regular update of security patches Fraud protection ---------- G55 C114, C115, C116, C117, C120 IG114, IG114 (b), (c), (d), (e), (f), (h), (i), (j) IG115 (a), (b) IG116 (a) IG117 IG120, IG120 (a), (b), (c), (d)	Use SSL/TLS for transmission over the network Remote management allowed Remove unnecessary applications Enable event and activity logging Install antivirus, anti-malware, endpoint firewall Regular update of security patches Fraud protection ---------- G55 C114, C115, C116, C119, C120 IG114, IG114 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k) IG115 (a), (b) IG116 (a) IG120	allowed Remove unnecessary applications Enable system scanning Enable event and activity logging Install antivirus, anti-malware, endpoint firewall Regular update of security patches ---------- G55 C114, C115, C116, C119, C120 IG114, IG114 (c), (e), (i), (j), (k) IG115 (a), (b) IG116 (a) IG120

Area	Top secret	Secret	Confidential	Restricted	Unclassified
Security monitoring & incident management					
Incidence response coverage	Real time event, activity, system monitoring Monitor hosts, network traffic, logs Traffic inspection Transaction inspection Correlation of access patterns Anomaly detection Dedication incident response team Top priority incident resolution Preventive and detective security capability Identity management systems Segregate and isolate system in-case of incident Remove access to system in-case of incident ---------- G56 C121, C122, C123, C124 IG121, IG121 (a), (b), (c), (d), (e), (f), IG122, IG 122 (a), (b) IG123, IG 123 (a), (b), (c), (d), (e), (f), (g) IG124, IG 124 (a), (b), (c), (d), (e), (f), (g), (h)	Real time event, activity, system monitoring Monitor hosts, network traffic, logs Traffic inspection Transaction inspection Correlation of access patterns Anomaly detection Dedication incident response team Top priority incident resolution Preventive and detective security capability Identity management systems Segregate and isolate system in-case of incident Remove access to system in-case of incident ---------- G56 C121, C122, C123, C124 IG121, IG121 (a), (b), (c), (d), (e), (f), IG122, IG 122 (a), (b) IG123, IG 123 (a), (b), (c), (d), (e), (f), (g) IG124, IG 124 (a), (b), (c), (d), (e), (f), (g), (h)			
Breach scenarios	Record of known vulnerabilities Post incidence analysis	Record of known vulnerabilities Post incidence analysis	Record of known vulnerabilities Post incidence analysis	Record of known vulnerabilities Post incidence analysis	Record of known vulnerabilities Post incidence analysis

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	Correlation with previous incidents Potential breach scenarios Remediation measures Forensic analysis ---------------- G57 C125 IG125, IG125 (a), (b), (c)	Correlation with previous incidents Potential breach scenarios Remediation measures Forensic analysis ---------------- G57 C125 IG125, IG125 (a), (b), (c)	Correlation with previous incidents Potential breach scenarios Remediation measures Forensic analysis ---------------- G57 C125 IG125, IG125 (a), (b), (c)	Remediation measures ---------------- G57 C125 IG125, IG125 (a), (b)	Remediation measures ---------------- G57 C125 IG125, IG125 (a), (b)
Security intelligence information	Log of activity, event, transaction Security incident and event monitoring External intelligence ---------------- G58 C126 IG126, IG126 (a), (b)	Log of activity, event, transaction Security incident and event monitoring External intelligence ---------------- G58 C126 IG126, IG126 (a), (b)	Log of activity, event, transaction Security incident and event monitoring External intelligence ---------------- G58 C126 IG126, IG126 (a), (b)	Log of activity, event, transaction ---------------- G58 C126 IG126, IG126 (a)	Log of activity, event, transaction ---------------- G58 C126 IG126, IG126 (a)
Enterprise log management	Secure management of logs Restricted access to logs Integrity protection of log information Standardized format of logs Log of all activity and events Log retention for 2 years (or as per sector specific laws/regulations) Time stamping as per central time server ---------------- G59 C127, C128, C129, C130, C131 IG127, IG127 (a),	Secure management of logs Restricted access to logs Integrity protection of log information Standardized format of logs Log of all activity and events Log retention for 2 years (or as per sector specific laws/regulations) Time stamping as per central time server ---------------- G59 C127, C128, C129, C130	Secure management of logs Restricted access to logs Integrity protection of log information Standardized format of logs Log of all activity and events Log retention for 1 year (or as per sector specific laws/regulations) Time stamping as per central time server ---------------- G59 C127, C128, C129, C130	Secure management of logs Restricted access to logs Integrity protection of log information Standardized format of logs Log of all activity and events Log retention for 1 year (or as per sector specific laws/regulations) Time stamping as per central time server ---------------- G59 C127, C128, C129, C130	Secure management of logs Restricted access to logs Integrity protection of log information Standardized format of logs Log of all activity and events Log retention for 1 year (or as per sector specific laws/regulations) Time stamping as per central time server ---------------- G59 C127, C128, C129, C130

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	(b), (c) IG128, IG 128 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (r), (s), (t), (u), (v) IG129 IG130, IG130 (a), (b), (c) IG131, IG131 (a), (b), (c), (d), (e), (f)	IG127, IG127 (a), (b), (c) IG128, IG 128 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (r), (s), (t), (u), (v) IG129 IG130, IG130 (a), (b), (c)	IG127, IG127 (a), (b), (c) IG128, IG 128 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (r), (s), (t), (u), (v) IG129 IG130, IG130 (a), (b), (c)	IG127, IG127 (a), (b), (c) IG128, IG 128 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (r), (s), (t), (u), (v) IG129 IG130, IG130 (a), (b), (c)	IG127, IG127 (a), (b), (c) IG128, IG 128 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (r), (s), (t), (u), (v) IG129 IG130, IG130 (a), (b), (c)
Deployment of skilled resources	Technical expertise in incidence evaluation Clear identification of roles Simulation training of potential incidents Competent cyber forensics and investigation practice ---------------- G60 C132 IG132, IG 132 (a), (b), (c), (d)	Technical expertise in incidence evaluation Clear identification of roles Simulation training of potential incidents Competent cyber forensics and investigation practice ---------------- G60 C132 IG132, IG 132 (a), (b), (c), (d)	Technical expertise in incidence evaluation Clear identification of roles Competent cyber forensics and investigation practice ---------------- G60 C132 IG132, IG 132 (a), (b), (c), (d)	Technical expertise in incidence evaluation Clear identification of roles ---------------- G60 C132 IG132, IG 132 (a), (b), (c), (d)	Technical expertise in incidence evaluation Clear identification of roles ---------------- G60 C132 IG132, IG 132 (a), (b), (c), (d)
Disciplinary action	Liability of employee or authorized third party personnel or entity ---------------- G61 C122 IG122, IG 122 (c), (d)	Liability of employee or authorized third party personnel or entity ---------------- G61 C122 IG122, IG 122 (c), (d)	Liability of employee or authorized third party personnel or entity ---------------- G61 C122 IG122, IG 122 (c), (d)	Liability of employee or authorized third party personnel or entity ---------------- G61 C122 IG122, IG 122 (c), (d)	Liability of employee or authorized third party personnel or entity ---------------- G61 C122 IG122, IG 122 (c), (d)
Structure & responsibility	Liability of employee or authorized third party personnel or entity ----------------	Liability of employee or authorized third party personnel or entity ----------------	Liability of employee or authorized third party personnel or entity ----------------	Liability of employee or authorized third party personnel or entity ----------------	Liability of employee or authorized third party personnel or entity ----------------

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	G62 C122, C125 IG122, IG 122 (c), (d) IG125, IG 125 (a), (b)	G62 C122, C125 IG122, IG 122 (c), (d) IG125, IG 125 (a), (b)	G62 C122, C125 IG122, IG 122 (c), (d) IG125, IG 125 (a), (b)	G62 C122, C125 IG122, IG 122 (c), (d) IG125, IG 125 (a), (b)	G62 C122, C125 IG122, IG 122 (c), (d) IG125, IG 125 (a), (b)
Incident management awareness and training	Quarterly training of users ---------------- G63 C123 IG123, IG123 (g), (h)	Quarterly training of users ---------------- G63 C123 IG123, IG123 (g), (h)	Bi-annual training of users ---------------- G63 C123 IG123, IG123 (g), (h)	Bi-annual training of users ---------------- G63 C123 IG123, IG123 (g), (h)	Bi-annual training of users ---------------- G63 C123 IG123, IG123 (g), (h)
Communication of incidents	Log information sharing only with authorized law enforcement agencies/ bodies under formal written notice or court orders Sharing of breach information with Information Security Steering committee (ISSC), sectorial CERT teams and CERT- In ---------------- G64 C134, C135 IG 134 IG135	Log information sharing only with authorized law enforcement agencies/ bodies under formal written notice or court orders Sharing of breach information with Information Security Steering committee (ISSC), sectorial CERT teams and CERT-In ---------------- G64 C134, C135 IG 134 IG135	Log information sharing only with authorized law enforcement agencies/ bodies under formal written notice or court orders Sharing of breach information with Information Security Steering committee (ISSC), sectorial CERT teams and CERT-In ---------------- G64 C134, C135 IG 134 IG135	Log information sharing only with authorized law enforcement agencies/ bodies under formal written notice or court orders Sharing of breach information with Information Security Steering committee (ISSC), sectorial CERT teams and CERT-In ---------------- G64 C134, C135 IG 134 IG135	Log information sharing only with authorized law enforcement agencies/ bodies under formal written notice or court orders Sharing of breach information with Information Security Steering committee (ISSC), sectorial CERT teams and CERT-In ---------------- G64 C134, C135 IG 134 IG135
Cloud computing					
Security considerations in contract	Not permitted on cloud platform ---------------- G65 IG136	Not permitted on cloud platform ---------------- G65 IG136	Contractual liability of service provider for data security Stringent non-disclosure agreements Right to audit service provider Availability of customized logs ----------------	Contractual liability of service provider for data security Stringent non-disclosure agreements Right to audit service provider Availability of customized logs ----------------	Contractual liability of service provider for data security Stringent non-disclosure agreements Right to audit service provider Availability of customized logs ----------------

Area	Top secret	Secret	Confidential	Restricted	Unclassified
			G65 IG136, IG136 (a), (b), (c), (d)	G65 IG136, IG136 (a), (b), (c), (d)	G65 IG136, IG136 (a), (b), (c), (d)
Alignment of security policies	Not permitted on cloud platform --- G66 IG137	Not permitted on cloud platform --- G66 IG137	Alignment with organizations security policy Service provider to provide updated process documentation, configuration standards, training records, incident response plans Compliance certificates and report as per global standards --- G66 IG137, IG137 (a), (b),	Alignment with organizations security policy Service provider to provide updated process documentation, configuration standards, training records, incident response plans Compliance certificates and report as per global standards --- G66 IG137, IG137 (a), (b),	Alignment with organizations security policy Service provider to provide updated process documentation, configuration standards, training records, incident response plans Compliance certificates and report as per global standards --- G66 IG137, IG137 (a), (b),
Data security in cloud environment	Not permitted on cloud platform --- G67 IG138	Not permitted on cloud platform --- G67 IG138	*For service provider:* Security assessment prior to patch deployment Third part assessment of service provider Prohibit sharing of racks or physical infra Segregation from other tenants --- G67 IG138, IG138 (a), (b), (c), (d), (e)	*For service provider:* Security assessment prior to patch deployment Third part assessment of service provider Prohibit sharing of racks or physical infra Segregation from other tenants --- G67 IG138, IG138 (a), (b), (c), (d), (e)	*For service provider:* Security assessment prior to patch deployment Third part assessment of service provider Segregation from other tenants --- G67 IG138, IG138 (a), (b), (e)
Authentication in cloud environment	Not permitted on cloud platform --- G68 IG139	Not permitted on cloud platform --- G68 IG139	*For service provider:* authentication and authorization on logical access --- G68 IG139	*For service provider:* authentication and authorization on logical access --- G68 IG139	*For service provider:* authentication and authorization on logical access --- G68 IG139

Area	Top secret	Secret	Confidential	Restricted	Unclassified
Continuity of operations	Not permitted on cloud platform --- G69 IG140	Not permitted on cloud platform --- G69 IG140	Migrate data to other service provider Secure deletion of data --- G69 IG140	Migrate data to other service provider Secure deletion of data --- G69 IG140	Migrate data to other service provider Secure deletion of data --- G69 IG140
Definition of roles and responsibilities	Not permitted on cloud platform --- G70 IG141	Not permitted on cloud platform --- G70 IG141	*For service provider:* Segregation of duties and job roles Role based training Security training and awareness Non- disclosure agreement --- G70 IG141, IG141 (a), (b)	*For service provider:* Role based training Security training and awareness Non- disclosure agreement --- G70 IG141 (a), (b)	*For service provider:* Role based training Security training and awareness Non- disclosure agreement --- G70 IG141 (a), (b)
Security monitoring	Not permitted on cloud platform --- G71 IG142	Not permitted on cloud platform --- G71 IG142	*For service provider:* Continuous security monitoring of cloud environment Incident management mechanism --- G71 IG142, IG142 (a)	*For service provider:* Continuous security monitoring of cloud environment Incident management mechanism --- G71 IG142, IG142 (a)	*For service provider:* Continuous security monitoring of cloud environment Incident management mechanism --- G71 IG142, IG142 (a)
Availability of logs	Not permitted on cloud platform --- G72 IG143	Not permitted on cloud platform --- G72 IG143	*For service provider:* Availability of event, activity, access, maintenance, change, upgrade logs --- G72	*For service provider:* Availability of event, activity, access, maintenance, change, upgrade logs --- G72	*For service provider:* Availability of event, activity, access, maintenance, change, upgrade logs --- G72

Area	Top secret	Secret	Confidential	Restricted	Unclassified
			IG143	IG143	IG143
Third party security assessments	Not permitted on cloud platform --- G73 IG144	Not permitted on cloud platform --- G73 IG144	Bi-annual third party security assessment and audits --- G73 IG144	Bi-annual third party security assessment and audits --- G73 IG144	Annual third party security assessment and audits --- G73 IG144
Data security	Not permitted on cloud platform --- G74 IG145	Not permitted on cloud platform --- G74 IG145	AES 256-bit encryption VPN over TLS or IPSEC --- G74 IG145	AES 256-bit encryption VPN over SSL --- G74 IG145	AES 256-bit encryption VPN over SSL --- G74 IG145
Use of authorized cloud services	Not permitted on cloud platform --- G75 IG146	Not permitted on cloud platform --- G75 IG146	Authorized service providers Government cloud services --- G75 IG146	Authorized service providers Government cloud services --- G75 IG146	Authorized service providers Government cloud services --- G75 IG146
Mobility and BYOD					
Mobile device policy	Not permitted on mobile platform --- G76 IG147	Not permitted on mobile platform --- G76 IG147	Not permitted on mobile platform --- G76 IG147	User provisioning User de-provisioning Device usage List of authorized devices Data control mechanism Security requirement – Mobile device management (MDM) Secure device configuration Allowed services --- G76 IG147, IG 147 (a), (b), (c), (d), (e), (f), (g), (h), (i)	User provisioning User de-provisioning Device usage List of authorized devices Data control mechanism Security requirement – Mobile device management (MDM) Secure device configuration Allowed services --- G76 IG147, IG 147 (a), (b), (c), (d), (e), (f), (g), (h), (i)

Area	Top secret	Secret	Confidential	Restricted	Unclassified
Risk evaluation of devices	Not permitted on mobile platform --- G77 IG148	Not permitted on mobile platform --- G77 IG148	Not permitted on mobile platform --- G77 IG148	Security testing of devices Vulnerability scan Device patch management --- G76 IG147, IG 147 (a)	Security testing of devices Vulnerability scan Device patch management --- G76 IG147, IG 147 (a)
Allocation of mobile devices	Not permitted on mobile platform --- G78 IG147	Not permitted on mobile platform --- G78 IG147	Not permitted on mobile platform --- G78 IG147	User device registration Device security configuration --- G78 IG147	User device registration Device security configuration --- G78 IG147
Device lifecycle management and governance	Not permitted on mobile platform --- G79 IG149	Not permitted on mobile platform --- G79 IG149	Not permitted on mobile platform --- G79 IG149	Enforce policies for application access, password management, Create encrypted container for official information Monitor device health Antivirus and firewall installation Secure deletion of information on de-provisioning --- G79 IG149, IG149 (a), (b), (c), (d), (e)	Enforce policies for application access, password management, Create encrypted container for official information Monitor device health Antivirus and firewall installation Secure deletion of information on de-provisioning --- G79 IG149, IG149 (a), (b), (c), (d), (e)
Data transmission and storage	Not permitted on mobile platform --- G80 IG150	Not permitted on mobile platform --- G80 IG150	Not permitted on mobile platform --- G80 IG150	Device storage encryption Access authorization 2 factor authentication to applications	Device storage encryption Access authorization 2 factor authentication to applications

Area	Top secret	Secret	Confidential	Restricted	Unclassified
				Limited device management privileges Restricted access to open networks Remote wipe and secure deletion of data Limited installation of third party applications Daily backup of official information --- G80 IG150, IG150 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k)	Limited device management privileges Restricted access to open networks Remote wipe and secure deletion of data Limited installation of third party applications Daily backup of official information --- G80 IG150, IG150 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k)
Awareness	Not permitted on mobile platform --- G81 IG151	Not permitted on mobile platform --- G81 IG151	Not permitted on mobile platform --- G81 IG151	Mobile security awareness training --- G81 IG151	Mobile security awareness training --- G81 IG151
Virtualization					
Evaluate risks associated with virtual technologies	Documentation of access paths to information Comprehensive risk assessment covering virtualized assets and processes --- G82 IG152, IG152 (a), (b)	Documentation of access paths to information Comprehensive risk assessment covering virtualized assets and processes --- G82 IG152, IG152 (a), (b)	Documentation of access paths to information Comprehensive risk assessment covering virtualized assets and processes --- G82 IG152, IG152 (a), (b)	Documentation of access paths to information Comprehensive risk assessment covering virtualized assets and processes --- G82 IG152	
Strengthen physical access	Physical security measures for virtualized environment Protect admin access to virtual	Physical security measures for virtualized environment Protect admin access to virtual	Physical security measures for virtualized environment Protect admin access to virtual	Physical security measures for virtualized environment Protect admin access to virtual	

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	systems ---------------- G83 IG153, IG153 (a)	systems ---------------- G83 IG153, IG153 (a)	systems ---------------- G83 IG153, IG153 (a)	systems ---------------- G83 IG153, IG153 (a)	
Segregation of virtual traffic	Segregation of virtual traffic through Virtual LAN, routers and switches ---------------- G84 IG154	Segregation of virtual traffic through Virtual LAN, routers and switches ---------------- G84 IG154	Segregation of virtual traffic through Virtual LAN, routers and switches ---------------- G84 IG154	Segregation of virtual traffic through Virtual LAN, routers and switches ---------------- G84 IG154	
Implement defense in depth	Establish trust zones for different environments Role based access control Adherence to secure configuration practices Diligent patch management ---------------- G85 IG155, IG155 (a), (b), (c), (d)	Establish trust zones for different environments Role based access control Adherence to secure configuration practices Diligent patch management ---------------- G85 IG155, IG155 (a), (b), (c), (d)	Establish trust zones for different environments Role based access control Adherence to secure configuration practices Diligent patch management ---------------- G85 IG155, IG155 (a), (b), (c), (d)	Establish trust zones for different environments Role based access control Adherence to secure configuration practices Diligent patch management ---------------- G85 IG155	
Harden the virtualization management console	Protect root access Defense against MAC spoofing Standard configuration Disable unused ports and services Disable cross-platform data transfer Restricted and monitored connections ---------------- G86 IG156, IG156 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j)	Protect root access Defense against MAC spoofing Standard configuration Disable unused ports and services Disable cross-platform data transfer Restricted and monitored connections ---------------- G86 IG156, IG156 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j)	Protect root access Defense against MAC spoofing Standard configuration Disable unused ports and services Disable cross-platform data transfer Restricted and monitored connections ---------------- G86 IG156, IG156 (a), (b), (c), (d), (e), (f), (g), (h), (i), (j)	Protect root access Defense against MAC spoofing Standard configuration Disable unused ports and services Disable cross-platform data transfer Restricted and monitored connections ---------------- G86 IG156	

Area	Top secret	Secret	Confidential	Restricted	Unclassified
Vulnerability information	Specific focus on vulnerabilities of virtualized environment ---------------- G87 IG157	Specific focus on vulnerabilities of virtualized environment ---------------- G87 IG157	Specific focus on vulnerabilities of virtualized environment ---------------- G87 IG157	Specific focus on vulnerabilities of virtualized environment ---------------- G87 IG157	
Logging and monitoring	Monitoring of privilege accounts, virtualized image creation instances, unauthorized access attempts, multiple failed login attempts, system lockout, critical file changes ---------------- G88 IG158, IG158 (a)	Monitoring of privilege accounts, virtualized image creation instances, unauthorized access attempts, multiple failed login attempts, system lockout, critical file changes ---------------- G88 IG158, IG158 (a)	Monitoring of privilege accounts, virtualized image creation instances, unauthorized access attempts, multiple failed login attempts, system lockout, critical file changes ---------------- G88 IG158, IG158 (a)	Monitoring of privilege accounts, virtualized image creation instances, unauthorized access attempts, multiple failed login attempts, system lockout, critical file changes ---------------- G88 IG158, IG158 (a)	
Social media					
Limit exposure of official information	No internet facility on systems Strict control over information transmission Strict control over applications used on systems Strictly prohibited from communication over unauthorized channels ---------------- G89 IG159, IG159 (a)	No internet facility on systems Strict control over information transmission Strict control over applications used on systems Strictly prohibited from communication over unauthorized channels ---------------- G89 IG159, IG159 (a)	No internet facility on systems Strict control over information transmission Strict control over applications used on systems Strictly prohibited from communication over unauthorized channels ---------------- G89 IG159, IG159 (a)	No internet facility on systems Strict control over information transmission Strict control over applications used on systems Strictly prohibited from communication over unauthorized channels ---------------- G89 IG159, IG159 (a)	Access permitted to use social media Security testing of third party applications installed on information systems or organization website ---------------- G89 IG159, IG159 (a)
Permitted official use	Protected from all kinds of unauthorized disclosure Strict non-disclosure agreements with employees and third parties	Protected from all kinds of unauthorized disclosure Strict non-disclosure agreements with employees and third parties	Protected from all kinds of unauthorized disclosure Strict non-disclosure agreements with employees and third parties	Protected from all kinds of unauthorized disclosure Strict non-disclosure agreements with employees and third parties	Designated function and authorized person allowed use of social media Training on safety measure for using internet Strict non-

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	---------- G90 IG160 (b)	---------- G90 IG160 (b)	---------- G90 IG160 (b)	---------- G90 IG160 (b)	disclosure agreements with employees and third parties ---------- G90 IG160 (a), (b)
Security testing					
Security evaluation	Availability of tools for network discovery, network post and service identification, vulnerability scanning Evaluation of all systems, networks, applications ---------- G91 IG161, IG161 (a)	Availability of tools for network discovery, network post and service identification, vulnerability scanning Evaluation of all systems, networks, applications ---------- G91 IG161, IG161 (a)	Availability of tools for network discovery, network post and service identification, vulnerability scanning Evaluation of all systems, networks, applications ---------- G91 IG161, IG161 (a)	Availability of tools for network discovery, network post and service identification, vulnerability scanning Evaluation of key systems, networks, applications ---------- G91 IG161, IG161 (a)	Evaluation of all systems, networks, applications ---------- G91 IG161
Testing scenarios	Ongoing scenario testing – insider threat, compromise of perimeter, introduction of malware, vulnerability exploit, perimeter defense, override of security appliances, reconnaissance, enumeration ---------- G92 IG162, IG162 (a), (b)	Ongoing scenario testing – insider threat, compromise of perimeter, introduction of malware, vulnerability exploit, perimeter defense, override of security appliances, reconnaissance, enumeration ---------- G92 IG162, IG162 (a), (b)	Quarterly scenario testing – insider threat, compromise of perimeter, introduction of malware, vulnerability exploit, perimeter defense, override of security appliances, reconnaissance, enumeration ---------- G92 IG162, IG162 (a), (b)	Quarterly scenario testing – insider threat, compromise of perimeter, introduction of malware, vulnerability exploit, perimeter defense, override of security appliances, reconnaissance, enumeration ---------- G92 IG162, IG162 (a), (b)	Bi-annual scenario testing – breach of perimeter defense, override of security appliances, reconnaissance, enumeration ---------- G92 IG162, IG162 (b)
Overt and covert testing	Ongoing black hat testing post approval from HOD/ information owner Ongoing white hat testing post approval from HOD/ information owner ----------	Ongoing black hat testing post approval from HOD/ information owner Ongoing white hat testing post approval from HOD/ information owner ----------	Quarterly black hat testing post approval from HOD/ information owner Quarterly white hat testing post approval from HOD/ information owner ----------	Quarterly black hat testing post approval from HOD/ information owner Quarterly white hat testing post approval from HOD/ information owner ----------	Annual black hat testing post approval from HOD/ information owner Bi - annual white hat testing post approval from HOD/ information owner ----------

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	G93 IG163, IG163 (a), (b)	G93 IG163, IG163 (a), (b)	G93 IG163, IG163 (a), (b)	G93 IG163, IG163 (a), (b)	G93 IG163, IG163 (a), (b)
Vulnerability existence	Validation of discovered vulnerabilities Documentation of discovered vulnerabilities Severity classification of discovered vulnerabilities ---------------- G94 IG164	Validation of discovered vulnerabilities Documentation of discovered vulnerabilities Severity classification of discovered vulnerabilities ---------------- G94 IG164	Validation of discovered vulnerabilities Documentation of discovered vulnerabilities Severity classification of discovered vulnerabilities ---------------- G94 IG164	Validation of discovered vulnerabilities Documentation of discovered vulnerabilities Severity classification of discovered vulnerabilities ---------------- G94 IG164	Validation of discovered vulnerabilities Documentation of discovered vulnerabilities Severity classification of discovered vulnerabilities ---------------- G94 IG164
Security audit					
Determine security auditing requirements	Quarterly meeting with relevant stakeholders such as information owner/ HoD ---------------- G95 IG165, IG165 (a), (b), (c)	Quarterly meeting with relevant stakeholders such as information owner/ HoD ---------------- G95 IG165, IG165 (a), (b), (c)	Bi-annual meeting with relevant stakeholders such as information owner/ HoD ---------------- G95 IG165, IG165 (a), (b), (c)	Bi-annual meeting with relevant stakeholders such as information owner/ HoD ---------------- G95 IG165, IG165 (a), (b), (c)	Yearly meeting with relevant stakeholders such as information owner/ HoD ---------------- G95 IG165, IG165 (a), (b), (c)
Periodicity and nature of audits	Quarterly security audit of all information systems, network devices, processes, governance procedures etc. ---------------- G96 IG166, IG166 (a), (b), (c)	Quarterly security audit of all information systems, network devices, processes, governance procedures etc. ---------------- G96 IG166, IG166 (a), (b), (c)	Bi-annual security audit of all information systems, network devices, processes, governance procedures etc. ---------------- G96 IG166, IG166 (a), (b), (c)	Bi-annual security audit of all information systems, network devices, processes, governance procedures etc. ---------------- G96 IG166, IG166 (a), (b), (c)	Yearly security audit of all information systems, network devices, processes, governance procedures etc. ---------------- G96 IG166, IG166 (a), (b), (c)
Audit management function/ Evidence and artifact/ Management reporting and actions	Dedicated audit function Subject matter experts/ specialized information security auditors Availability of all categories of logs Availability of advanced analysis	Dedicated audit function Subject matter experts/ specialized information security auditors Availability of all categories of logs Availability of advanced analysis	Dedicated audit function Subject matter experts/ specialized information security auditors Availability of all categories of logs Availability of advanced analysis	Cross functional audit Availability of all categories of logs Availability of advanced analysis tools Audit findings communicated to HOD	Cross functional audit Availability of all categories of logs Availability of advanced analysis tools Audit findings communicated to HOD

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	tools Audit findings communicated to ISSC Priority correction of audit issues ---------------- G97, G98, G99 IG167, IG167 (a), (b), (c), (d), (e), (f), (g), (h), IG168, IG168 (a) IG179, IG69 (a)	tools Audit findings communicated to ISSC Priority correction of audit issues ---------------- G97, G98, G99 IG167, IG167 (a), (b), (c), (d), (e), (f), (g), (h), IG168, IG168 (a) IG179, IG69 (a)	tools Audit findings communicated to ISSC Priority correction of audit issues ---------------- G97, G98, G99 IG167, IG167 (a), (b), (c), (d), (e), (f), (g), (h), IG168, IG168 (a) IG179, IG69 (a)	Timely correction of audit issues ---------------- G97, G98, G99 IG167, IG167 (a), (b), (c), (d), (e), (f), (g), (h), IG168, IG168 (a) IG179, IG69 (a)	Timely correction of audit issues ---------------- G97, G98, G99 IG167, IG167 (a), (b), (c), (d), (e), (f), (g), (h), IG168, IG168 (a) IG179, IG69 (a)
Business continuity					
Inventory of operational processes/ Risk assessment and impact analysis/ Protection from disruption	Protect from disruption Quarterly risk assessment Quarterly business impact analysis ---------------- G100, G101, G102, IG170, IG170 (a), (b), (c) IG171, IG171 (a), (b), (c) IG172	Protect from disruption Quarterly risk assessment Quarterly business impact analysis ---------------- G100, G101, G102, IG170, IG170 (a), (b), (c) IG171, IG171 (a), (b) IG172	Protect from disruption Quarterly risk assessment Quarterly business impact analysis ---------------- G100, G101, G102, IG170, IG170 (a), (b) IG171, IG171 (a), (b) IG172	Protect from disruption Bi-annual risk assessment Bi-annual business impact analysis ---------------- G100, G101, G102, IG170, IG170 (a), (b) IG171, IG171 (a), (b) IG172	Protect from disruption Yearly risk assessment Yearly business impact analysis ---------------- G100, G101, G102, IG170, IG170 (a), (b) IG171, IG171 (a), (b) IG172
Test and management of continuity plans/ Improvement of continuity plans	Quarterly exercise and mock drills Identification of areas of improvement and communication to ISSC ---------------- G103, G105 IG173 IG175, IG175 (a)	Quarterly exercise and mock drills Identification of areas of improvement and communication to ISSC ---------------- G103, G105 IG173 IG175, IG175 (a)	Quarterly exercise and mock drills Identification of areas of improvement and communication to ISSC ---------------- G103, G105 IG173 IG175, IG175 (a)	Bi-annual exercise and mock drills Identification of areas of improvement and communication to ISSC ---------------- G103, G105 IG173 IG175, IG175 (a)	Yearly exercise and mock drills Identification of areas of improvement and communication to ISSC ---------------- G103, G105 IG173 IG175, IG175 (a)
Security capability continuity	Continuity of security capability Consistent data security for disaster	Continuity of security capability Consistent data security for disaster recovery	Continuity of security capability Consistent data security for disaster recovery	Continuity of security capability Consistent data security for disaster recovery	Continuity of security capability Consistent data security for disaster recovery

Area	Top secret	Secret	Confidential	Restricted	Unclassified
	recovery site ---------------- G104 IG174, IG174 (a), (b)	site ---------------- G104 IG174, IG174 (a), (b)	site ---------------- G104 IG174, IG174 (a), (b)	site ---------------- G104 IG174, IG174 (a), (b)	site ---------------- G104 IG174, IG174 (a), (b)
Open source technology					
Integration/ Licensing/ Installation/ Additional requirement/ Expertise/ Availability of support	Independent security evaluation Security testing and evaluation Compatibility with existing technology Lifecycle support On-going vulnerability scans ---------------- G106, G107, G108, G109, G110, G111, G112 IG176, IG177, IG178, IG179, IG180, IG181, IG181 (a), (b), (c), (d)	Independent security evaluation Security testing and evaluation Compatibility with existing technology Lifecycle support On-going vulnerability scans ---------------- G106, G107, G108, G109, G110, G111, G112 IG176, IG177, IG178, IG179, IG180, IG181, IG181 (a), (b), (c), (d)	Independent security evaluation Security testing and evaluation Compatibility with existing technology Lifecycle support On-going vulnerability scans ---------------- G106, G107, G108, G109, G110, G111, G112 IG176, IG177, IG178, IG179, IG180, IG181, IG181 (a), (b), (c), (d)	Independent security evaluation Security testing and evaluation Compatibility with existing technology Lifecycle support Vulnerability scans ---------------- G106, G107, G108, G109, G110, G111, G112 IG176, IG177, IG178, IG179, IG180, IG181, IG181 (a), (b), (c), (d)	Independent security evaluation Security testing and evaluation Compatibility with existing technology Lifecycle support Vulnerability scans ---------------- G106, G107, G108, G109, G110, G111, G112 IG176, IG177, IG178, IG179, IG180, IG181, IG181 (a), (b), (c), (d)

Annexure

29. Annexures

Annexure 1 – References

1A - List of government advisories on information security

S. No.	Name/ Title	Issued by	Details
1.	Manual of departmental security instructions	Ministry of Home Affairs	1994
2.	Cyber Security Policy for Government of India	National Informatics Center	V 2.0, 30th August, 2010
3.	IT security policy	CERT- In	
4.	Cyber security policy & procedures	Inter-Ministerial Task Force on Assessment of Indian Cyber Defense Strategies & Preparedness	V0.1, Draft under circulation
5.	Guidelines for Protection of National Critical Information Infrastructure	National Technical Research Organization	V 1.0, June 2013
6.	Information systems security guidelines for the banking and Financial sector	Reserve Bank of India	
7.	Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism	CERT – In	March 2012
8.	National Cyber Security Policy	DeitY	July 2013
9.	Computer Security Guidelines	IB	2006
10.	Guidelines for Sensitivity Assurance of Imported Equipment	Ministry of Science & Technology	

1B – List of information security frameworks

S. No.	Name/ Title	Issued by	Details
1.	ISO 27001:2005	International Organization for Standardization (ISO)	2005
2.	ISO 27001:2013	International Organization for Standardization (ISO)	2013
3.	DSCI Security Framework	Data Security Council of India (DSCI)	2010
4.	Common Security Framework (CSF)	Health Information Trust Alliance (HITRUST)	2012
5.	COBIT 5	Information Systems Audit and Control Association (ISACA)	2012

1C – List of risk assessment frameworks

S. No.	Name/ Title	Issued by	Details
1.	ISO 27005:2008	International Organization for Standardization (ISO)	2008
2.	OCTAVE	Software Engineering Institute (SEI)	2001
3.	RISK IT	ISACA	2009
4.	Risk Management Framework (RMF)	National Institute of Standards and Technology (NIST)	NIST Special Publication 800-37

1D – List of security assessment methodologies

S. No.	Name/ Title	Issued by	Details
1.	DSCI Assessment Framework - Security	DSCI	2012
2.	B.A.S.E.	SANS Institute	2005
3.	ISSAF	Open Information Systems Security Group (OISSG)	
4.	ASSET	NIST	SP 800-53 Rev. 4, *2013*

1E – List of application security methodologies

S. No.	Name/ Title	Issued by	Details
1.	Open Web Application Security Project (OWASP)	Open Web Application Security Project (OWASP)	SWAF Manifesto v0.08, 2010

1F – List of business continuity management frameworks

S. No.	Name/ Title	Issued by	Details
1.	ISO 22301:2012	International Organization for Standardization (ISO)	V 1.0, 2012
2.	BS 25999-2:2007	British Standards Institution	2007

Annexure 2 – Mapping of guidelines and controls in NISPG

2A. Mapping of guidelines and controls in Security domains

Security domain - Guidelines and implementation			
Guideline	**Area**	**Identifier**	**Description**
Network and infrastructure security			
G1	Inventory of assets and infrastructure	C, IG1	Identification & classification
		C, IG2	Network diagram
		C, IG3	Network configuration
G2	Security testing of network & infrastructure devices	C, IG4	Testing and certification of network & infrastructure device
G3	Network perimeter security	C, IG5	Network security measures
		C, IG6	Security of IPv6 device
G4	Network Zones	C, IG7	Segmentation
		C, IG8	Security zones
		C, IG9	Network traffic segregation
G5	LAN security	C, IG10	LAN security
G6	Wireless architecture	C, IG11	Wireless LAN security
G7	Network security management	C, IG12	Disabling unused ports
		C, IG13	Personal Devices Usage policy
		C, IG14	Restricting access to public network
		C, IG15	Network access control
		C, IG16	Firmware upgrade
		C, IG17	Network change management
		C, IG18	Securing transmission media
		C, IG21	Audit and review
G8	Unauthorized device connection	C, IG19	Default device credentials
		C, IG20	Connecting devices
G9	Extending connectivity to third parties	C, IG22	Extending connectivity to third parties
Identity, access and privilege management			
G10	Governance procedures for access rights, identity & privileges	C, IG23	Operational requirement mapping
		C, IG24	Unique identity of each user
		C, IG25	User access management
		C, IG26	Access control policies
		C, IG27	Need – to – know access

		C, IG28	Review of user privileges
		C, IG29	Special privileges
G11	Authentication & authorization for access	C, IG30	Authentication mechanism for access
		C, IG31	Inactive accounts
		C, IG32	Acceptable usage of Information assets & systems
G12	Password management	C, IG33	Password policy
		C, IG34	Default device credentials
G13	Credential monitoring	C, IG35	Monitoring and retention of logs
		C, IG36	Unsuccessful login attempts
G14	Provisioning personal devices and remote access	C, IG37	Ad-hoc access to systems
		C, IG38	Remote access
		C, IG39	Provisioning of personal devices
G15	Segregation of duties	C, IG40	Segregation of duties
G16	Access record documentation	C, IG25	User access management
G17	Linkage of logical and physical access	C, IG26	Access control policies
G18	Disciplinary actions	C, IG41	User awareness & liability
Physical security			
G19	Map and characteristics of physical facilities	C, IG42	Map and characteristics of physical facilities
G20	Protection from hazard	C, IG43	Hazard assessment
		C, IG44	Hazard protection
G21	Physical boundary protection	C, IG45	Securing gateways
		C, IG46	Identity badges
		C, IG47	Entry of visitors & external service providers
		C, IG48	Visitor verification
		C, IG49	Infrastructure protection
		C, IG50	Guarding facility
		C, IG51	Vehicle entry
G22	Restricting entry	C, IG45	Securing gateways
		C, IG46	Identity badges
		C, IG52	Correlation between physical and logical security
G23	Interior security	C, IG53	Monitoring & surveillance

		C, IG54	Disposal of equipment
		C, IG55	Protection of information assets and systems
		C, IG56	Authorization for change
		C, IG57	Inactivity timeout
		C, IG58	Protection of access keys
		C, IG59	Shoulder surfing
G24	Security zones	C, IG60	Categorization of zones
G25	Access to restricted area	C, IG61	Access to restricted areas
		C, IG62	Visitor device management
G26	Physical activity monitoring and review	C, IG63	Physical access auditing and review
Application security			
G27	Application security process	C, IG64	Application security process
G28	Application design	C, IG65	Application security architecture
G29	Application threat management	C, IG66	Application User authentication
		C, IG67	Secure configuration
		C, IG68	Ports & services
		C, IG69	Session management
		C, IG70	Input validation
		C, IG71	Error handling
G30	Application security testing	C, IG72	Application security testing
		C, IG73	Code review
		C, IG74	Black box testing
G31	Data management	C, IG75	Data handling
		C, IG76	Least privileges
		C, IG77	Segregation of duties
G32	Application lifecycle management	C, IG78	Secure software development life-cycle (SDLC) processes
		C, IG79	Application change control
G33	Application vulnerability intelligence	C, IG80	Application vulnerability intelligence
G34	Application security governance	C, IG81	Application logs & monitoring
Data security			

G35	Data discovery, identification & classification	C, IG82	Data discovery
		C, IG83	Data classification
G36	Cryptography & encryption	C, IG84	Cryptography & encryption
G37	Key management	C, IG85	Key management
G38	Information leakage prevention	C, IG86	Data-at-rest
		C, IG87	Data-masking
		C, IG88	Database management
		C, IG89	Public mail and collaboration tools
		C, IG90	External media & printing devices
		C, IG91	Preventing loss of information
		C, IG92	Backup
		C, IG93	Data retention and disposal
G39	Information access rights	C, IG91	Preventing loss of information
G40	Third party access	C, IG94	Third party access
G41	Monitoring & review	C, IG95	Monitoring & review
G42	Breach management & corrective action	C, IG96	Breach management
Personnel security			
G43	Awareness & training	C, IG97	Training and Awareness
G44	Employee verification	C, IG98	Employee verification
G45	Authorizing access to third parties	C, IG99	Authorizing access to third parties
		C, IG101	Disciplinary processes
G46	Record of authorized users	C, IG102	Record of authorized users
G47	Acceptable usage policy	C, IG100	Acceptable use policies
G48	Monitoring and review	C, IG103	Monitoring and review
G49	Limiting exposure of information	C, IG104	Non- disclosure agreements
		C, IG105	Legal and contractual obligations
		C, IG106	Communication Practices
Threat and vulnerability management			
G50	Interdependence of assets & systems	C, IG107	Interdependence of assets & systems

G51	Standardized operating environment	C, IG108	Standard operating environment
G52	Including TVM in change management	C, IG109	Threat assessment
G53	Integration with external intelligence sources	C, IG110	Integration with external intelligence
G54	Intelligence gathering	C, IG111	Vulnerabilities knowledge management
		C, IG112	Changing threat ecosystem
		C, IG113	Threats emanated from third parties
G55	Technical policies	C, IG114	System hardening
		C, IG115	Patch management
		C, IG116	Malware protection
		C, IG117	Perimeter threat protection
		C, IG118	Protection from fraudulent activity
		C, IG119	Configuration of endpoints
		C, IG120	Remediation
Security monitoring & incident management			
G56	Incidence response coverage	C, IG121	Security incident monitoring
		C, IG122	Incident management
		C, IG123	Incident identification
		C, IG124	Incident evaluation
		C, IG125	Escalation process
G57	Breach scenarios	C, IG126	Breach information
G58	Security intelligence information	C, IG127	Configuring devices for logging
G59	Enterprise log management	C, IG128	Activity logging
		C, IG129	Log information
		C, IG130	Log information correlation
		C, IG131	Protecting Log information
G60	Deployment of skilled resources	C, IG132	Deployment of skilled resources
G61	Disciplinary action	C, IG122	Incident management

G62	Structure & responsibility	C, IG122	Incident management
		C, IG125	Escalation process
G63	Incident management awareness and training	C, IG123	Incident identification
G64	Communication of incidents	C, IG133	Incident reporting
		C, IG134	Sharing of log information with law enforcement agencies
		C, IG135	Communication of incidents
Cloud computing			
G65	Security considerations in contract	IG136	Security considerations in contract
G66	Alignment of security policies	IG137	Alignment of security policies
G67	Data security in cloud environment	IG138	Data security in cloud environment
G68	Authentication in cloud environment	IG139	Authentication in cloud environment
G69	Continuity of operations	IG140	Continuity of operations
G70	Definition of roles and responsibilities	IG141	Definition of roles and responsibilities
G71	Security monitoring	IG142	Security monitoring
G72	Availability of logs	IG143	Availability of logs
G73	Third party security assessments	IG144	Third party security assessments
G74	Data security	IG145	Data security
G75	Use of authorized cloud services	IG146	Use of authorized cloud services
Mobility and BYOD			
G76	Mobile device policy	IG147	Mobile device policy
G77	Risk evaluation of devices	IG148	Risk evaluation of devices
G78	Allocation of mobile devices	IG147	Mobile device policy
G79	Device lifecycle management and governance	IG149	Device lifecycle management and governance
G80	Data transmission and storage	IG150	Data transmission and storage

G81	Awareness	IG151	Awareness
Virtualization			
G82	Evaluate risks associated with virtual technologies	IG152	Evaluate risks associated with virtual technologies
G83	Strengthen physical access	IG153	Strengthen physical access
G84	Segregation of virtual traffic	IG154	Segregation of virtual traffic
G85	Implement defense in depth	IG155	Implement defense in depth
G86	Harden the virtualization management console	IG156	Harden the virtualization management console
G87	Vulnerability information	IG157	Vulnerability information
G88	Logging and monitoring	IG158	Logging and monitoring
Social media			
G89	Limit exposure of official information	IG159	Limit exposure of official information
G90	Permitted official use	IG160	Permitted official use
Security testing			
G91	Security evaluation	IG161	Security evaluation
G92	Testing scenarios	IG162	Testing Scenarios
G93	Overt and covert testing	IG163	Overt and covert testing
G94	Vulnerability existence	IG164	Vulnerability Existence
Security audit			
G95	Determine security auditing requirements	IG165	Determine security auditing requirements
G96	Periodicity and nature of audits	IG166	Periodicity and nature of audits
G97	Audit management function	IG167	Audit management function
G98	Evidence and artifact	IG168	Evidence and artifact
G99	Management reporting and actions	IG169	Management reporting and actions
Business continuity			

G100	Inventory of operational processes	IG170	Inventory of operational processes
G101	Risk assessment and impact analysis	IG171	Risk assessment and impact analysis
G102	Protection from disruption	IG172	Protection from disruption
G103	Test and management of continuity plans	IG173	Test and management of continuity plans
G104	Security capability continuity	IG174	Security capability continuity
G105	Improvement of continuity plans	IG175	Improvement of continuity plans
Open source technology			
G106	Integration	IG176	Integration
G107	Licensing	IG177	Licensing
G108	Security testing		
G109	Installation	IG178	Installation
G110	Additional requirements	IG179	Additional requirements
G111	Expertise	IG180	Expertise
G112	Availability of support	IG181	Availability of support

2B. Table of guidelines under technology specific ICT deployment and essential security practices

Number	Description
Cloud computing	
G65	Security considerations in contract
G66	Alignment of security policies
G67	Data security in cloud environment
G68	Authentication in cloud environment
G69	Continuity of operations
G70	Definition of roles and responsibilities
G71	Security monitoring
G72	Availability of logs
G73	Third party security assessments
G74	Data security
G75	Use of authorized cloud services
Mobility and BYOD	
G76	Mobile device policy
G77	Risk evaluation of devices
G78	Allocation of mobile devices
G79	Device lifecycle management and governance
G80	Data transmission and storage
G81	Awareness
Virtualization	
G82	Evaluate risks associated with virtual technologies
G83	Strengthen physical access
G84	Segregation of virtual traffic
G85	Implement defense in depth
G86	Harden the virtualization management console
G87	Vulnerability information
G88	Logging and monitoring
Social media	
G89	Limit exposure of official information
G90	Permitted official use
Security testing	
G91	Security evaluation
G92	Testing scenarios
G93	Overt and covert testing

G94	Vulnerability existence
Security audit	
G95	Determine security auditing requirements
G96	Periodicity and nature of audits
G97	Audit management function
G98	Evidence and artifact
G99	Management reporting and actions
Business continuity	
G100	Inventory of operational processes
G101	Risk assessment and impact analysis
G102	Protection from disruption
G103	Test and management of continuity plans
G104	Security capability continuity
G105	Improvement of continuity plans
Open source technology	
G106	Integration
G107	Licensing
G108	Security testing
G109	Installation
G110	Additional requirements
G111	Expertise
G112	Availability of support

Annexure 3 – Guidelines issued by National Critical Information Infrastructure Protection Centre, National Technical Research Organization

S. No.	Control
N1	Identification of CIIs
N2	Vertical and horizontal interdependencies
N3	Information security department
N4	Information security policy
N5	Training and Skill Up gradation
N6	Data loss prevention
N7	Access control policies
N8	Limiting admin privileges
N9	Perimeter protection
N10	Incident response
N11	Risk assessment management
N12	Physical security
N13	Identification and Authentication
N14	Maintenance plan
N15	Maintaining Monitoring and Analyzing Logs
N16	Penetration testing
N17	Data storage - Hashing and Encryption
N18	Feedback mechanism
N19	Security certification
N20	Asset and Inventory Management
N21	Contingency planning
N22	Disaster recovery site
N23	Predictable failure prevention
N24	Information/data leakage protection
N25	DoS/DDoS Protection
N26	Wi-Fi Security
N27	Data Back-up Plan
N28	Secure architecture deployment
N29	Web application security
N30	Testing and evaluation of hardware and software
N31	Hardening of hardware and software
N32	Period audit
N33	Compliance of Security Recommendations

N34	Checks and balances for negligence
N35	Advanced Persistent threats (APT) Protection
N36	Network device protection
N37	Cloud security
N38	Outsourcing and vendor security
N39	Critical information disposal and transfer
N40	Intranet security

Annexure 4 – Guidelines and controls mentioned in "Cyber Security Policy for Government of India" ver 2.0 released 30th August, 2010

Note: The guidelines and controls mentioned in this policy document are bifurcated as per operational areas and contain general guidance spread across multiple domains

S.No.	Areas	Guidelines and Controls
1.	Acceptable use of client systems	Virus and malicious code
		H/W, OS & Application software
		Email use
		Password security
		Portable storage media
		Network access policy
		Client system logs
2.	Security for system administrator	
3.	Security policy for network connected to Internet	Network access
		Client antivirus
		Gateway antivirus
		Network hardening
		Network Architecture
		Security Administration
		Monitoring & reporting
		Incident handling
		Security Audit
		Policy review
		Policy enforcement
4.	Security policy for department	Portable storage media
		Network access policy applicable for users
		Applications
		Audit trail and event log
		Security audit
5.	Application security guidelines	General guidelines
		Web application vulnerabilities
		Cross site scripting
		Malicious file execution
		Insecure direct object reference
		Cross site request forgery
		Information leakage and improper error handling

		Broken authentication and session management
		Insecure cryptographic storage
		Insecure communication
		Failure to restrict URL access
6.	Asset management guidelines	Asset management
		Nomenclature for asset ID
		Organization
		Location of bhawan
		Type of asset
		Sub type
		Numeric value
		Review and updation
7.	Client system security guidelines	
8.	Network device security guidelines	General
		Firewall guidelines
		Intrusion Prevention System (IPS) guidelines
		Switch configuration
		Router configuration
		Operating system up- gradation
		SNMP protocol
		Banner message
		Backup
		Log maintenance
9.	Password management guidelines	General
		Password complexity
		Password reset
		Password change
		Account lockout
		Password storage
10.	Security guidelines for user	Unattended client systems
		Internet usage
		Email usage
		Portable storage media
		Additional security measure for laptops
11.	Security policy dissemination	

	guidelines	
12.	Time synchronization guidelines	
13.	Wireless network security guidelines	
14.	Change management process	
15.	Security incident management process	

Annexure 5 – List of control objectives specified as per FISMA

NIST SP 800-53 CONTROLS	
AC-1	Access control policy and procedures
AC-2	Account management
AC-3	Access enforcement
AC-4	Information flow enforcement
AC-5	Separation of duties
AC-6	Least privilege
AC-7	Unsuccessful logon attempts
AC-8	System use notification
AC-9	Previous logon (access) notification
AC-10	Concurrent session control
AC-11	Session lock
AC-12	Session termination
AC-13	Withdrawn
AC-14	Permitted actions without identification or authentication
AC-15	Withdrawn
AC-16	Security attributes
AC-17	Remote access
AC-18	Wireless access
AC-19	Access control for mobile devices
AC-20	Use of external information systems
AC-21	Information sharing
AC-22	Publicly accessible content
AC-23	Data mining protection
AC-24	Access control decisions
AC-25	Reference monitor
AT-1	Security awareness and training policy and procedures
AT-2	Security awareness training
AT-3	Role-based security training
AT-4	Security training records
AT-5	Withdrawn
AU-1	Audit and accountability policy and procedures
AU-2	Audit events
AU-3	Content of audit records
AU-4	Audit storage capacity

AU-5	Response to audit processing failures
AU-6	Audit review, analysis, and reporting
AU-7	Audit reduction and report generation
AU-8	Time stamps
AU-9	Protection of audit information
AU-10	Non-repudiation
AU-11	Audit record retention
AU-12	Audit generation
AU-13	Monitoring for information disclosure
AU-14	Session audit
AU-15	Alternate audit capability
AU-16	Cross-organizational auditing
CA-1	Security Assessment and Authorization Policies and Procedures
CA-2	Security assessments
CA-3	System interconnections
CA-4	Withdrawn
CA-5	Plan of action and milestones
CA-6	Security authorization
CA-7	Continuous monitoring
CA-8	Penetration testing
CA-9	Internal system connections
CM-1	Configuration management policy and procedures
CM-2	Baseline configuration
CM-3	Configuration change control
CM-4	Security impact analysis
CM-5	Access restrictions for change
CM-6	Configuration settings
CM-7	Least functionality
CM-8	Information system component inventory
CM-9	Configuration management plan
CM-10	Software usage restrictions
CM-11	User-installed software
CP-1	Contingency planning policy and procedures
CP-2	Contingency plan
CP-3	Contingency training
CP-4	Contingency plan testing

CP-5	Withdrawn
CP-6	Alternate storage site
CP-7	Alternate processing site
CP-8	Telecommunications services
CP-9	Information system backup
CP-10	Information system recovery and reconstitution
CP-11	Alternate communications protocols
CP-12	Safe mode
CP-13	Alternative security mechanisms
IA-1	Identification and authentication policy and procedures
IA-2	Identification and authentication (organizational users)
IA-3	Device identification and authentication
IA-4	Identifier management
IA-5	Authenticator management
IA-6	Authenticator feedback
IA-7	Cryptographic module authentication
IA-8	Identification and authentication (non-organizational users)
IA-9	Service identification and authentication
IA-10	Adaptive identification and authentication
IA-11	Re-authentication
IR-1	Incident response policy and procedures
IR-2	Incident response training
IR-3	Incident response testing
IR-4	Incident handling
IR-5	Incident monitoring
IR-6	Incident reporting
IR-7	Incident response assistance
IR-8	Incident response plan
IR-9	Information spillage response
IR-10	Integrated information security analysis team
MA-1	System maintenance policy and procedures
MA-2	Controlled maintenance
MA-3	Maintenance tools
MA-4	Nonlocal maintenance
MA-5	Maintenance personnel
MA-6	Timely maintenance

MP-1	Media protection policy and procedures
MP-2	Media access
MP-3	Media marking
MP-4	Media storage
MP-5	Media transport
MP-6	Media sanitization
MP-7	Media use
MP-8	Media downgrading
PE-1	Physical and environmental protection policy and procedures
PE-2	Physical access authorizations
PE-3	Physical access control
PE-4	Access control for transmission medium
PE-5	Access control for output devices
PE-6	Monitoring physical access
PE-7	Withdrawn
PE-8	Visitor access records
PE-9	Power equipment and cabling
PE-10	Emergency shutoff
PE-11	Emergency power
PE-12	Emergency lighting
PE-13	Fire protection
PE-14	Temperature and humidity controls
PE-15	Water damage protection
PE-16	Delivery and Removal
PE-17	Alternate work site
PE-18	Location of information system components
PE-19	Information leakage
PE-20	Asset monitoring and tracking
PL-1	Security planning policy and procedures
PL-2	System security plan
PL-3	Withdrawn
PL-4	Rules of Behavior
PL-5	Withdrawn
PL-6	Withdrawn
PL-7	Security concept of operations
PL-8	Information security architecture

PL-9	Central management
PS-1	Personnel security policy and procedures
PS-2	Position risk designation
PS-3	Personnel screening
PS-4	Personnel termination
PS-5	Personnel transfer
PS-6	Access agreements
PS-7	Third-party personnel security
PS-8	Personnel sanctions
RA-1	Risk Assessment Policy and Procedures
RA-2	Security categorization
RA-3	Risk assessment
RA-4	Withdrawn
RA-5	Vulnerability scanning
RA-6	Technical surveillance countermeasures survey
SA-1	System and services acquisition policy and procedures
SA-2	Allocation of Resources
SA-3	System development life cycle
SA-4	Acquisition process
SA-5	Information system documentation
SA-6	Withdrawn
SA-7	Withdrawn
SA-8	Security engineering principles
SA-9	External information system services
SA-10	Developer configuration management
SA-11	Developer security testing and evaluation
SA-12	Supply chain protections
SA-13	Trustworthiness
SA-14	Criticality analysis
SA-15	Development process, standards, and tools
SA-16	Developer-provided training
SA-17	Developer security architecture and design
SA-18	Tamper resistance and detection
SA-19	Component authenticity
SA-20	Customized development of critical components
SA-21	Developer screening

SA-22	Unsupported system components
SC-1	System and communications protection policy and procedures
SC-2	Application partitioning
SC-3	Security function isolation
SC-4	Information in shared resources
SC-5	Denial of service protection
SC-6	Resource availability
SC-7	Boundary protection
SC-8	Transmission confidentiality and integrity
SC-9	Withdrawn
SC-10	Network disconnect
SC-11	Trusted path
SC-12	Cryptographic key establishment and management
SC-13	Cryptographic protection
SC-14	Withdrawn
SC-15	Collaborative computing devices
SC-16	Transmission of security attributes
SC-17	Public key infrastructure certificates
SC-18	Mobile code
SC-19	Voice over internet protocol
SC-20	Secure name/address resolution service (authoritative source)
SC-21	Secure name/address resolution service (recursive or caching resolver)
SC-22	Architecture and provisioning for name/address resolution service
SC-23	Session authenticity
SC-24	Fail in known state
SC-25	Thin nodes
SC-26	Honeypots
SC-27	Platform-independent applications
SC-28	Protection of Information at Rest
SC-29	Heterogeneity
SC-30	Concealment and Misdirection
SC-31	Covert channel analysis
SC-32	Information system partitioning
SC-33	Withdrawn
SC-34	Non-modifiable executable programs

SC-35	Honey clients
SC-36	Distributed Processing and Storage
SC-37	Out-of-Band Channels
SC-38	Operations security
SC-39	Process isolation
SC-40	Wireless link protection
SC-41	Port and I/O Device Access
SC-42	Sensor Capability and Data
SC-43	Usage restrictions
SC-44	Detonation chambers
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw remediation
SI-3	Malicious code protection
SI-4	Information system monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security function verification
SI-7	Software, Firmware, and Information Integrity
SI-8	Spam protection
SI-9	Withdrawn
SI-10	Information input validation
SI-11	Error handling
SI-12	Information Handling and Retention
SI-13	Predictable failure prevention
SI-14	Non-persistence
SI-15	Information output filtering
SI-16	Memory protection
SI-17	Fail-safe procedures
PM-1	Information security program plan
PM-2	Senior information security officer
PM-3	Information security resources
PM-4	Plan of Action and Milestones Process
PM-5	Information system inventory
PM-6	Information Security Measures of Performance
PM-7	Enterprise architecture
PM-8	Critical infrastructure plan
PM-9	Risk management strategy

PM-10	Security authorization process
PM-11	Mission/business process definition
PM-12	Insider threat program
PM-13	Information security workforce
PM-14	Testing, Training, and Monitoring
PM-15	Contacts with Security Groups and Associations
PM-16	Threat awareness program

For more information refer: NIST Special Publications in the 800 series:

http://csrc.nist.gov/publications/PubsSPs.html

Annexure 6 – List of SANS 20 critical controls

S. No.	Control
S1	Inventory of authorized & unauthorized devices
S2	Inventory of authorized & unauthorized software
S3	Secure configurations for hardware & software on laptops, workstations, & servers
S4	Secure configurations for network devices such as firewalls, routers, & switches
S5	Boundary defense
S6	Maintenance, monitoring, & analysis of audit logs
S7	Application software security
S8	Controlled use of administrative privileges
S9	Controlled access based on need to know
S10	Continuous vulnerability assessment & remediation
S11	Account monitoring & control
S12	Malware defenses
S13	Limitation & control of network ports, protocols, & services
S14	Wireless device control
S15	Data loss prevention
S16	Secure network engineering
S17	Penetration tests & red team exercises
S18	Incident response capability
S19	Data recovery capability
S20	Security skills assessment & appropriate training to fill gaps

For more information refer: http://www.sans.org/critical-security-controls/

Annexure 7 – ISO 27001 list of controls

A. ISO 27001:2013

S. No.	Primary Security Domain	ISO 27001 Requirement (Reference)
	A.5.1 Management direction for information security	
1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. (A.5.1.1)
2	Review of the information security policy	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. (A.5.1.2)
	A.6.1 Internal organization	
3	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated. (A.6.1.1)
4	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. (A.6.1.2)
5	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained. (A.6.1.3)
6	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. (A.6.1.4)
7	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project. (A.6.1.5)
	A 6.2 Mobile devices and teleworking	
8	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. (A.6.2.1)
9	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites. (A.6.2.2)
	A.7.1 Prior to employment	
10	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. (A.7.1.1)
11	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security. (A.7.1.2)
	A.7.2 During employment	
12	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. (A.7.2.1)
13	Information security	All employees of the organization and, where relevant, contractors

	awareness, education and training	shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. (A.7.2.2)
14	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. (A.7.2.3)
	A.7.3 Termination and change of employment	
15	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced. (A.7.3.1)
	A.8.1 Responsibility for assets	
16	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. (A.8.1.1)
17	Ownership of assets	Assets maintained in the inventory shall be owned. (A.8.1.2)
18	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. (A.8.1.3)
19	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. (A.8.1.4)
	A.8.2 Information classification	
20	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. (A.8.2.1)
21	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. (A.8.2.2)
22	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. (A.8.2.3)
	A.8.3 Media handling	
23	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. (A.8.3.1)
24	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.(A.8.3.2)
25	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. (A.8.3.3)
	A.9.1 Business requirements of access control	
26	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements. (A.9.1.1)

27	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use. (A.9.1.2)
	A.9.2 User access management	
28	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights. (A.9.2.1)
29	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. (A.9.2.2)
30	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled. (A.9.2.3)
31	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.(A.9.2.4)
32	Review of user access rights	Asset owners shall review users' access rights at regular intervals. (A.9.2.5)
33	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. (A.9.2.6)
	A.9.3 User responsibilities	
34	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information. (A.9.3.1)
	A.9.4 System and application access control	
35	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy. (A.9.4.1)
36	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. (A.9.4.2)
37	Password management system	Password management systems shall be interactive and shall ensure quality passwords. (A.9.4.3)
38	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. (A.9.4.4)
39	Access control to program source code	Access to program source code shall be restricted. (A.9.4.5)
	A.10.1 Cryptographic controls	
40	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. (A.10.1.1)
41	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle. (A.10.1.2)

	A.11.1 Secure Areas	
42	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. (A.11.1.1)
43	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. (A.11.1.2)
44	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied. (A.11.1.3)
45	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. (A.11.1.4)
46	Working in secure areas	Procedures for working in secure areas shall be designed and applied. (A.11.1.5)
47	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. (A.11.1.6)
	A.11.2 Equipment	
48	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. (A.11.2.1)
49	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. (A.11.2.2)
50	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage. (A.11.2.3)
51	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity. (A.11.2.4)
52	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization. (A.11.2.5)
53	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises. (A.11.2.6)
54	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. (A.11.2.7)
55	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection. (A.11.2.8)
56	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. (A.11.2.9)
	A.12.1 Operational procedures and responsibilities	

57	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them. (A.12.1.1)
58	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled. (A.12.1.2)
59	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. (A.12.1.3)
60	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment. (A.12.1.4)
	A.12.2 Protection from malware	
61	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. (A.12.2.1)
	A.12.3 Backup	
62	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. (A.12.3.1)
	A.12.4 Logging and monitoring	
63	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. (A.12.4.1)
64	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access. (A.12.4.2)
65	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed. (A.12.4.3)
66	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source. (A.12.4.4)
	A.12.5 Control of operational software	
67	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems. (A.12.5.1)
	A.12.6 Technical vulnerability management	
68	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. (A.12.6.1)
69	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented. (A.12.6.2)
	A.12.7 Information systems audit considerations	
70	Information systems	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to

	audit controls	minimise disruptions to business processes. (A.12.7.1)
	A.13.1 Network security management	
71	Network controls	Networks shall be managed and controlled to protect information in systems and applications. (A.13.1.1)
72	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. (A.13.1.2)
73	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks. (A.13.1.3)
	A 13.2 Information transfer	
74	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. (A.13.2.1)
75	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties. (A.13.2.2)
76	Electronic messaging	Information involved in electronic messaging shall be appropriately protected. (A.13.2.3)
77	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented. (A.13.2.4)
	A.14.1 Security requirements of information systems	
78	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems. (A.14.1.1)
79	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. (A.14.1.2)
80	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. (A.14.1.3)
	A.14.2 Security in development and support processes	
81	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization. (A.14.2.1)
82	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. (A.14.2.2)
83	Technical review of applications after	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. (A.14.2.3)

	operating platform changes	
84	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled. (A.14.2.4)
85	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts. (A.14.2.5)
86	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. (A.14.2.6)
87	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development. (A.14.2.7)
88	System security testing	Testing of security functionality shall be carried out during development. (A.14.2.8)
89	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. (A.14.2.9)
	A.14.3 Test Data	
90	Protection of test data	Test data shall be selected carefully, protected and controlled. (A.14.3.1)
	A. 15.1 Information security in supplier relationships	
91	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. (A.15.1.1)
92	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. (A.15.1.2)
93	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. (A.15.1.3)
	A. 15.2 Supplier service delivery management	
94	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery. (A.15.2.1)
95	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. (A.15.2.2)

	A.16.1 Management of information security incidents and improvements	
96	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. (A.16.1.1)
97	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible. (A.16.1.2)
98	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services. (A.16.1.3)
99	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. (A.16.1.4)
100	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures. (A.16.1.5)
101	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. (A.16.1.6)
102	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. (A.16.1.7)
	A.17.1 Information security continuity	
103	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. (A.17.1.1)
104	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. (A.17.1.2)
105	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. (A.17.1.3)
106	**A.17.2 Redundancies**	
107	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. (A.17.2.1)
	A.18.1 Compliance with legal and contractual requirements	
108	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. (A.18.1.1)

109	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. (A.18.1.2)
110	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. (A.18.1.3)
111	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. (A.18.1.4)
112	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations. (A.18.1.5)
	A.18.2 Information security reviews	
113	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur. (A.18.2.1)
114	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. (A.18.2.2)
115	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards. (A.18.2.3)

B. ISO 27001:2005

S. No.	Primary Security Domain	ISO 27001 Requirement (Reference)
	A.5.1 Information security policy	
1	Information security policy document	An information security policy document shall be approved by the management, published and communicated to all employees and relevant external parties. (A.5.1.1)
2	Review of the information security policy	The information security policy shall be reviewed and revised at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. (A.5.1.2)
	A.6.1 Internal organization	
3	Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. (A.6.1.1)
4	Information security coordination	Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. (A.6.1.2)

5	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined. (A.6.1.3)
6	Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be defined and implemented. (A.6.1.4)
7	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.(A.6.1.5)
8	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained. (A.6.1.6)
9	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained (A.6.1.7)
10	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur. (A.6.1.8)
	A 6.2 External parties	
11	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access. (A.6.2.1)
12	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets. (A.6.2.2)
13	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.(A.6.2.3)
	A.7.1 Responsibility for assets	
14	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. (A.7.1.1)
15	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization. (A.7.1.2)
16	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented. (A.7.1.3)
	A.7.2 Information classification	
17	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. (A.7.2.1)

18	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization. (A.7.2.2)
	A.8.1 Prior to employment	
19	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.(A.8.1.1)
20	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.(A.8.1.2)
21	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security. (A.8.1.3)
	A.8.2 During employment	
22	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.(A.8.2.1)
23	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.(A.8.2.2)
24	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.(A.8.2.3)
	A.8.3 Termination or change of employment	
25	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned. (A.8.3.1)
26	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.(A.8.3.2)
27	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. (A.8.3.3)
	A.9.1 Secure areas	
28	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities. (A.9.1.1)
29	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.(A.9.1.2)
30	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied.(A.9.1.3)

31	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.(A.9.1.4)
32	Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.(A.9.1.5)
33	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.(A.9.1.6)
	A.9.2 Equipment security	
34	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.(A.9.2.1)
35	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.(A.9.2.2)
36	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.(A.9.2.3)
37	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.(A.9.2.4)
38	Security of equipment off premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.(A.9.2.5)
39	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.(A.9.2.6)
40	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.(A.9.2.7)
	A.10.1 Operational procedures and responsibilities	
41	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.(A.10.1.1)
42	Change management	Changes to information processing facilities and systems shall be controlled.(A.10.1.2)
43	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.(A.10.1.3)
44	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.(A.10.1.4)
	A.10.2 Third party service delivery management	
45	Service delivery	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.(A.10.2.1)

46	Monitoring and review ofthird party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.(A.10.2.2)
47	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.(A.10.2.3)
	A.10.3 System planning and acceptance	
48	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.(A.10.3.1)
49	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.(A.10.3.2)
	A.10.4 Protection against malicious and mobile code	
50	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.(A.10.4.1)
51	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.(A.10.4.2)
	A.10.5 Back-up	
52	Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.(A.10.5.1)
	A.10.6 Network security management	
53	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.(A.10.6.1)
54	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.(A.10.6.2)
	A.10.7 Media handling	
55	Management of removable media	There shall be procedures in place for the management of removable media.(A.10.7.1)
56	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.(A.10.7.2)
57	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.(A.10.7.3)

58	Security of system documentation	System documentation shall be protected against unauthorized access.(A.10.7.4)
	A.10.8 Exchange of information	
59	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.(A.10.8.1)
60	Exchange agreements	Exchange agreements shall be established for the exchange of information and software between the organization and external parties.(A.10.8.2)
61	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.(A.10.8.3)
62	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.(A.10.8.4)
63	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.(A.10.8.5)
	A.10.9 Electronic commerce services	
64	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.(A.10.9.1)
65	On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.(A.10.9.2)
66	Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.(A.10.9.3)
	A.10.10 Monitoring	
67	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.(A.10.10.1)
68	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.(A.10.10.2)
69	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.(A.10.10.3)
70	Administrator and operator logs	System administrator and system operator activities shall be logged.(A.10.10.4)
71	Fault logging	Faults should be logged, analysed, and appropriate action taken.(A.10.10.5)
72	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.(A.10.10.6)

	A.11.1 Business requirement for access control	
73	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.(A.11.1.1)
	A.11.2 User access management	
74	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.(A.11.2.1)
75	Privilege management	The allocation and use of privileges shall be restricted and controlled.(A.11.2.2)
76	User password management	The allocation of passwords shall be controlled through a formal management process.(A.11.2.3)
77	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.(A.11.2.4)
	A.11.3 User responsibilities	
78	Password use	Users shall be required to follow good security practices in the selection and use of passwords.(A.11.3.1)
79	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.(A.11.3.2)
80	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.(A.11.3.3)
	A.11.4 Network access control	
81	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.(A.11.4.1)
82	User authentication forexternal connections	Appropriate authentication methods shall be used to control access by remote users.(A.11.4.2)
83	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.(A.11.4.3)
84	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.(A.11.4.4)
85	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks.(A.11.4.5)
86	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications. (A.11.4.6)
87	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.(A.11.4.7)
	A 11.5 Operating system access control	

88	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.(A.11.5.1)
89	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.(A.11.5.2)
90	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.(A.11.5.3)
91	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.(A.11.5.4)
92	Session time-out	Inactive sessions shall shut down after a defined period of inactivity.(A.11.5.5)
93	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.(A.11.5.6)
	A.11.6 Application and information access control	
94	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.(A.11.6.1)
95	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.(A.11.6.2)
	A.11.7 Mobile computing and teleworking	
96	Mobile computing and communications	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using computing and communication facilities.(A.11.7.1)
97	Teleworking	A policy, operational plans and procedures shall be developed and implemented for Teleworking activities.(A.11.7.2)
	A.12.1 Security requirements of information systems	
98	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.(A.12.1.1)
	A. 12.2 Correct processing in applications	
99	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.(A.12.2.1)
100	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.(A.12.2.2)
101	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.(A.12.2.3)
102	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.(A.12.2.4)
	A. 12.3 Cryptographic controls	

103	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.(A.12.3.1)
104	Key management	Key management shall be in place to support the organization's use of cryptographic techniques.(A.12.3.2)
	A.12.4 Security of system files	
105	Control of operational software	There shall be procedures in place to control the installation of software on operational systems.(A.12.4.1)
106	Protection of system test data	Test data shall be selected carefully, and protected and controlled.(A.12.4.2)
107	Access control to program source code	Access to program source code shall be restricted.(A.12.4.3)
	A.12.5 Security in development and support processes	
108	Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.(A.12.5.1)
109	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.(A.12.5.2)
110	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.(A.12.5.3)
111	Information leakage	Opportunities for information leakage shall be prevented.(A.12.5.4)
112	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.(A.12.5.5)
	A.12.6 Technical Vulnerability Management	
113	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.(A.12.6.1)
	A.13.1 Reporting information security events and weaknesses	
114	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.(A.13.1.1)
115	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.(A.13.1.2)
	A.13.2 Management of information security incidents and improvements	
116	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.(A.13.2.1)
117	Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.(A.13.2.2)

118	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).(A.13.2.3)
	A.14.1 Information security aspects of business continuity management	
119	Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.(A.14.1.1)
120	Business continuity and risk assessment	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.(A.14.1.2)
121	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.(A.14.1.3)
122	Business continuity planningframework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.(A.14.1.4)
123	Testing, maintaining and reassessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.(A.14.1.5)
	A.15.1 Compliance with legal requirements	
124	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.(A.15.1.1)
125	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.(A.15.1.2)
126	Protection of organizationalrecords	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.(A.15.1.3)
127	Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.(A.15.1.4)
128	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.(A.15.1.5)

129	Regulation of cryptographic controls	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.(A.15.1.6)
	A.15.2 Compliance with security policies and standards, and technical compliance	
130	Compliance with security policies and standards	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.(A.15.2.1)
131	Technical compliance checking	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.(A.15.2.2)
	A.15.3 Information System Audit Considerations	
132	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes. (A.15.3.1)
133	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise. (A.15.3.2)

For more information refer: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Annexure 8 – Mapping of NISP controls with global security frameworks/ standards

NISP Control Number	NISP Control Title	ISO 27001:2005	SANS 20 Critical	NTRO 40 Critical Controls	FISMA Controls
C1	Identification & classification	A.7.1.1	S1, S7		SA-8, CM-8, CM-9, PM-5
C2	Network diagram	A.7.1.1	S1, S7		SA-8, CM-8, CM-9, PM-5
C3	Network configuration	A.11.4.3, A.11.4.7	S4, S10	N36	AC-4, AC-17, AC-18, AC-19, IA-3
C4	Testing and certification of network & infrastructure device	A.10.6.2		N19	SA-9, SC-8, SC-9
C5	Network security measures	A.10.6.1, A.10.6.2	S5, S7	N9, N24, N25	AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23, SA-9
C6	Security of IPv6 device				
C7	Segmentation	A.11.4.5	S1, S19		AC-4, SA-8, SC-7
C8	Security zones	A.10.6.2	S1, S5, S7, S19	N9	CA-3, SC-7, SC-8, SC-9, PM-7, SA-8, SA-9
C9	Network traffic segregation	A.11.4.7	S1, S10, S19		AC-4, AC-17, AC-18
C10	LAN security		S16	N36	
C11	Wireless LAN security		S14	N26	AC-18
C12	Disabling unused ports		S7, S11, S13, S14	N36	CM7, AC-18
C13	Personal Devices Usage policy		S3, S7, S13		RA-5, SI-3
C14	Restricting access to public network		S1, S7, S13	N7, N26	
C15	Network access control	A.11.4.6	S1, S7, S13	N7, N26	AC-3, AC-6, AC-17, AC-18, SC-7
C16	Firmware upgrade		S3, S4	N36	
C17	Network change management	A.10.1.2	S3, S4, S7, S10		CM-1, CM-3, CM-4, CM-5, CM-9
C18	Securing transmission media				
C19	Default device credentials		S3		IA-5
C20	Connecting devices	A.10.7.1	S1	N7	MP-2, PE-16

C21	Audit and review	A.10.10.1	S1	N20, N32, N34	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12
C22	Extending connectivity to third parties	A.10.7.4, A.10.8.5	S13	N38	MP-4, SA-5, CA-1, CA-3
C23	Operational requirement mapping	A.12.1.1	S3		SA-1, SA-3, SA-4
C24	Unique identity of each user	A.8.3.3, A.11.2.1		N13	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2, PS-4, PS-5
C25	User access management	A.8.3.3, A.11.2.1	S12, S16	N8, N13	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2, PS-4, PS-5
C26	Access control policies	A.8.3.3, A.11.1.1, A.10.2.2, A.10.10.2	S12, S16	N7, N8, N13	AC-1, AC-2, AC-5, AC-6, AC-17, AC-18, AC-19, CM-5, MP-1, SI-9, AC-2, PS-4, PS-5
C27	Need – to – know access	A.11.2.2, A.11.4.1	S9	N7, N8	AC-1, AC-2, AC-5, AC-6, AC-17, AC-18, AC-20, AC-21, PE-1, PE-2, SI-9
C28	Review of user privileges	A.10.2.2, A.11.2.1, A.11.2.2	S12, S16	N8	SA-9, AC-1, AC-2, AC-6, AC-21, IA-5, PE-1, PE-2, SI-9
C29	Special privileges		S12	N8	AC-6
C30	Authentication mechanism for access	A.11.5.2	S12	N13	IA-2, IA-4, IA-5, IA-8
C31	Inactive accounts	A.11.2.1	S12, S16		AC-1, AC-2, AC-21, IA-5, PE-1, PE-2
C32	Acceptable usage of Information assets & systems	A.7.1.3			AC-20, PL-4
C33	Password policy	A.11.2.3	S12	N13	IA-5
C34	Default device credentials		S10		IA-5
C35	Monitoring and retention of logs		S6, S14	N15	PE-6, PE-8
C36	Unsuccessful login attempts				
C37	Ad-hoc access to systems	A.9.2.5			MP-5, PE-17
C38	Remote access	A.11.4.2			AC-17, AC-18, AC-20, CA-3, IA-2, IA-8
C39	Provisioning of personal devices		S3		MP-2, AC-19, AC-20
C40	Segregation of duties				
C41	User awareness & liability	A.8.2.1, A.8.2.2	S8, S20	N5	PL-4, PS-6, PS-7, SA-9, AT-2,

					AT-3, IR-2
C42	Map and characteristics of physical facilities				
C43	Hazard assessment	A.9.1.4		N22, N23	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8
C44	Hazard protection	A.9.1.4		N12, N22, N23	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8
C45	Securing gateways	A.9.1.2	S5	N9	PE-3, PE-5, PE-6, PE-7
C46	Identity badges				
C47	Entry of visitors & external service providers	A.9.1.3		N38	PE-3, PE-4, PE-5
C48	Visitor verification				PE-7, PE-8
C49	Infrastructure protection	A.9.2.3			PE-9
C50	Guarding facility	A.9.1.1, A.9.1.6		N12, N23	PE-3, PE-3 , PE-7, PE-16
C51	Vehicle entry	A.9.1.6		N12	PE-3 , PE-7, PE-16
C52	Correlation between physical and logical security	A.11.4.4	S4	N12	AC-3, AC-6, AC-17, AC-18, PE-3, MA-3, MA-4
C53	Monitoring & surveillance	A.9.2.1		N23	PE-1, PE-18
C54	Disposal of equipment	A.10.7.2		N20, N39	MP-6
C55	Protection of information assets and systems	A.9.1.1, A.10.7.3	S8	N12, N24	PE-3, MP-2, SI-12
C56	Authorization for change	A.10.1.2			CM-1, CM-3, CM-4, CM-5, CM-9
C57	Inactivity timeout	A.11.3.2, A.11.5.5			AC-11, IA-2, PE-3, PE-5, PE-18, SC-10, AC-11, SC-10
C58	Protection of access keys			N12, N24	
C59	Shoulder surfing				
C60	Categorization of zones				
C61	Access to restricted areas	A.9.1.3, A.9.1.5, A.9.2.7	S8	N7 , N12	AT-2, AT-3, PL-4, PS-6, PE-2, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8, PE-16, MP-5,
C62	Visitor device management	A.9.2.6			MP-6

C63	Physical access auditing and review	A.10.1.2, A.10.1.4, A.10.10.1		N34	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12
C64	Application security process	A.12.5.2, A12.4.1	S2, S6		CM-3, CM-4, CM-9, SI-2
C65	Application security architecture	A.12.5.2	S6, S7	N29	CM-3, CM-4, CM-9, SI-2
C66	Application User authentication		S2		
C67	Secure configuration	A.10.3.2, A.12.2.4	S2, S6	N29	CA-2, CA-6, CM-3, CM-4, CM-9, SA-11
C68	Ports & services		S11		CM-7, AC-17, AC-17
C69	Session management	A.11.5.6, A.11.5.5			NONE
C70	Input validation	A.12.2.1	S6, S7		SI-10
C71	Error handling	A.12.2.4	S7		NONE
C72	Application security testing	A.10.1.4	S6	N29	CM-2
C73	Code review	A.10.4.1		N29	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7
C74	Black box testing		S17	N16	RA-5
C75	Data handling				
C76	Least privileges	A.11.5.4	S8, S9		AC-3, AC-6
C77	Segregation of duties	A.10.1.3	S12	N7	AC-5
C78	Secure software development life-cycle (SDLC) processes	A.10.1.4, A.12.4.1, A.12.4.2	S6, S7	N29	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, PL-4, SA-6, SA-7,
C79	Application change control	A.12.5.1, A.12.5.3	S3, S6		CM-1, CM-3, CM-4, CM-5, CM-9, SA-10
C80	Application vulnerability intelligence				
C81	Application logs & monitoring		S6	N15	
C82	Data discovery				
C83	Data classification	A.7.1.2, A.7.2.1, A.7.2.2	S15		CM-8, CM-9, PM-5, RA-2, AC-16, MP-2, MP-3, SC-16
C84	Cryptography & encryption	A.10.9.2, A.12.3.1	S8, S12, S17	N17	SC-3, SC-7, SC-8, SC-9, SC-12, SC-13, SC-14, IA-7

C85	Key management	A.12.2.3, A.12.3.2	S12,	N17	AU-10, SC-8, SI-7, SC-12, SC-17
C86	Data-at-rest	A.10.8.3	S12	N17	MP-5
C87	Data-masking			N17	
C88	Database management		S16		
C89	Public mail and collaboration tools	A.10.8.4	S15		
C90	External media & printing devices	A.8.3.2, A.9.2.6, A.10.7.1	S5		
C91	Preventing loss of information	A.8.3.2, A.9.2.6, A.12.5.4	S15		PS-4, PS-5, MP-6, AC-4, PE-19
C92	Backup	A.10.5.1	S8, S19	N27	CP-9
C93	Data retention and disposal		S6	N39	
C94	Third party access				
C95	Monitoring & review				
C96	Breach management				
C97	Training and Awareness	A.8.2.2	S9, S20	N5	AT-2, AT-3, IR-2
C98	Employee verification	A.8.1.2			PS-3
C99	Authorizing access to third parties				
C100	Acceptable use policies	A.7.1.3	S2, S9		AC-20, PL-4
C101	Disciplinary processes	A.8.1.3, A.8.2.3	S9	N5	AC-20, PL-4, PS-6, PS-7, PS-8
C102	Record of authorized users				
C103	Monitoring and review				
C104	Non- disclosure agreements	A.6.1.5		N38	PL-4, PS-6, SA-9
C105	Legal and contractual obligations	A.6.1.5			PL-4, PS-6, SA-9
C106	Communication Practices				
C107	Interdependence of assets & systems				
C108	Standard operating environment	A.10.1.1, A.10.1.2, A.10.7.1	S3, S9	N6, N7	
C109	Threat assessment		S10	N35, N6, N13	
C110	Integration with external intelligence	A.6.2.1	S1, S2		CA-3, PM-9, RA-3, SA-1, SA-9, SC-7, CA-3, PS-7, SA-9
C111	Vulnerabilities knowledge management	A.12.6.1	S10, S6	N32, N30, N16, N18	
C112	Changing threat ecosystem		S4, S5	N35	
C113	Threats emanated from third parties	A.6.2.1, A.6.2.3	S4, S12		

C114	System hardening	A.12.2.2	S3	N31	
C115	Patch management		S3, S4		
C116	Malware protection	A.10.4.1	S5, S12, S20	N35	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7
C117	Perimeter threat protection	A.10.4.1	S1, S19, S4, S10, S20		AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7
C118	Protection from fraudulent activity				
C119	Configuration of endpoints		S3		
C120	Remediation		S5	N18 , N33	
C121	Security incident monitoring	A.10.2.2	S5		SA-9
C122	Incident management	A.13.1.2, A.13.2.1, A.8.2.3	S18	N10	PL-4, SI-2, SI-4, SI-5, IR-1
C123	Incident identification	A.13.2.3	S18	N10	AU-9, IR-4
C124	Incident evaluation	A.13.2.1	S18	N10	IR-1
C125	Escalation process	A.13.1.1, A.13.2.2, A.6.1.3, A.6.1.2, A.10.1.3	S18	N10	AU-6, IR-1, IR-6, SI-4, SI-5, IR-4
C126	Breach information	A.13.2.2, A.13.2.3	S1, S7	N5	IR-4, AU-9, IR-4
C127	Configuring devices for logging	A.10.10.4	S4, S6	N15	AU-2, AU-12
C128	Activity logging		S4, S6, S14	N15	
C129	Log information	A.10.10.3	S6, S14	N15	AU-9
C130	Log information correlation	A.10.10.3, A.10.10.4			
C131	Protecting Log information				
C132	Deployment of skilled resources				
C133	Incident reporting	A.13.1.1, A.13.1.2	S18	N10, N18	AU-6, IR-1, IR-6, SI-4, SI-5, PL-4, SI-2, SI-4, SI-5
C134	Sharing of log information with law enforcement agencies				
C135	Communication of incidents			N10, N18	

Annexure 9 – Mapping of NISP guidelines & controls with National Institute of Standards and Technology (NIST) cyber security framework

NIST Cybersecurity Framework		NISPG
Category	**Subcategory**	**Guidelines**
IDENTIFY (ID)		
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	G1
	ID.AM-2: Software platforms and applications within the organization are inventoried	
	ID.AM-3: Organizational communication and data flows are mapped	G64
	ID.AM-4: External information systems are catalogued	G58
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	G35
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Covered in policy section 8
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Covered in policy
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Covered in policy
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	G50
	ID.BE-5: Resilience requirements to support delivery of critical services are established	G55
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	Covered in policy
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Covered in policy
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Covered in policy
	ID.GV-4: Governance and risk management processes address cybersecurity risks	Covered in policy
Risk Assessment (ID.RA): The organization understands	ID.RA-1: Asset vulnerabilities are identified and documented	G51, G54

NIST Cybersecurity Framework		NISPG
Category	**Subcategory**	**Guidelines**
the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	G53, G54
	ID.RA-3: Threats, both internal and external, are identified and documented	G54
	ID.RA-4: Potential business impacts and likelihoods are identified	G57
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	G57
	ID.RA-6: Risk responses are identified and prioritized	G56
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	G95
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	
PROTECT (PR)		
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	G10, G11
	PR.AC-2: Physical access to assets is managed and protected	G21
	PR.AC-3: Remote access is managed	G14
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	G10, G15
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	G4
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	G43
	PR.AT-2: Privileged users understand roles & responsibilities	G46, G47
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	G40, G43
	PR.AT-4: Senior executives understand roles & responsibilities	G43
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	G15
Data Security (PR.DS):	PR.DS-1: Data-at-rest is protected	G38

NIST Cybersecurity Framework		NISPG
Category	**Subcategory**	**Guidelines**
Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-2: Data-in-transit is protected	G38
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	G1, G38, G50
	PR.DS-4: Adequate capacity to ensure availability is maintained	
	PR.DS-5: Protections against data leaks are implemented	G38, G41, G42
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	G34
	PR.DS-7: The development and testing environment(s) are separate from the production environment	G30, G32
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	G51
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	G32
	PR.IP-3: Configuration change control processes are in place	G34, G38, G49, G52
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	G38
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	G19
	PR.IP-6: Data is destroyed according to policy	G38
	PR.IP-7: Protection processes are continuously improved	G55, G58
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	G58, G62, G63
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	G55, G56, G102, G103
	PR.IP-10: Response and recovery plans are tested	G57, G103
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	G43
	PR.IP-12: A vulnerability management plan is developed and implemented	G55
Maintenance (PR.MA): Maintenance and repairs of industrial control and	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	G7, G8

NIST Cybersecurity Framework		NISPG
Category	**Subcategory**	**Guidelines**
information system components is performed consistent with policies and procedures.	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	G14
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	G2, G10, G41, G59, G72, G98
	PR.PT-2: Removable media is protected and its use restricted according to policy	G38
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	G10
	PR.PT-4: Communications and control networks are protected	G23, G24, G25
DETECT (DE)		
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	G7
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	G54, G57
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	G53, G54, G57, G58
	DE.AE-4: Impact of events is determined	G57, G58
	DE.AE-5: Incident alert thresholds are established	G56
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	G7, G8, G9, G45, G48, G54, G56
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	G20, G21
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	G23, G26, G41, G71
	DE.CM-4: Malicious code is detected	G30, G32, G33
	DE.CM-5: Unauthorized mobile code is detected	G74
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	G38, G40, G41, G54
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	G39, G41
	DE.CM-8: Vulnerability scans are performed	G49, G54, G55
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	G62, G70
	DE.DP-2: Detection activities comply with all applicable requirements	G57, G58
	DE.DP-3: Detection processes are tested	G57, G58

NIST Cybersecurity Framework		NISPG
Category	**Subcategory**	**Guidelines**
anomalous events.	DE.DP-4: Event detection information is communicated to appropriate parties	G63, G64
	DE.DP-5: Detection processes are continuously improved	G58
RESPOND (RS)		
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	G56
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	G62
	RS.CO-2: Events are reported consistent with established criteria	G64
	RS.CO-3: Information is shared consistent with response plans	G62, G64
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	G56, G52, G62, G64
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	G53, G54, G58
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities	RS.AN-1: Notifications from detection systems are investigated	G56
	RS.AN-2: The impact of the incident is understood	G54, G56, G57
	RS.AN-3: Forensics are performed	G56, G58
	RS.AN-4: Incidents are categorized consistent with response plans	G56
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	G56
	RS.MI-2: Incidents are mitigated	G55, G56
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	G56, G57
	RS.IM-2: Response strategies are updated	G56, G57

NIST Cybersecurity Framework		NISPG
Category	**Subcategory**	**Guidelines**
RECOVER (RC)		
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	G102, G103, G104, G105
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	G103, G105
	RC.IM-2: Recovery strategies are updated	G105
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	G64
	RC.CO-2: Reputation after an event is repaired	G64
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	G101, G102, G103

Annexure 10 – Introduction to international standards and frameworks

A. National Institute of Standards and Technology (NIST) cybersecurity framework

1.1. **Improving Critical Infrastructure Cybersecurity** was the subject of the Executive Order 13636, issued by President Obama on February 12, 2013. It vested the National Institute of Standards and Technology (NIST) with the responsibility of developing a voluntary cybersecurity framework. NIST coordinated the industry-led effort that draws on existing standards, guidelines, and best practices, to develop the Cybersecurity Framework. The Framework, aimed at the owners and operators of the critical infrastructure, is expected to help reduce cyber risks to critical infrastructure.

NIST began the development of the Cybersecurity Framework by issuing a Request for Information (RFI) in February, 2013, to gather relevant input from industry, academia, and other stakeholders to:

- Identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities;
- Specify high-priority gaps for which new or revised standards are needed; and
- Collaboratively develop action plans by which these gaps can be addressed

1.1.1. The idea was to use existing standards, guidelines and best practices to reduce cyber risk across sectors and develop capabilities to address the full-range of quickly changing threats. The framework will provide a flexible toolkit any business or other organization can use to gauge how well prepared it is to manage cyber risks and what can be done to strengthen its defenses

1.1.2. It is vital that companies understand their digital assets and accurately assess the maturity of their cyber protections so they can properly allocate resources. They need to continuously invest in maintaining awareness of existing threats to preventing, detecting, and responding to attacks to recovering from them.

1.1.3. The *Framework to reduce Cyber Risks to Critical Infrastructure*, after several rounds of public consultation, was released in February, 2014

1.2. **Outline of Cybersecurity Framework:** The focus is on defining the overall Framework and provides guidance on its usage. The Framework is intended to be used throughout the organization.

1.2.1. Senior executives can use it to evaluate how prepared they are to deal with potential cybersecurity-related impacts on their assets, and on their ability to deliver their business services and products

1.2.2. User guide will help organizations understand how to apply the Framework. It is not a detailed manual; it will help users at different levels to:

1.2.2.1. Understand and assess the cybersecurity capabilities, readiness, and risks of their organizations

1.2.2.2. Identify areas of strength and weakness and aspects of cybersecurity on which they should productively focus, and learn what informative standards, guidelines, and practices are available and applicable to their organizations

1.3. **The Framework's core structure:**

1.3.1. **Five major cybersecurity functions and their categories**, sub-categories, and information references. *Key functions: Know, Prevent, Detect, Respond, and Recover*. Broken further into categories, e.g. *prevent categories*: identity and access management, physical security, and training and awareness. It further identifies underlying *key sub-categories*. Then *matches them with informative references such as existing standards, guidelines, and practices for each sub-category*. A matrix showing the functions, categories, sub-categories, and informative references is provided.

1.3.2. **Three Framework Implementation Levels (FILs)** associated with an organization's cybersecurity functions and how well that organization implements the framework. Three implementation levels reflect organizational maturity. The approach rolls up functions and FILs in a way that allows them to assess an organization's risk and readiness viewed through their specific roles and responsibilities – whether they are senior executives, business process managers, or operations managers.

1.3.3. **A compendium of informative references**, existing standards, guidelines, and practices to assist with specific implementation

1.4. **The Framework has been designed and is intended to:**

1.4.1. Be an adaptable, flexible, and scalable tool for voluntary use

1.4.2. Assist in assessing, measuring, evaluating, and improving an organization's readiness to deal with cybersecurity risks

1.4.3. Be actionable across an organization

1.4.4. Be prioritized, flexible, repeatable, performance-based, and cost-effective to rely on standards, methodologies, and processes that align with policy, business, and technological approaches to cybersecurity

1.4.5. Complement rather than to conflict with current regulatory authorities

1.4.6. Promote, rather than to constrain, technological innovation in this dynamic arena

1.4.7. Focus on outcomes

1.4.8. Raise awareness and appreciation for the challenges of cybersecurity but also the means for understanding and managing the related risks

1.4.9. Be consistent with voluntary international standards

1.5. The NIST cybersecurity framework (provides a "language for expressing, understanding and managing cybersecurity risk, both internally and externally". It helps in identification and prioritization of actions for reducing risk and provides a tool for aligning policy, business and technological approaches to managing risk. The core framework consists of five functions:

1.5.1. **Identify:** develop visibility over systems, assets, data and capabilities which need to be protected, in accordance with their criticality

1.5.2. **Protect:** develop and implement appropriate safeguards, prioritizing through the organizations risk management process

1.5.3. **Detect:** develop and implement appropriate activities to identify occurrence of a breach of event

1.5.4. **Respond:** develop and implement appropriate activities to take action regarding a detected breach or event

1.5.5. **Recover:** develop and implement appropriate activities, to restore the appropriate capabilities that we impaired through a breach or event

B. DSCI Security Framework

1.1. Numerous organizations worldwide have adopted widely accepted & internationally recognized security frameworks and standards such as ISO 27001, which provide guidance & direction for establishing enterprise wide security program, processes and procedures. But problem arises when organizations channelize investments and resources to demonstrate compliance to such standards (e.g. extensive documentation, huge checklists) instead of identifying and mitigating real risks. Similar case has been observed with FISMA implementation in the United States – compliance to it has taken precedence over real security concerns in the networks and systems of the federal agencies. Thus focus has shifted towards the compliance, leaving maturity aspect at bay.

1.2. Given the rate at which attack proliferation has happened, and data breach incidents are increasing, organizations today need to develop and integrate a comprehensive security program to stay at pace with the attackers and attack vectors to stay secure. Threat environment in which we operate is getting complex and dynamic; attackers are evolving innovative techniques. In such a scenario, organizations cannot solely rely on certifications alone; though it may help provide assurance and demonstrate organization's commitment to their stakeholders and outside world. Though ISO 27001 standard, is a good starting point for organizations for implementing security, it is not an end by itself. When organizations operate in a vibrant, dynamic, evolving and competent environment – be it business, regulatory or threat environment as in case of security, organizations can only survive if they are able to draw a roadmap for coming years that entails future conditions & requirements, strategic options, building required competencies, etc. and not just focus on the present. This is achieved by doing long term planning and drawing a strategy to achieve the defined goals. But how many organizations today have a security strategy? How many organizations have a 5 year vision for security? Unfortunately - not many. Though, ISO 27001 has been phenomenal in establishing enterprise wide security processes, it falls short in the following areas:

1.2.1. ***Long Term Strategic Planning in Security*** –Today, security practitioners strongly believe that security should be treated as a business enabler and not as a hurdle – adding value to business, by allowing business to offer innovative solutions & services to international markets round the clock, increasing productivity, reducing cost, providing customer delight, etc. If such an approach needs to materialize, security needs to be revitalized by working more closely with the business and IT and being given strategic importance within the organization. Unfortunately, many standards are controls based standard - controls that are static in nature,

focused on mitigating the existing risks, not focused on addressing the futuristic requirements / risks that emerge from business expansion and innovation

1.2.2. ***Building Security Capability / Competence, using Maturity Criteria*** - Security is a continuous journey, and no organization can be 100% secure. However, it is important to measure the progress made / capabilities built over a period of time to address the evolving and perennial threats. This can be achieved by defining criteria against which an organization can measure its capability maturity in security. Many standards on the other hand promotes a 'yes/no' kind of approach to security, wherein an organization is certified as fully compliant if it has implemented the relevant controls. It does not provide any maturity criteria, which organizations can leverage to improve their security competence

1.2.3. ***Focus on Protecting Data*** – Many standards follow an asset centric and process oriented standard. Processes help provide guidelines for conducting operational tasks in a pre-defined manner, but if too much focus is given on processes, then it may happen that the objective for deploying a particular process may get lost (outcome may not be achieved). This also at times results in loss of productivity and is perceived as bureaucratic. In today's digital world, data has an economic value attached to it. In fact, in some industries like pharmaceutical, data is the life line of the organizations operating in the sector. Hackers and rogue insiders vie for this critical data. In such a scenario, the focus of all the security efforts should be on data, with lean processes and intelligent technologies deployed to protect it

1.2.4. ***Tracking Security Evolution*** – Security as a discipline has evolved over a period of time. The stimuli have been many - the dynamic threat landscape, strengthening regulatory regime, research & innovation, globalization, business models, technologies, etc. For an organization to be secure it is important that it keeps track of all the latest developments taking place in the field of security – be it skills, technologies or services. Today, specific security disciplines have evolved with very specific approaches to address the unique challenges faced. Specific trends and practices have been emerging to address the exact requirements of an individual discipline. The security market, both technology products and services, has solution offerings specific to an individual discipline. Security profession is also charting a path of specialization in these individual security disciplines. For e.g. Management of threats & vulnerabilities is a very critical discipline today, requiring specific skills, technologies and practices. Similarly, disciplines like Secure Content Management, Governance, Risk and Compliance do not find their rightful place in ISO 27001 standard. It fails to provide strategic and contemporary directions and guidance to organizations that are implementing and maintaining security

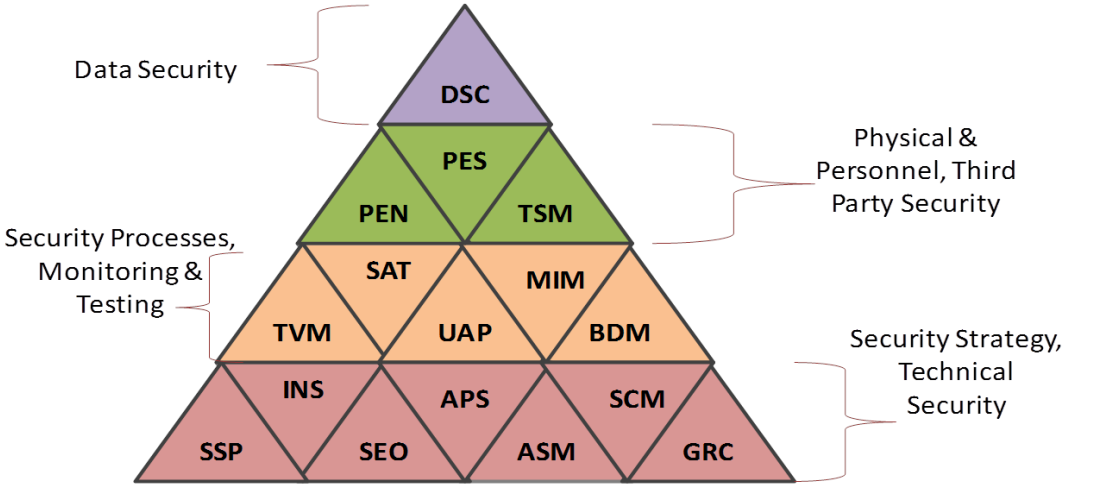
1.2.5. ***Integration and Interdependencies –*** Security disciplines, as explained in the point above, have number of interdependencies and therefore there is need for taking an integrated approach that links these disciplines appropriately for better protection. For e.g. Security Incident Management as a discipline requires inputs from Threat & Vulnerability Management, Infrastructure Management, Application Development, etc. to be effective. The ISO 27001 standard does not take such an integrative approach as it is focused on individual controls that are described and deployed in silos

1.2.6. There is a need to approach security differently - a way that helps overcome the above shortcomings of ISO 27001 and enables an organization focus on real threats in its environment, without worrying about compliance to regulations. It should be able to assess

organization's maturity in implementing security in different areas with a view to continually improve the same. Such an assessment should further help organization draw a strategic plan based on evolution of different disciplines of security, and their interdependencies, with continuous focus on protecting data. Compliance should be the outcome along with dynamic and vibrant security that enables quick response to threats, vulnerabilities and actual cyber-attacks

1.3. DSCI Security Framework (DSF©) is based on the following three foundational elements:

1.3.1. ***Security Principles***: Starting point of DSF© is a set of security principles that an organization should seek to adhere to. These include information ***visibility, vigilance, coverage & accuracy,***



SSP – Security Strategy & Policy	**SEO** – Security Organization	**ASM** – Asset Management	**GRC** – Governance, Risk & Compliance
INS – Infrastructure Security	**APS** – Application Security	**SCM** – Secure Content Management	**TVM** – Threat & Vulnerability Management
UAP – User Access & Privilege Management	**BDM** – Business Continuity & Disaster Management	**SAT** – Security Audit & Testing	**MIM** – Monitoring & Incident Management
PEN – Physical & Environmental Security	**TSM** – Third Party Security Management	**PES** – Personnel Security	**DSC** – Data Security

discipline in defense; ***focus on strategic, tactical and operational layers and compliance demonstration***. DSCI believes that approach to security which is based on these principles helps remove the focus from extensive documentation, checklists and controls, and enables an organization achieve dynamism in security which gives it the agility to respond to threats and attacks.

1.3.2. ***Discipline Specific Approach***: DSF© view of security is ***discipline-specific***. Unlike other standards, it does not specify any controls. Instead, it outlines best practices in these disciplines that are based on recent learning by organizations, analysts, and technology and solution providers. It leaves to the organization to select and implement controls specific to its operating environment and business requirements

1.3.3. It identifies maturity criteria in each of the 16 disciplines that form part of DSF©. While these disciplines are organized in four layers, it encourages organizations to focus on each individual discipline of security by implementing best practices, and moving up in maturity rating by using the maturity criteria. Focus on individual disciplines, and striving to achieve excellence in them is the path to real security.

1.3.4. ***Data-Centric Methodology***. DSCI focuses on a 'Visibility' exercise, which brings a consolidated view of data at the central level. It analyses and identifies the integrated view of the data within the findings. It creates a risk profile that is data centric. DSCI makes uses of its Best Practices approach to evaluate strategic options, both in terms of the processes and technological solutions available for addressing these risks, and strengthening the security posture. DSCI believes that once visibility over data is created at the central level, it is easier to bring dynamism in the security program as recent trends, vulnerabilities and incidents can be considered and appropriate risk management measures can be taken on a continuous basis.

1.3.5. Corollary to the visibility exercise is the establishment of privacy initiatives in the organization, since the flow of personal information processed reveals exposure to privacy risks at various stages. The DSCI Privacy Framework (DPF©), which has identified nine privacy principles for achieving privacy in an organization, through the implementation of nine best practices which are organized in three layers – Privacy Strategy & Processes, Information Usage, Access, Monitoring & Training and Personal Information Security for establishing privacy initiatives in an organization, helps an organization do that

1.4. Practices in each discipline of DSF© have been articulated under the following four sections:

1.4.1. ***Approach to the Security Discipline***: DSCI believes that there is a significant requirement of discussing the approaches, trends and practices that are driving an individual discipline. This section in each discipline articulates DSCI approach towards the discipline under discussion.

1.4.2. ***Strategy for the Security Discipline***: DSCI also believes that each security discipline deserves a strategic treatment that will not only mature its endeavor but also optimize the resources and efforts deployed. For each discipline, DSCI recommend approaches and processes that help take a strategic review of an organization's initiatives. This section will help managers to provide a strategic direction to the organization's initiatives in each discipline.

1.4.3. ***Best Practices for the Security Discipline***: DSCI recognizes a need for providing a detailed guidance for systematically planning and implementing security in the organization. This section, in each discipline, compiles the best practices for the security implementer.

1.4.4. ***Maturity of the Security Discipline: DSCI believes in assessment of the outcomes and for fair*** assessment, comprehension of appropriate parameters is necessary. The DSF© has defined a total of *170 maturity criteria* for the 16 disciplines.

1.4.5. DSF© especially through its maturity criteria can be used to determine an organization's security capability in different disciplines of security. This can be of particular relevance in outsourcing relationships where client organizations want to determine the overall and / or Line of Service specific security capability of service provider organizations.

1.5. Framework Benefits

DSF© offers key benefits as follows:

Offers a set of principles for implementation of true security	*Helps align security to current trends understanding & practices*	*Focuses on bringing relevance to security, hence, realistic security*
Provides means to improve dynamism in security	*Ensures comprehensiveness & coverage through the disciplines*	*Provides strategic directions to security initiatives*
Offers detailed guidance for implementation	*Supports maturity improvement through outcome based metrics*	*Promises revitalization of security initiatives for data security*
Provides means for integration, convergence & collaboration	*Content support to manager, implementer, consultant, auditor*	*Comprehensive and structured ecosystem around the framework*

C. PCI – DSS

1.1. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies that process, store or transmit credit card information maintain a secure environment and that operations and transactions are secure

1.2. The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.). The Standard can be found here: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

1.3. PCI DSS 2.0 (Payment Card Industry Data Security Standard Version 2.0) is the second version and was released in 2010. The third revision is due in 2014.It is important to note, the payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

1.4. The PCI DSS specifies and elaborates on six major objectives[1]:

1.4.1. First, a secure network must be maintained in which transactions can be conducted. This requirement involves the use of firewalls that are robust enough to be effective without causing undue inconvenience to cardholders or vendors. Specialized firewalls are available for wireless LANs, which are highly vulnerable to eavesdropping and attacks by malicious hackers. In addition, authentication data such as personal identification numbers (PINs) and passwords must not involve defaults supplied by the vendors. Customers should be able to conveniently and frequently change such data

1.4.2. Second, cardholder information must be protected wherever it is stored. Repositories with vital data such as dates of birth, mothers' maiden names, Social Security numbers, phone numbers and mailing addresses should be secure against hacking. When cardholder data is transmitted through public networks, that data must be encrypted in an effective way. Digital

[1] http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

encryption is important in all forms of credit-card transactions, but particularly in e-commerce conducted on the Internet

1.4.3. Third, systems should be protected against the activities of malicious hackers by using frequently updated anti-virus software, anti-spyware programs, and other anti-malware solutions. All applications should be free of bugs and vulnerabilities that might open the door to exploits in which cardholder data could be stolen or altered. Patches offered by software and operating system (OS) vendors should be regularly installed to ensure the highest possible level of vulnerability management

1.4.4. Fourth, access to system information and operations should be restricted and controlled. Cardholders should not have to provide information to businesses unless those businesses must know that information to protect themselves and effectively carry out a transaction. Every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be protected physically as well as electronically. Examples include the use of document shredders, avoidance of unnecessary paper document duplication, and locks and chains on dumpsters to discourage criminals who would otherwise rummage through the trash

1.4.5. Fifth, networks must be constantly monitored and regularly tested to ensure that all security measures and processes are in place, are functioning properly, and are kept up-do-date. For example, anti-virus and anti-spyware programs should be provided with the latest definitions and signatures. These programs should scan all exchanged data, all applications, all random-access memory (RAM) and all storage media frequently if not continuously

1.4.6. Sixth, a formal information security policy must be defined, maintained, and followed at all times and by all participating entities. Enforcement measures such as audits and penalties for non-compliance may be necessary

1.5. The 12 requirements of PCI DSS are as follows:

1.5.1. Install and maintain a firewall configuration to protect cardholder data

1.5.2. Do not use vendor-supplied defaults for system passwords and other security parameters

1.5.3. Protect stored cardholder data

1.5.4. Encrypt transmission of cardholder data across open, public networks

1.5.5. Use and regularly update antivirus software

1.5.6. Develop and maintain secure systems and applications

1.5.7. Restrict access to cardholder data by business need-to-know

1.5.8. Assign a unique ID to each person with computer access

1.5.9. Restrict physical access to cardholder data

1.5.10. Track and monitor all access to network resources and cardholder data

1.5.11. Regularly test security systems and processes

1.5.12. Maintain a policy that addresses information security

D. SANS 20 Controls

1.1. SANS has created the "20 Critical Security Controls" as a way of providing effective cyber defense against current and likely future Internet based attacks. Following these 20 controls will help establish, in their words, a "prioritized baseline of information security measures and controls." The target audience is Federal enterprise environments but it certainly could be used by commercial organizations.

1.2. It is a set of recommendations developed by a consortium of companies with the purpose of identifying specific controls that will make systems safer. In addition, most of the controls can be automated to various degrees through the use of tools.2

1.3. They offer a prioritized list of controls that have the greatest impact on improving security posture against real-world threats. Consortium for Cybersecurity Action (CCA) was established in 2012 to ensure that updated versions of the Critical Controls incorporate the most relevant threat information and to share lessons learned by organizations implementing them. The Critical Controls encompass and amplify efforts over the last decade to develop security standards, including the Security Content Automation Program (SCAP) sponsored by the National Institute of Standards and Technology (NIST) and the Associated Manageable Network Plan Milestones and Network Security Tasks developed by the National Security Agency (NSA).3

1.4. The presentation of each Critical Control includes:

1.4.1. Proof that the control blocks known attacks and an explanation of how attackers actively exploit the absence of this control.

1.4.2. Listing of the specific actions that organizations are taking to implement, automate, and measure effectiveness of this control. The sub-controls are grouped into four categories:

1.4.3. Quick wins that provide solid risk reduction without major procedural, architectural, or technical changes to an environment, or that provide such substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

1.4.4. Visibility and attribution measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

1.4.5. Improved information security configuration and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

1.4.6. Advanced sub-controls that use new technologies that provide maximum security but are harder to deploy or more expensive than commoditized security solutions.

[2] http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf
[3] http://www.sans.org/critical-security-controls/guidelines.php

E. NIST 800-53

1.1. NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," catalogs security controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002 (FISMA) and to help with managing cost effective programs to protect their information and information systems

1.2. NIST Special Publication 800-53 is part of the Special Publication 800-series that reports on the Information Technology Laboratory's (ITL) research, guidelines, and outreach efforts in information system security, and on ITL's activity with industry, government, and academic organizations. The catalog of security controls in Special Publication 800-53 can be effectively used to protect information and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios

1.3. Specifically, NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. This includes selecting an initial set of baseline security controls based on a FIPS 199 worst-case impact analysis, tailoring the baseline security controls, and supplementing the security controls based on an organizational assessment of risk. The security rules cover 17 areas including access control, incident response, business continuity, and disaster recoverability

1.4. A key part of the certification and accreditation process for federal information systems is selecting and implementing a subset of the controls (safeguards) from the Security Control Catalog NIST 800-53, (Appendix F). These controls are the management, operational, and technical safeguards (or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. To implement the needed safeguards or controls, agencies must first determine the security category of their information systems in accordance with the provisions of FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." The security categorization of the information system (low, moderate or high) determines the baseline collection of controls that must be implemented and monitored. Agencies have the ability to adjust these controls and tailor them to fit more closely with their organizational goals or environments

1.5. The guidelines have been developed to achieve more secure information systems and effective risk management within the federal government by:[4]

1.5.1. Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;

[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

1.5.2. Providing a stable, yet flexible catalog of security controls to meet current information protection needs and the demands of future protection needs based on changing threats, requirements, and technologies;

1.5.3. Providing a recommendation for security controls for information systems categorized in accordance with FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems;

1.5.4. Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and

1.5.5. Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

1.6. In addition to the security controls described above, this publication: i) provides a set of information security program management controls that are typically implemented at the organization level and not directed at individual organizational information systems; ii) provides a set of privacy controls based on international standards and best practices that help organizations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards; and iii) establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs, and organizations. Standardized privacy controls provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance to those requirements. Incorporating the same concepts used in managing information security risk, helps organizations implement privacy controls in a more cost-effective, risked-based manner

F. COBIT

1.1. COBIT[5] is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

1.2. With COBIT 5, ISACA introduced a framework for information security. It includes all aspects of ensuring reasonable and appropriate security for information resources. Its foundation is a set of principles upon which an organization should build and test security policies, standards, guidelines, processes, and controls:

1.2.1. Meeting stakeholder needs

1.2.2. Covering the enterprise end-to-end

1.2.3. Applying a single integrated framework

1.2.4. Enabling a holistic approach

1.2.5. Separating governance from management

[5] http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

1.3. Principle 1: Meeting stakeholder needs[6]: A group of stakeholders includes any individual or group affected by the current state or future state of a process, system, policy, etc. Stakeholder analysis is the process of identifying stakeholders so that their input can ensure outcomes match requirements. This is an important step in both project planning and risk management. Failure to involve all stakeholders, including InfoSec and audit teams, usually results in less than optimum outcomes at best. Worst case outcomes include failed projects or material audit deficiencies. Successful stakeholder analysis results in maximizing benefits, minimizing risk to or beyond expected outcomes, and optimizing resources. Further, ensuring integration of business and information assurance requirements into the development or acquisition of a solution is always preferable to trying to "hang" something onto a finished—but incomplete—system, network, or a physical controls framework.

1.4. Principle 2: Covering the enterprise end-to-end: Information security is often applied as series of point solutions, as defined in more detail in Principle 3. However, general application of security and assurance best practices requires security reviews as part of all business processes and IT development and implementation activities. This isn't just a horizontal integration. Rather, all levels of management must include InfoSec in every business strategic and operational planning activity.

1.5. Principle 3: Applying a single integrated framework: Application of security controls is often a point-and-shoot activity. Many organizations tend to fix specific issues without stepping back and applying policies and controls that impact multiple vulnerabilities in network or system attack surfaces. Designing a complete framework includes all aspects of information storage, flow, and processing, providing a foundation for more efficient control implementation.

1.6. Principle 4: Enabling a holistic approach: As support for developing an integrated framework, it's important to see information security as a set of related components: not as set of silos. Each component is driven by enablers and other factors affecting organization risk. COBIT 5 for Information Security provides a list of enablers and describes how they interrelate. Enablers help organizations integrate operations and security into the outcomes of all principles defined here. As always, this is done in a way to meet stakeholder requirements.

1.7. Principle 5: Separating governance from management: This principle establishes a line between setting objectives and measuring outcomes. According to COBIT 5 for Information Security:

"Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balances, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives."

While governance and management are separate functions performed by designated teams, they must support each other. Governance defines outcomes and management implements technology and processes to meet those outcomes. Governance then determines if outcomes are met and provides feedback to help management make necessary adjustments.

[6] http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/#.

Annexure 11 – Security as business imperative

1.1. **The Cost of Security:** Traditionally, Information security has focused resources to keep all assets within the environment of the government ministry/department by building secure firewalls to ward off any attacks. However, with an evolving threat landscape that includes social engineering, spear phishing, etc., there may be several vulnerable attack points, which make it imperative for the security function to be revitalized. If organizations fail to understand the value of their own assets, risk becomes immaterial; therefore it is important to put a value on information from several perspectives. Information security should be seen as a solution that reduces the fear by creating trust. Trust that the risk is taken away and used for malicious intent and activities detrimental to the security and interests of our nation

1.2. Any security breach or loss of information may have an adverse impact on the functioning of government organizations and may have an adverse impact on national security or national interests. A breach in the United States - referred to as *wiki-leaks* - led to public disclosure of thousands of confidential government reports, documents, intelligence and diplomatic cables; much to the embarrassment of the US government. A security breach may not only cause loss of information and data, but also have a daunting financial effect, loss of reputation and confidence of the public against the government, which may lead to an overall decrease in trust in the government, litigation or lead to adverse conditions for national security and national interests. There have been similar incidents worldwide, as illustrated in the table below.

Large Data Breaches	
Heartland information systems	130 Million credit cards information
National Archives	76 million records
Sony Play station	77 million and 24.6 million records in 2 separate incidents
Sega Website attack	1.29 million customer records

Cyber Espionage: Stealing Sensitive Info	
Operation 'Shady RAT'	Widespread cyber espionage *5 Years | 14 countries | 70 Public & Private Cos*
Operation 'Night Dragon'	Targeted Oil & Energy Cos *5 Years | 14 countries | 70 Public & Private Cos*
Nitro Attack	Info on Advanced Materials *Chemical Cos| Defense Industry*
Rockwell & Boeing	Info on B1 Bomber *25000 pages of sensitive Info*
German Insider	Economic Espionage *Helicopter technology*

1.3. Other similar breaches have been reported worldwide and continue to menace governments and the industry. To stay ahead of the evolving security threat curve, government bodies need to be proactive, rather than being reactive to incidents and breaches. The real benefits of a robust security framework and practices and the return on investment made on security may not be directly realized; however organizations need to understand the importance and value of robust security architecture after an incident occurs – which involves additional, avoidable costs to the government. Global studies have indicated that in the majority of cases, investment in quality, effective IT security would have been considerably less than the costs incurred following a breach.

Annexure 12 – Positioning of security division within the organization

1.1. Security Division traditionally has been part of the IT department within an organization. However, over a period of time, there emerged many elements that needed attention of the security division, which fall outside the boundaries of IT. Security requires organization wide efforts to bring different functions together; establish collaboration that spreads awareness and seeks cooperation; focuses on coordination while managing security affairs, and requires integrated approach while analyzing and solving the problems. Positioning of the security division matters a lot for its effectiveness and security organization has to be independent of IT and perhaps report to the board. Some of the key recommendation for establishing security organization should be:

1.1.1. The growing complexity of managing security, increasing role of security in the success of ventures, and rising exposure of a government organization to these risks necessitates the elevation of security in an organization's ecosystem. Security should be part of the strategic planning of organization and should be involved in the compliance management or organizations risk management functions. It should coordinate with other government organizations such as departments/ ministry for ensuring security as part of the service delivery

1.1.2. The key skills required by a successful security leader or CISO should be more managerial, collaborative and communicative, rather than primarily technical. She/he should have the ability to build consensus and influence decisions, inside the organization and within IT

1.1.3. The Security leader or CISO should ensure that his team has the necessary skill-set and competencies, both from procedural and technical aspects across relevant security domains within the organization. He/she should ensure that there is adequate number of qualified professionals; and wherever required the gaps should be full-filled through services from subject matter experts by options such as hiring 3rd parties/contracts/offshore models

Annexure 13 – Risk Assessment for information security

1.1. **Purpose**

1.1.1. Risk assessments are a means of informing the management on information security risks; provide insights into effectiveness of existing control measures (including alternative plans); and help determine what is necessary to reduce risks to information to a reasonable level

1.1.2. Risk assessment requires application of management policies, procedures and practices to the tasks of identifying, analyzing, treating, and monitoring risk and includes assessment of risk based on the context and criticality of information assets to organizations

1.1.3. As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage. Regardless of the types of risk being considered, all risk assessments generally include the following elements:

1.1.3.1. Identifying threats that could harm and, thus, adversely affect classified information and information assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters

1.1.3.2. Identify information security threats relevant to the information they hold

1.1.3.3. Assessing vulnerabilities, both internal and external to organizations

1.1.3.4. Estimating the likelihood that such threats will materialize based on historical information

1.1.3.5. Identifying the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important

1.1.3.6. Estimating, the potential losses or damage that could occur if a threat materializes, including recovery costs

1.1.3.7. Analyzing impact (i.e., harm) to national security and internal security, and the likelihood that harm will occur with disclosure, theft or misuse of such information

1.1.3.8. Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls

1.1.3.9. Deploying appropriate controls or measures which adequately respond to information risk or reduce the impact or help in evaluating the alternative courses of action or determine appropriate courses of action consistent with organizational, and/or national risk acceptance

1.1.3.10. Documenting the results and developing an action plan

1.1.3.11. Assessing the residual risks and undertake monitoring measures for appropriate governance through determination of the effectiveness of risk responses consistent with organizational risk frame and identify risk-impacting changes to organizational information systems

1.1.3.12. Verifying that planned risk responses are implemented and information security requirements derived from and traceable to organizational functions, national security requirements, government directives, regulations and guidelines are satisfied

1.2. **Threats to information**

1.2.1. Information systems are subject to threats because of *either known or unknown vulnerabilities or the change in the threat landscape* or when *there are inadequate controls/measures over the known vulnerabilities*.

1.2.2. Although addressing vulnerabilities in an operational ecosystem is the primary reason for conducting risk assessment, organization should be aware of the fact that any change in the current process/technological ecosystem or addition of new components (process/technology) may expose it to new security risk that may compromise national security.

1.2.3. The applicability of these threats depends on the *details of the evaluation of the vulnerabilities or newer or changed processes, and can have adverse effects on operations and assets, individuals, organizations, and the nation, through exploitation of both known and unknown vulnerabilities compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems*

1.2.4. Threats to information systems can include purposeful attacks to information system, environmental disruptions, human/machine errors, and structural technological integration issues, process failures, and can result in harm to the national and economic security interests of the country

1.2.5. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the IT and operational functions of their organizations. One of the important mitigating factors is clear and unambiguous responsibilities for each role, and positioning trained personnel for that role

1.3. **Risk Assessment Indicators**

1.3.1. The Risk Assessment table below provides guidance to organizations on indicators of key risks and advises them on the security impact that a trigger might impose on the organization

1.3.2. The model below is indicative and only provides reference ideas for an organization to make use of, while conducting risk assessment exercise

1.4. **Scope and Applicability of Risk Assessments**

1.4.1. Risk assessment is a key part of effective information security management and facilitates decision making at all tiers of operations including at ***organization level, operational process level, and information system level***. Risk assessments are generally conducted throughout the system development lifecycle, from pre-system acquisition (i.e., solution analysis and technology development), system acquisition (i.e., development and production deployment), and on implementation (i.e. operations/support).

1.4.2. There are no specific requirements with regard to level of detail that characterizes any particular risk assessment. The methodologies[7], tools, and techniques used to conduct such risk assessments or the format and content of assessment results and any associated reporting mechanisms vary from organization to organization depending on requirement and information sensitivity.

1.4.3. Organizations should be cautioned that risk assessments are often not precise instruments of measurement and reflect the limitations of the specific assessment methodologies, tools, and techniques employed; the subjectivity, quality, and trustworthiness of the data used; the interpretation of assessment results; and the skills and expertise of those individuals or groups conducting the assessments.

1.4.4. *Risk assessments can support a wide variety of risk-based decisions and activities by organizational officials across all three tiers in the risk management.* As organizational functions, processes, information systems, threats, and environments of operation tend to change over time, *the validity and usefulness of any risk assessment is bounded with time.*

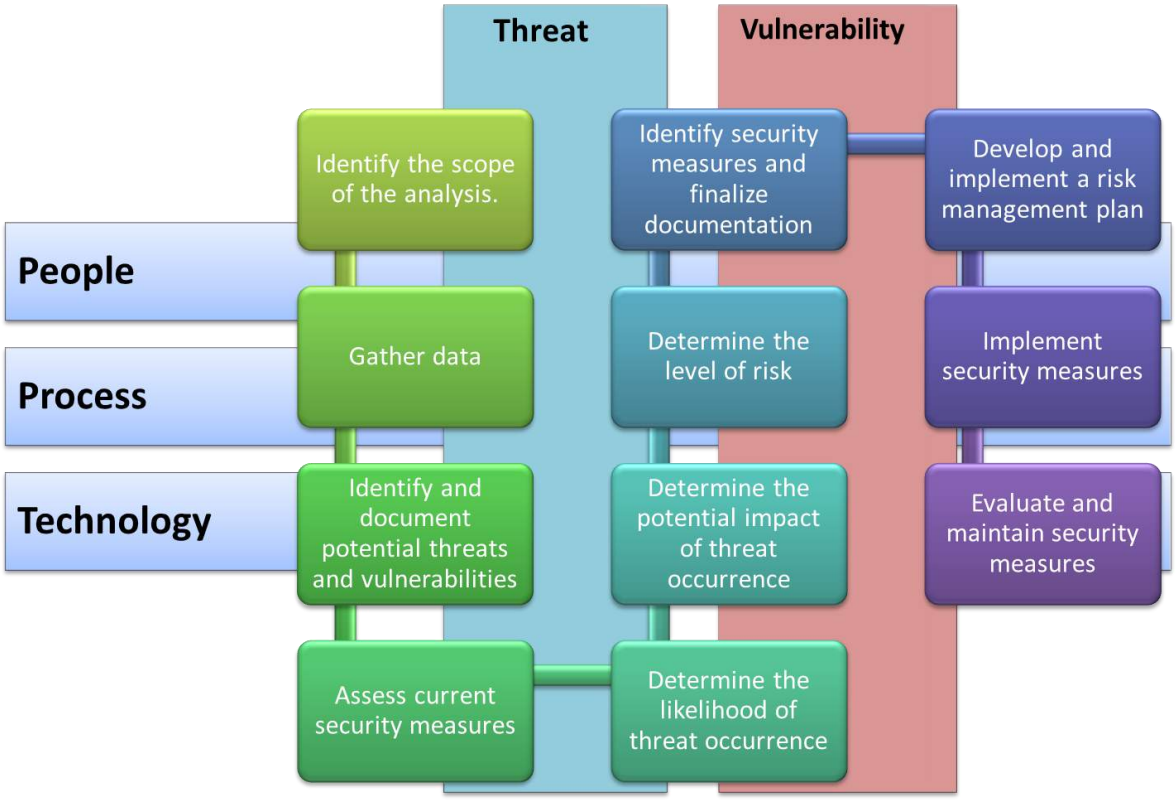


Figure 4: Risk Assessment overview

1.5. **Key Recommendations**

1.5.1. Risk assessment is an important measure of organization effectiveness towards information security and provides management requisite information needed to determine appropriate courses of action in response to identified risks. For providing a comprehensive view to the management, it is imperative that security leaders perform the following:

[7] Risk Assessment Methodologies: 1. OCTAVE - http://www.cert.org/octave/, 2. COSO - http://www.coso.org/ 3. FMEA - http://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis

1.5.1.1. Work with management and department heads to identify information and classify it based on its sensitive to information security. They should develop information security policies and standards that focus on protection of critical processes and technology that have implication on organizational security

1.5.1.2. Adopt a strategic Information risk management approach that balances national requirements with the objectives of the organization. They need to work with the management and department heads to identify and resolve information risks arising from technology or operational process on an ongoing basis

1.5.1.3. Centralize Information security risk program to enable a composite view of risk issues across the organization and its partner ecosystem i.e. suppliers, vendors, service providers, etc. It needs to establish consistent risk assessment and compliance processes that help the organization understand its information security risk exposure

1.5.1.4. Establish clear accountability between the organization and IT for Information security risk and define liabilities in case of breach of information

1.6. **Initiating a Risk Assessment**

1.6.1. There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors

1.6.2. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. A quantitative approach should estimate the ramification towards national security and internal security due to risk based on (1) the likelihood that a damaging event will occur, or threats on classified information shall be realized, (2) the importance of classified information towards national security and internal security, and (3) the potential costs and consequence of mitigating actions that could be taken

1.6.3. When reliable data is not available to draw such conclusions, a qualitative approach can be taken by defining risk in more subjective and general terms such as high, medium, and low. In this regard, qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods

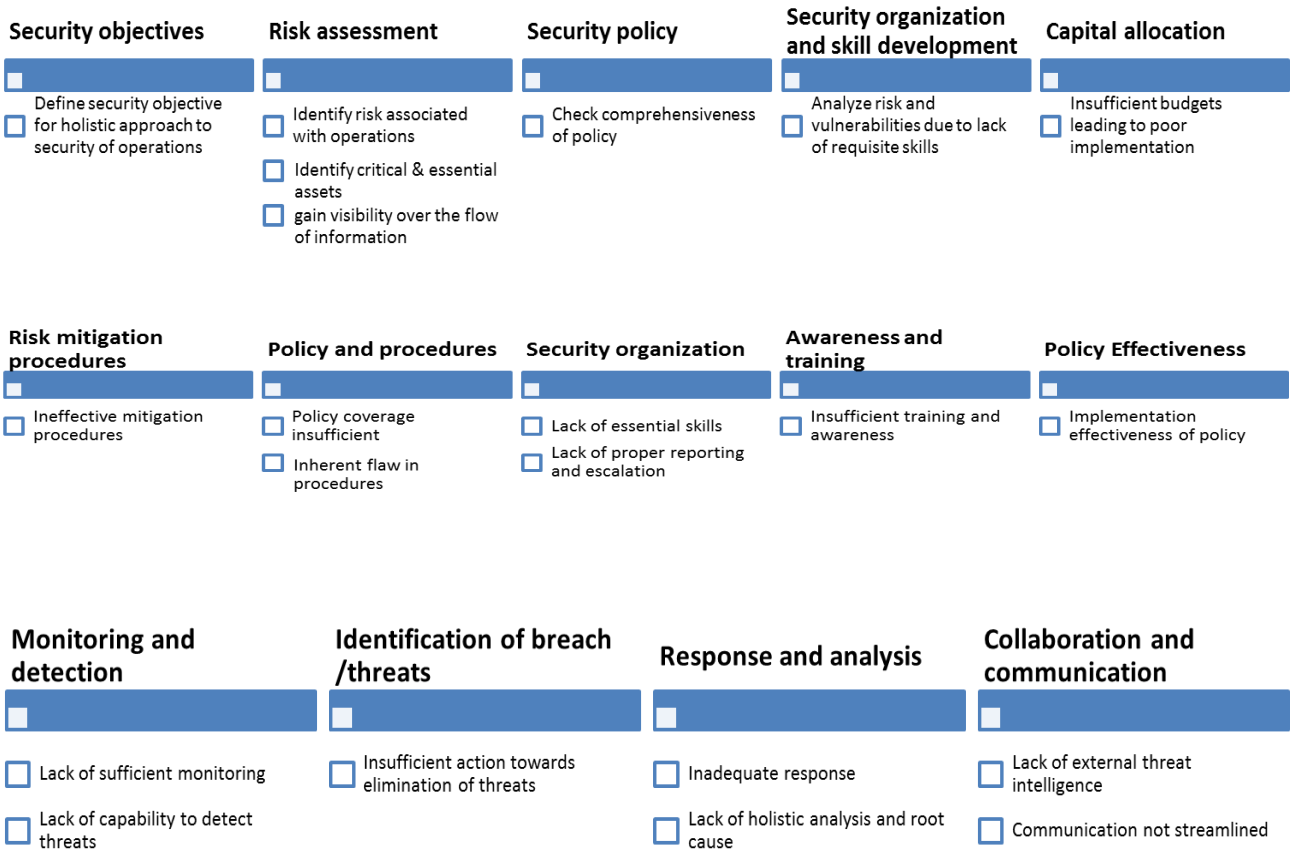
1.6.4. A few sample security risk assessment triggers are mentioned in the table below:

Trigger	Details	Security aspects	Decisions
Known/unknown vulnerability or change in threat landscape	Information that may be sensitive to national security	Criticality of the information towards national security	Is the information under threat of national concern? What will be the impact of loss?
Residents/ consumer	Operational needs	Activities/ tasks that	How is the consumer

requirement	expand, leading to increase in the amount of threats and vulnerability.	that may expose information of national importance	involved in the operational process? What is the nature of engagement of the organization? What actions of consumer can lead to threat to information?
Function/processes • ***Process flow*** • ***Process design***	Impact on process & services delivery, making use of information	Sensitivity of information use in business processes New possibilities of exposure & leakage of information	Cost of technology? • Risk of Failure • Implementation challenges • Threat to business
Technology adoption • ***Infrastructure*** • ***Applications*** • ***End points*** • ***Access interfaces*** • ***Storage options*** • ***Web/cloud/mobile*** • ***Analytics***	Impacted Application /product/ system/ interfaces using information Access/ transfer /ports /protocol/ services accessing information Information Services provided - On-premise, cloud, mobile, Social	Expectations of information security risk arising due to vulnerabilities & threat from technological usage, their configurations & Integrations Integration issues with legacy systems /applications/endpoint Security architecture/ controls/ new measures aligned to security	Budget implication of Efforts, resources, process & technology?
Resources • ***Leadership*** • ***SMEs*** • ***Vendor arrangements*** • ***Outsourcing Model***	Type of skills (area , level, (process/technology) / No. of resources, experience In-house/outsource who handle	Proportionality of skilled resources to information security requirements Insider Threats, Unintentional data leakage	Will control over information hamper transparency/ accountability for the organization?

	information		
Geographical /operating location	Location Hazards/ Physical Access and continuity impacting information	Physical and Environmental security issues having an impact on Information access	How will physical and environmental security be hampered by operating in a specific location?
Outsourcing arrangement	External parties/ providers having access to information	Audit & Monitoring issues; contractual obligations	How do we ensure security of information in the outsourced environment?
Compliance/ regulations	Liability/fines demonstration measure	Governance & Legal Challenges	What regulations/ compliance need to be adhered with?

1.6.5. Security risk assessment sample areas



Annexure 14 – Glossary

S.no.	Term	Definition
1.	Access Control Mechanism	Security safeguards i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.
2.	Access Type	Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types.
3.	Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
4.	Administrative Account	A user account with full privileges on a computer
5.	Advance Persistent Threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors e.g., cyber, physical, and deception. These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: i) pursue its objectives repeatedly over an extended period of time; ii) adapts to defenders' efforts to resist it; and iii) is determined to maintain the level of interaction needed to execute its objectives.
6.	AES	Advanced Encryption Standard, is a symmetric block data encryption technique.
7.	AP	A wireless Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.
8.	Application	A software program hosted by an information system; Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.
9.	Attribute-Based Access Control	Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.
10.	Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

11.	Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
12.	Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
13.	Back Door	Typically unauthorized hidden software or hardware mechanism used to circumvent security controls.
14.	Baseline Security	The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.
15.	BCP	Business continuity planning identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity.
16.	Black Box Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.
17.	Botnets	Collection of computers that are infected with small bits of code bots) that allows a remote computer to control some or all of the functions of the infected machines. The bot-master who controls the infected computers has the ability to manipulate them individually, or collectively as bot armies that act in concert. Botnets are typically used for disreputable purposes, such as Denial of Service attacks, click fraud, and spam.
18.	Boundary Protection Device	A device with appropriate mechanisms that: i) facilitates the adjudication of different interconnected system security policies e.g., controlling the flow of information into or out of an interconnected system); and/or ii) provides information system boundary protection.
19.	BS 25999	BS 25999 is the British Standards Institution (or BSI) standards for business continuity management.
20.	Buffer overflow	The result of a programming flaw. Some computer programs expect input from the user for example; a Web page form might accept phone numbers from prospective customers). The program allows some virtual memory for accepting the expected input. If the programmer did not write his program to discard extra input e.g., if instead of a phone number, someone submitted one thousand characters), the input can overflow the amount of memory allocated for it, and break into the portion of memory where code is executed. A skillful hacker can exploit this flaw to make someone's computer execute the hacker's code. Used interchangeably with the term, "buffer overruns."
21.	CMF	A content management framework (CMF) is a system that facilitates the use of reusable components or customized software for managing web content. It shares aspects of a web application framework and a content management system (CMS).

22.	CMS	A content management system (CMS) is an interface that allows users to publish content directly to the Web. The process of adding content pages directly to the Web is one step ahead of creating and uploading pages from a local machine because it allows a large number of people to add and share the data remotely.
23.	COBIT	Control Objectives for Information and Related Technology is a framework created by ISACA for information technology management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
24.	Code	System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.
25.	Code Review	Code review is systematic examination of computer source code. It is intended to find and fix mistakes overlooked in the initial development phase, improving both the overall quality of software and the developers' skills.
26.	Common Control	A security control that is inherited by one or more organizational information systems.
27.	Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
28.	Configuration Control	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
29.	Criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.
30.	Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
31.	Cyber Incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.
32.	Cyber Infrastructure	Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services e.g., managed security services) are part of

		cyber infrastructure.
33.	Cyber Security	The ability to protect or defend the use of cyberspace from cyber-attacks.
34.	DAST	Dynamic application security testing (DAST) technologies are designed to detect conditions indicative of security vulnerability in an application in its running state.
35.	Data Security	Protection of data from unauthorized accidental or intentional modification, destruction, or disclosure.
36.	DB Security	Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability.
37.	Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
38.	Denial of service attacks/ distributed denial-of-service (DDoS)	A type of attack aimed at making the targeted system or network unusable, often by monopolizing system resources. A distributed denial of service (DDoS) involves many computer systems, possibly hundreds, all sending traffic to a few choice targets. The term "Denial of Service" is also used imprecisely to refer to any outwardly-induced condition that renders a computer unusable, thus "denying service" to its rightful user.
39.	DHCP	The Dynamic Host Configuration Protocol is a standardized network protocol that is used by network devices to configure the IP settings of another device, such as a computer, laptop or tablet.
40.	DLP	Data loss/leak prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
41.	DMZ	Demilitarized zone is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network.
42.	DR	Disaster recovery (DR) the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning in the midst of disruptive events.

43.	DRM	Digital rights management (DRM) is a systematic approach to copyright protection for digital media. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they've purchased.
44.	DSF	DSCI Security Framework is comprised of 16 disciplines that are organized in four layers. DSF brings a fresh outlook to the security initiatives of an organization by focusing on each individual discipline of security.
45.	Encryption	Conversion of plaintext to cipher text through the use of a cryptographic algorithm.
46.	End-to-End Security	Safeguarding information in an information system from point of origin to point of destination.
47.	External network	Any network that can connect to yours, with which you have neither a trusted or semi-trusted relationship. For example, a company's employees would typically be trusted on your network, a primary vendor's network might be semi-trusted, but the public Internet would be untrusted — hence, External.
48.	Firewall	A gateway that limits access between networks in accordance with local security policy.
49.	Hashing	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.
50.	HTTP	Hyper Text Transfer Protocol is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
51.	IAM	An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.
52.	ICT Personnel	An information and communication technology personnel is responsible for the development, management and support of the infrastructure at an organization.
53.	Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
54.	IDS	Intrusion Detection systems - A class of networking products devoted to detecting attacks from hackers. Network-based intrusion detection systems examine the traffic on a network for signs of unauthorized access or attacks in progress, while host-based systems look at processes running on a local machine for activity an administrator has defined as "bad."

55.	IEEE	The Institute of Electrical and Electronics Engineers is dedicated to advancing technological innovation and excellence
56.	Information Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and 3) availability, which means ensuring timely and reliable access to and use of information.
57.	Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
58.	Information Security Life Cycle	The phases through which an information system passes, typically characterized as initiation, development, operation, and termination i.e., sanitization, disposal and/or destruction).
59.	Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
60.	Information Security Risk	The risk to organizational operations including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
61.	Information Type	A specific category of information e.g., secret, confidential, proprietary, investigative, public, contractor sensitive, security management) etc. defined by an organization.
62.	Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
63.	Intrusion	Unauthorized act of bypassing the security mechanisms of a system.
64.	IP	Internet Protocol is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.
65.	IPS	Intrusion prevention systems IPS), also known as intrusion detection and prevention systems IDPS) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

66.	IPsec	IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks.
67.	ISO 27001	It is an information security management system (ISMS) standard published by the International Organization for Standardization (ISO). ISO/IEC 27001:2005 formally specifies a management system that is intended to bring information security under explicit management control.
68.	ISO 27005	The purpose of ISO 27005 is to provide guidelines for information security risk management. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
69.	MAC	Media Access Control address is a hardware address that uniquely identifies each node of a network.
70.	Malicious agents	A person of malicious intent who researches, develops, and uses techniques to defeat security measures and invade computer networks.
71.	Management Security Controls	The security controls i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security.
72.	NAC	Network Access Control is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement
73.	Need-to-Know	A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.
74.	Network Hardening	Hardening is usually the process of securing a system by reducing its surface of vulnerability. A system has a larger vulnerability surface, the more that it does; in principle a single-function system is more secure than a multipurpose one. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.
75.	NIST 800	The NIST 800 Series is a set of documents that describe United States federal government computer security policies, procedures and guidelines.
76.	NIST 800-53	NIST 800-53 is a publication that recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security.
77.	OCATVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation are a suite of tools, techniques, and methods for risk-based information security strategic assessment and

		planning.
78.	OSSTMM	The Open Source Security Testing Methodology Manual (OSSTMM) was released by Pete Herzog and is distributed by the Institute for Security and Open Methodologies (ISECOM). This document is concentrated on improving the quality of enterprise security as well as the methodology and strategy of testers.
79.	OTP	One-time password is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords.
80.	OWASP	The Open Web Application Security Project is an open-source web application security project. The OWASP community includes corporations, educational organizations, and individuals from around the world.
81.	Password	A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.
82.	Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
83.	PCI-DSS	The Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure.
84.	Penetration Testing	Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.
85.	Privilege Management	The definition and management of policies and processes that define the ways in which the user is provided access rights to enterprise systems. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information in directories.
86.	Protocol	Set of rules and formats, semantic and syntactic, permitting information systems to exchange information
87.	Remote Access	The ability for an organization's users to access its nonpublic computing resources from external locations other than the organization's facilities.

88.	Role-Based Access Control – (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.
89.	Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
90.	SAST	Static application security testing (SAST) is a set of technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyze an application from the “inside out” in a nonrunning state.
91.	SDLC	The software development life cycle is a framework defining tasks performed at each step in the software development process. It consists of a detailed plan describing how to develop, maintain and replace specific software.
92.	Secure Socket Layer (SSL)	A protocol used for protecting private information during transmission via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:”
93.	Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
94.	Security Incident Breach	A security incident breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of sensitive information maintained or processed by the organization
95.	Sensitivity	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
96.	Session hijacking	An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker's goal is to gain access to a server while bypassing normal authentication measures.
97.	SHA 2	Secure hash algorithm SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS).
98.	SIEM	Security Information and Event Management (SIEM) provides real-time analysis of security alerts generated by network hardware and applications. SIEM is sold as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.

99.	SNMP	Simple Network Management Protocol is an "Internet-standard protocol for managing devices on IP networks". It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention
100.	Social Engineering	A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.
101.	Spoofing	Altering data packets to falsely identify the originating computer. Spoofing is generally used when a hacker wants to make it difficult to trace where the attacks are coming from.
102.	SSH	Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.
103.	SSID	Service set identifier is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network that acts as a password when a device tries to connect to the basic service set a component of the IEEE 802.11 WLAN architecture.
104.	Standard	A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.
105.	Threat	Any circumstance or event with the potential to adversely impact organizational operations including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
106.	Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
107.	Threat Modeling	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
108.	TLS	Transport Layer Security, a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.
109.	Traffic flood attacks	Traffic flooding attacks such as DoS/DDoS and Internet Worm.
110.	UTM	UTM combines multiple security features into a single platform to protect against attacks, viruses, Trojans, spyware and other malicious threats. Complexity is reduced and management is simplified because multiple layers of protection are delivered under this single management

		console.
111.	VPN	Virtual private network is a network that is constructed by using public wires — usually the Internet — to connect to a private network, such as a company's internal network. There are a number of systems that enable to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
112.	Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
113.	Vulnerability assessments	Vulnerability Assessment is the process of identifying network and device vulnerabilities before hackers can exploit the security holes. It helps detect network and system vulnerabilities.
114.	WAF	A web application firewall is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall.
115.	WLAN	A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
116.	WLAN IPS	The primary purpose of a Wireless Intrusion Prevention system is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure.
117.	WPA	WPA is a security technology for Wi-Fi wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy).
118.	WPA-2	Wi-Fi Protected Access 2, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.

Annexure 15 – Additional references

1. Glossary of Key Information Security Terms, NIST: http://infohost.nmt.edu/~sfs/Regs/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
2. Harvard: http://www.security.harvard.edu/glossary-terms
3. SANS: http://www.sans.org/security-resources/glossary-of-terms/
4. Cybersecurity Framework: http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
5. NIST Special Publications in the 800 series: http://csrc.nist.gov/publications/PubsSPs.html
6. DSCI Security Framework: http://www.dsci.in/taxonomypage/63
7. Federal Information Security Management Act FISMA): www.csrc.nist.gov/drivers/documents/FISMA-final.pdf
8. Risk Assessment Methodologies: OCTAVE - http://www.cert.org/octave/
9. COSO - http://www.coso.org/
10. PCI standards documentation: https://www.pcisecuritystandards.org/security_standards/
11. COBIT : http://www.isaca.org/COBIT/Pages/default.aspx
12. Open source architecture frameworks www.opensecurityarchitecture.org