सत्यमेव जयते

Version 2.0 16 January 2015

Guidelines for Protection of Critical Information Infrastructure

National Critical Information Infrastructure Protection Centre
Goverment of India

Guidelines for the Protection of National Critical Information Infrastructure

Version 2.0

National Critical Information Infrastructure
Protection Centre
New Delhi

Version 2.0 released on 16 January 2015

Designed, Published and Printed by NCIIPC, New Delhi.

Contents

List of Figures

Glossary

ACL	Access Control List
AMC	Annual Maintenance Contract
APT	Advanced Persistent Threats
CC	Common Criteria
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
COTS	Commercial-Of-The-Shelf
DDOS	Distributed Denial Of Service
DNS	Domain Name Server
DMZ	De Militarized Zone
DOS	Denial Of Service
DR/BCP	Disaster Recovery/ Business Continuity Planning
EAL	Evaluation and Assurance Level
HaaS	Hardware As A Service
IaaS	Information As A Service
IC	Implementation Controls
IS	Information Security
ISD	Information Security Department
ISMS	Information Security Management System
LAN	Local Area Network
MITM	Man-In-The-Middle-Attacks

MZ	Militarized Domain
NDA	Non Disclosure Agreement
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
OC	Operational Controls
OEM	Original Equipment Manufacturer
PaaS	Platform As A Service
PC	Planning Controls
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PPP	Public Private Partnership
RAC	Role Based Access Controls
RBAC	Role Based Access Control
SaaS	Software As A Service
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SOC	Security Operation Centre
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterrupted Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTR	Vulnerability Threat Risk
WAN	Wide Area Network

Executive Summary

1. Protection of Critical Information Infrastructure (CII) is of paramount concern to governments worldwide. To address this threat, the Government of India has notified the 'National Critical Information Infrastructure Protection Centre' (NCIIPC) as the nodal agency vide Gazette of India notification on 16th January 2014.

2. NCIIPC is driven by its mission to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country. To achieve this, it is essential to ensure that relevant security mechanisms are built into Critical Information Infrastructure as key design features.

3. The National Security Advisor had in July 2013 released a document listing forty controls and corresponding guiding principles for the protection of CIIs. In view of the dynamic nature of cyberspace and to ensure the continued relevance of these controls, NCIIPC is continuously reassessing these based on ongoing experience as well as feedback from NCII constituents, these controls have been grouped into five sets (or families). While all Controls in a family may not be relevant to a particular organization / infrastructure, it is important that conscious sign off (on both, controls implemented, as well as dropped) is taken from senior management based on residual risk acceptable to the Organization.

4. The five families of controls are:

4.1 **Planning Controls** for ensuring that the security is taken as a key design parameter for all new CIIs at conceptualisation and design level itself.

4.2 **Implementation Controls** for translating the design/conceptualisation planning into mechanisms for protecting the CII. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

4.3 **Operational Controls** for ensuring that the desired security posture is maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected / poorly protected CII.

4.4 **Disaster Recovery/ Business Continuity Planning (BCP) Controls** for ensuring minimum downtime and the restoration process

4.5 **Reporting and Accountability Controls** for ensuring adequate accountability and oversight exercised by Senior management, as well as reporting to concerned Government agencies where required enforced through compliance controls.

5. In circumstances where a particular control may not provide the best fit, the concerned organization needs to consider compensatory controls which could also be procedural, so as to ensure that the attack surface presented by the organization's Information Infrastructure is minimized.

6. This document has been made after extensive consultation of available literature, strongly modulated by the experience of the NCIIPC team in handling and consulting various CII across various segments across industry in the country. Feedback and constructive criticism / advice is solicited with the aim of developing a collective national enterprise towards securing our critical national assets.

1. Introduction

1.1. Information Infrastructure is the term usually used to describe the totality of inter-connected computers and networks, and information flowing through them. Certain parts of this Information Infrastructure, could be dedicated for management / control etc of infrastructure providers' e.g. Power generation, Gas/oil pipelines, or support our economy or national fabric e.g. Banking / Telecom etc. The contribution of the services supported by these infrastructures, and more importantly, the impact of any sudden failure or outage on our National well being or National Security marks them as being Critical.

1.2. By extension, information infrastructure supporting the operations of Critical Infrastructure (CI) marks this as Critical Information infrastructure (CII). These Networks operate/monitor and control important Governmental and Societal functions and services including, but not limited to, Power (Generation/transmission/ distribution etc), Telecommunication (mobile/landline/internet etc), Transportation (Air/land/rail/sea etc), Defence etc. These CII are becoming increasingly dependent on their information infrastructure for information management, communication and control functions.

1.3. In the Information Technology Act 2000, Critical Information Infrastructure has been defined as:

"Critical Information Infrastructure means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".

1.4. A significant characteristic of this CII is the increasingly intricate interdependence between various CII. Any delay, distortion or disruption in the functioning of these CIIs has the potential to quickly cascade across other CII with the potential to cause political, economic, social or national instability.

1.5. In the dynamic arena of cyber space, the challenge inherent in securing our National CIIs is exponentially increasing, perhaps as a factor of the ubiquitous presence of services etc relying on this CII. These CII are vulnerable to cyber attacks for various reasons using multiple attack methodologies. This document discusses some vulnerabilities alongwith suggested counter-measures for critical information infrastructure of the country.

2. Identification of CIIs

2.1 A fundamental question concerns the identification of CII. In this, the most logical approach dictates that this identification be undertaken on the basis of identification of critical business processes as determined by the business owner / owning entity. The information infrastructure supporting these critical business processes, therefore, logically gets identified as CII. Similarly, we could have CII supporting critical data flows between entities, the disruption or manipulation of which could impact process flows.

2.2 Further, networks are characterized by a system of interconnected nodes and links. We can identify and classify a node as critical if either:

2.2.1 It alone can exert such influence on other nodes that a serious disruption of governmental or societal infrastructure can occur.

2.2.2 It forms an integral part of an ensemble of nodes, which can be attacked or otherwise influence in a similar manner, such that aggregate malfunction can lead to serious disruption.

2.3 An evaluation of all likely nodes in order to estimate criticality would, apart from being time consuming, become quickly outdated due to the dynamic nature of these systems. Many similar nodes can be critical at the same time. NCIIPC, has therefore made a beginning by suggesting indicative parameters for identification of CIIs as:

2.3.1 Functionality of the System/Information Infrastructure being supported.

2.3.2 Degree of Complementarities with other information infrastructure in country.

2.3.3 Associated Social, Political or Strategic values.

3. Protection of CIIs

3.1 As the emerging societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies, it would therefore be natural to follow an analytical chain beginning with technical specifications and causally running through systems, actors, threats, vulnerabilities, consequences and finally countermeasures / mitigation / remediation.

3.2 Vulnerabilities are the flaws, loophole or backdoors used by attackers to manipulate or take control of the system, to access and steal the information or to degrade / deny the functioning of the system. Numerous vulnerabilities exists at different sectors/levels viz. Web Applications, Servers, SCADA Systems etc. Figure 1 shows the different branches of cyber infrastructure along with commonly used attack vectors.

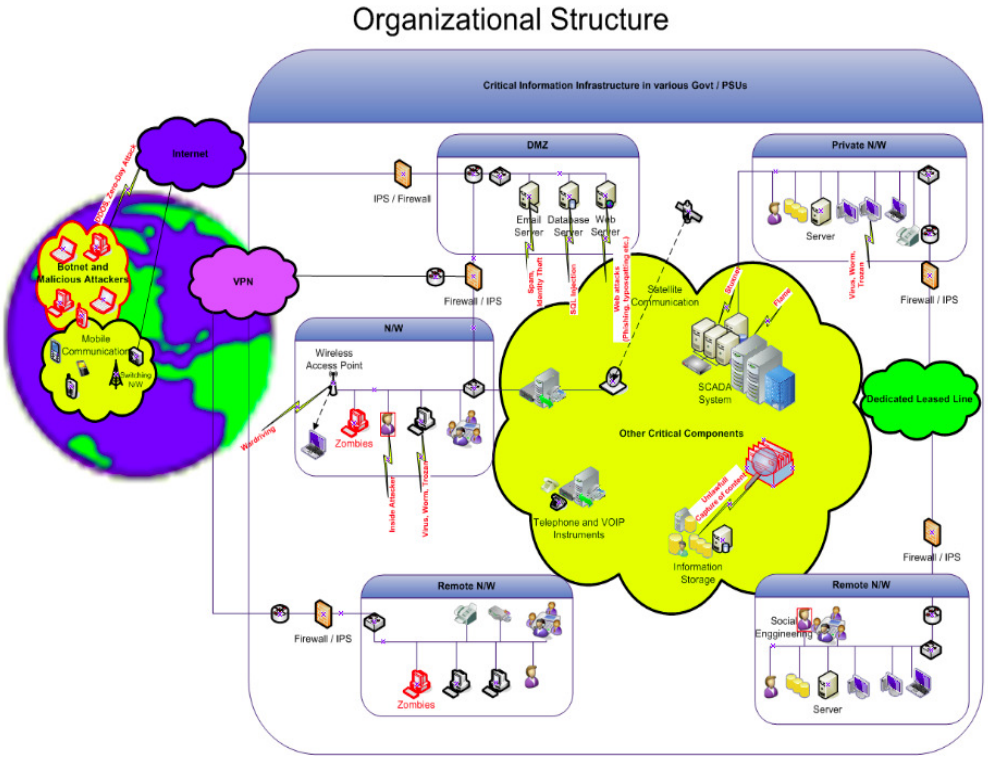

Figure 1: Common Attack Vectors on CII

3.3 There are multiple segments/services inherent in the architecture of any Critical Information Infrastructure like SCADA, VPN services, e-mail, web services, network services etc. These are under continuous threat from variously motivated malicious hackers/attackers. In the case of CII, the attackers are more than likely to have strong state support from any

number of adversaries. Common attack vectors used include - web application attacks, client side attacks, network attacks, attacks using malware and APTs (Advanced Persistent Threats), DOS/DDOS attacks, social engineering/spear phishing attacks, brute force attacks, MITM (Man-in-the-Middle) and interception attacks, routing attacks, supply chain contamination attacks, DNS attacks, targeted attacks by evading/bypassing perimeter protection devices etc.

3.4 Recent attacks on cyber infrastructure indicate that attackers are increasingly targeting SCADA Systems and supporting infrastructure widely used in almost all critical industrial set-ups such as oil, gas, nuclear, aviation etc.

4. NCIIPC: Policy and Strategy

4.1 With the increasing convergence of communication technologies and shared Information systems in India, Critical Sectors are becoming increasingly dependent on their CII. These CIIs are interconnected, interdependent, complex and distributed across various geographical locations. Threats to CII, ranging from terrorist attacks, through organized crimes, to espionage, malicious cyber activities etc, are following a far more aggressive growth trajectory. Protection of CII and, hence, CI of the Nation is the one of the paramount concerns of the Government. To this end, Government of India, has designated 'National Critical Information Infrastructure Protection Centre' (NCIIPC) as the national nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 for taking all measures including associated Research and Development for the protection of CIIs in India.

4.2 NCIIPC is driven by its mission "To take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information security awareness among all stakeholders" and with a vision "to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the nation".

4.3 Guiding principles for NCIIPC include:

4.3.1. Development of mechanisms to facilitate Identification of CII in conjunction with CI organisations

4.3.2. Protection of CII through a risk management approach

4.3.3. Ensuring compliance of NCIIPC policies, guidelines, advisories/ alerts etc. by CIIs.

4.3.4. Develop capabilities for real time warning system and facilitate sharing of information on emerging threats, cyber attacks, vulnerabilities etc with CIIs.

4.3.5 Lead and coordinate national programs and policies on Critical Information Infrastructure.

4.3.6 Establish national and international linkages / initiatives including R&D for the protection of CII

4.3.7 Promote Indigenous Research and Development (R&D) relating to protection of Critical Information Infrastructure including Modelling and Simulation of Complex CII, development of CIIP tools and Threat Scenarios.

4.3.8 Develop mechanisms to facilitate sharing of information on Information Security breaches, incidents, cyber attacks, espionage etc among CII stake holders as well as with NCIIPC.

4.3.9 Facilitate thematic workshops and Information Security Awareness and Training Programme through PPP.

4.3.10 Facilitate capacity building towards creation of highly skilled manpower through engaging Premier Institutes like IISc, NITs etc as well as private/non government partners working on CIIP.

4.3.11 Establish Sectoral CERTs to deal with critical sector specific issues.

5. Best Practices, Controls and Guidelines

5.1 NCIIPC follows the best global practices, approaches, controls and guidelines for accomplishing its mandated mission of protecting CIIs, with the aim of providing safe, secure and resilient operational environments. While Version 1 of the guidelines enumerated forty controls, the present version has re categorised these into thirty five controls based on their functional impact in the development/ deployment/operationalisation cycle. While each control may not be required per se, it is expected that all CII would take a conscious decision regarding the applicability or otherwise of every control as a conscious process of minimising risk. In this contest, it is imperative that CII security move out of the realm of "IT" or "Cyber Security", and into a threat meriting Board level attention at par with Financial or Operational Risk Management.

5.2 The five families of controls into which the Guidelines for the protection of CII have been divided are:

5.2.1 **Planning Controls**: These set of controls are required to be assessed at the conceptualisation and design stage to ensure that security is taken as a key design parameter for all new CII.

5.2.2 **Implementation Controls**: These controls are required for translating the design/conceptualisation planning so as to ensure adequate and accurate translation of the security designs into actual system security configurations. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

5.2.3 **Operational Controls**: To ensure that security postures are maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

5.2.4 **Disaster Recovery/Business Continuity Planning (BCP) Controls**: These controls are essential to ensure minimum downtime, as well as to ensure that the restoration process factors in, and overcomes the initial vulnerabilities, or alternatively isolates infrastructure compromised by attackers, to ensure graceful degradation / minimum maintenance of Service provided by the CII.

5.2.5 **Reporting and Accountability Controls**: These controls ensure that adequate accountability and oversight is exercised by Senior management, as well as reposting to concerned Government agencies where required. This family of Controls also includes compliance controls.

5.3 Each of these controls is vital for the creation of safe, secure and resilient platforms. It is recommended that each organisation examine these

controls and evolve customised guidelines for the protection of its CIIs as per their critical Business/Operational process requirements. For this, sign off from senior management for controls not considered necessary to implement, or for which compensatory controls are established is highly recommended. In essence, it is essential for a holistic approach, examining all aspects of CII security to be adopted, with explicit acceptance of residual risk.

5.4 This document is intended to assist and advice the management and CISO (Chief Information Security Officer) of the Critical Sectors regarding the infrastructure, manpower, skill and guidelines required in meeting the ever growing and challenging task of the protection of their respective CIIs in consultation and coordination with NCIIPC.

5.5 Critical Controls mentioned in the subsequent sections are the minimum recommended by NCIIPC to be examined for implementation by each CII. Each control is explained with detailed illustrations. These Controls are updated periodically by NCIIPC to stay in tune with the requirements of constituent CII as well as to keep pace with emerging protocols and technologies. These thirty five Critical Controls can be sub-divided under five major sub-heads of Critical Controls as mentioned and highlighted in Figure 2.

Planning Controls

PC1: Identification of CII
PC2: Vertical and Horizontal Interdependencies
PC3: Information Security Department
PC4: Information Security Policy
PC5: Integration Control
PC6: VTR Assessment and Mitigation Controls
PC7: Security Architecture Controls including configuration Management and Mitigation Controls
PC8: Redundancy Controls
PC9: Legacy System Integration
PC10: Supply Chain Management – NDA's, Extensions and Applicability
PC11: Security Certifications
PC12: Physical Security Controls

Implementation Controls

IC1: Asset and Inventory Control
IC2: Access Control Policies
IC3: Identification and Authentication Control
IC4: Perimeter Protection

IC5: Physical and Environmental Security
IC6: Testing and Evaluation of Hardware and Softwares

Figure 2: NCIIPC: Best Practices Security Framework

Operational Controls

OC1: Data storage: Hashing and Encryption
OC2: Incident Management - Response
OC3: Training, Awareness and Skill up-gradation
OC4: Data Loss Prevention
OC5: Penetration Testing
OC6: Asset and Inventory Management
OC7: Network Device Protection
OC8: Cloud Protection
OC9: Critical Information Disposal and Transfer
OC10: Intranet Security
OC11: APT protection

Disaster Recovery/ Business Continuity Planning (BCP) Controls

DR1: Contingency Planning – Ggraceful degradation
DR2: Data Back-up and Recovery Plan, Disaster Recovery Site
DR3: Secure and Resilient Architecture Deployment

Reporting and Accountability Controls

RA1: Mechanism for threat reporting to Govt. Agencies
RA2: Periodic Audit and Vulnerability assessment
RA3: Compliance of Security Recommendation

6. Planning Controls (PC)

6.1 PC 1: Identification of Critical Information Infrastructure (CII)

6.1.1 **CII Identification**: Each critical sector is responsible to identify and categorize CIIs within their infrastructures on the basis of Functionality, Criticality Scale, Degree of Complementarities Political, Economic, Social and Strategic Values, degree of dependence, sensitivity etc. The identification of critical infrastructure is a dynamic process and must be reviewed periodically by all stakeholders to address changes in functional dependencies, technologies and protocols. CII identification is a part of national risk assessment which constitutes a holistic view of all risks to national security.

6.1.2 **Functionality** is a dynamic concept which includes the set of functions, procedures and or capabilities associated with a system or with its constituent parts. It may be viewed at two levels- Functional Uniqueness and Functional Dependency.

6.1.3 **Criticality Scale** is a heuristic rule for impact assessment based on multidimensional approach that includes availably, access, delivery and consummation of essential services.

6.1.4 **Degree of Complementarities** is a distinguishing characteristic of the Information Infrastructure is that it links other Information Infrastructure Systems together. Failure of one system has potential to shut down other Critical Information Infrastructure relatively quickly in a cascading manner.

6.1.5 **Political, Economic, Social and Strategic Values** includes what is held important for political stability, economic prosperity, fraternity, unity and integrity of Nation.

6.1.6 **Time Duration** has an important significance in the identification and categorization of CII. The same system may or may not be critical at different times / under different circumstances.

6.2 PC 2: Vertical and Horizontal Interdependencies

6.2.1 This section deals with the intricate relations between components that have been identified as critical between, as well as and within organizations – essentially, inter as well as intra organisation. CII cannot be viewed in isolation and all vertical and horizontal interdependencies with other CIIs or resources must be taken into consideration.

6.2.2 Vertical interdependency as shown in Figure 3 refers to the symbiotic relation between organisational layers (i.e. interdependencies of divisions and departments) within an organisation and that between organizations and subsidiaries, if any.

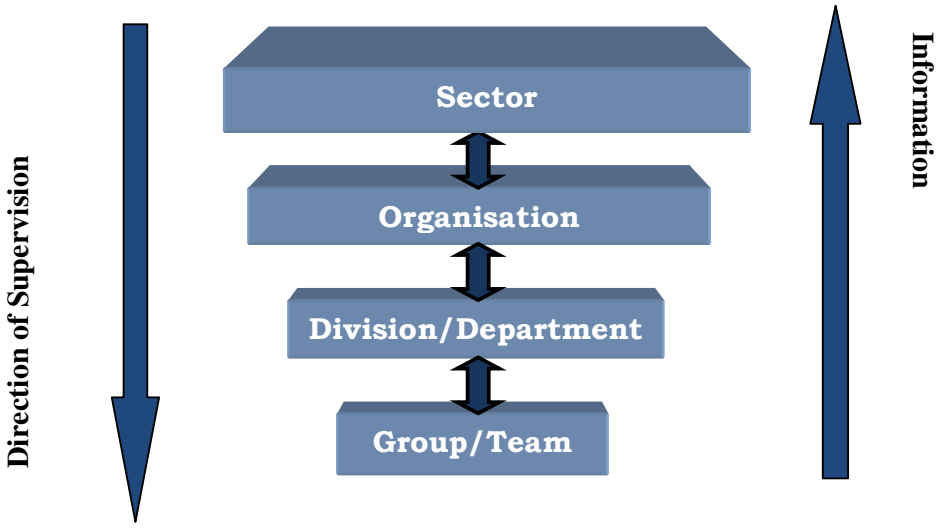

Figure 3: Vertical Interdependency

6.2.3 In the figure above, direction and supervision flows from top to bottom and information flows from bottom to top. Identification and understanding of linkages is an absolute necessity to establish a secure environment for CIIs.

6.2.4 Horizontal interdependency as shown, is based on the in-bound and out-bound interdependencies. In-bound interdependency includes role and services expected from an organisation by other organisations.

	Org.1	Org.2	Org.3	Org.4	Org.5
Org.1					
Org.2					
Org.3					
Org.4					
Org.5					

Out-bound Dependency

In-bound Dependency

Figure 4: Horizontal Interdependency

6.2.5 Out-bound dependency includes the service expectation by one particular organisation from others. On the basis of in-bound and out-bound dependencies the CII as a whole is to be established and a holistic approach is to be adopted for security.

6.3 **PC 3 Information Security Department (ISD)**

6.3.1 Every organization must plan for and have a strong and independent Information Security Department. This department must be responsible for ensuring the safety and security of IT assets of the organisation, alongwith ensuring the Safety and Security of data, controls, etc flowing over the CII. This includes preventing classified or critical information from being compromised and timely dissemination of relevant and valid information to the authorised elements in each identified CII. This Department would also study threats, risks, vulnerabilities and their solutions, providing security briefings, securing classified information, and teaching and enforcement activities related to information security.

6.3.2 It is recognised that CII would have its own control systems, SCADA devices etc, for which separate dedicated specialists may be deployed. It is the responsibility of Senior Management to ensure that these departments provide the necessary inputs to the ISD at every stage to ensure continuous, comprehensive protection of the enterprise network.

6.3.3 Security incidents, breaches etc must also be reported to ISD as per the Information Security policy of the organisation.

6.3.4 In order to manage the diverse domains of CIIs, it is proposed that every organisation within a critical sector must appoint a Chief Information Security Officer (CISO), who will head ISD for interfacing with NCIIPC.

6.3.5 Suggested roles and responsibilities of ISD:

(a) Planning

(b) Development

(c) Management

(d) Oversight.

6.3.6 Best Practices:

(a) **Planning**

i. Identify an annual work plan to achieve security goals and objectives consistent with the agency's strategic plan.

ii. Define the scope and boundaries of information security program and its implementation strategy. Where relevant, revise existing plans to ensure changes, new technologies etc continue to remain adequately secured.

iii. Understand legal and regulatory requirements.

iv. Estimation of budgetary and logistic requirements. There should be adequate annual financial arrangement for planning, maintenance and management of Information Security.
v. Define risk management framework after planning organisation-wide Information Security Management System (ISMS) in accordance with ISO/IEC 27001 Standard and other relevant security standards in consultation with NCIIPC.

(b) **Development**

i. Lead in the development of information security policies, standards, guidelines, processes, and procedures.
ii. Define formal processes for creating, documenting, reviewing, updating and implementing security policies.
iii. Design and development of Information and asset classification policy.
iv. Lead and coordinate development of organisation specific information security policies, procedures, guidelines and processes in consultation with various stake holders including NCIIPC.

(c) **Management**

i. Dissemination of information security policies, procedures and guidelines to all concerned.
ii. Conduct risk assessments, manage incidents, and provide internal and external reporting, involvement in security awareness education and training.
iii. Integration of information security processes with organisation's business processes.
iv. Periodic evaluation and review effectiveness of information security policies, procedures, standards, guidelines and processes etc.
v. Maintain a record of information security incidents and breaches.
vi. Coordinate and lead in implementation of 'Business Continuity Plan' and conduct mock drills to evaluate effective implementation of the same.
vii. Ensure HR management policies adequately incorporate Information Security Guidelines, including entry and exit checks such as Character and Antecedents check and exit management strategies.
viii. Secure disposal of E - Waste
ix. Ensure that all information systems within the organisation are adequately patched and updated.
x. Interface regularly with the core organisational Perspective planning Team to remain abreast of new technologies / equipment being

considered for deployment within the organisation, and evaluate their possible implications on existing systems.

(d) **Oversight**

i. Evaluate the effectiveness of ongoing security operational processes, monitor compliance for internal and external requirements.

ii. Evaluate compliance with respect to legal and regulatory requirements for information security.

iii. Perform information security audit at least annually or whenever significant changes have been made in IT Systems/Infrastructure. ISD must function **on 24x7x365 basis.**

6.3.7 Structure of ISD - The structure of ISD should be hierarchical with the CISO reporting directly to the head of the CII/organisation to ensure the understanding and involvement of Senior Management.

6.3.8 CISO may be assisted by different departments, divisions or groups in devising 'Information Security Policy' and ensuring its efficient and effective implementation. As shown in Figure 5 below, CISO is the nodal officer to interact with NCIIPC for feedback, trainings, advisories, breach reporting etc. CISO could be assisted by two departments:

6.3.9 HR/Training and Policy- being responsible for manpower and their trainings etc. This group will also help in devising the IS policy specific to CII/organisation in coordination with the other groups.

(a) Security Operation Centre (SOC) responsible for security event management and feedback.

(b) Apart from the above, an Audit/Pentest team for conducting periodic audits as per the IS policy is essential. In order to avoid potential conflict of Interest between the security enforcement and management role of the CISO and the essentially audit and reporting role of this group, it will be outside the direct control of the CISO and shall report directly to senior most management of the organisation.

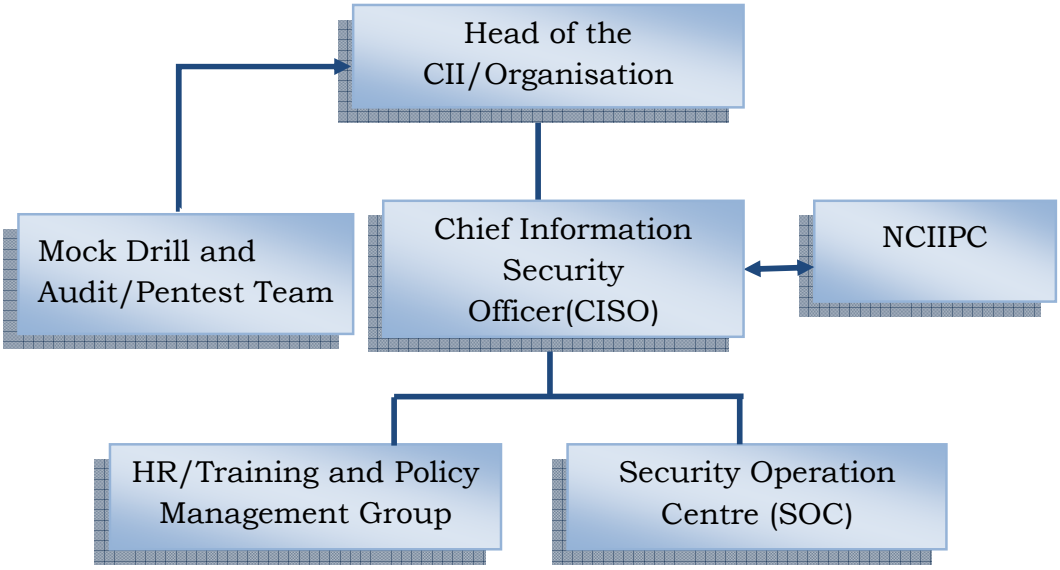

Figure 5: Structure of Information Security Department

6.4 **PC 4: Information Security Policy**

6.4.1 Each organisation needs an Information Security policy for Information security to protect from unauthorized access, use, disclosure, disruption, modification, recording or destruction, including incident management. The policy must rest on the bedrock of confidentiality, integrity and availability.

6.4.2 Information Security Policies are by design, statements of intent of the Senior Management, as to how the Information Security of their Organisation is to be managed. The Information Security policy must therefore reflect the intent and will of the management.

6.4.3 The policy must be a working document that outlines specific requirements, rules and norms that must be met. The Information Security policy should be a visionary document with legislative compliance which has the potential to act as a catalyst for Security and Safeguarding of CII.

6.4.4 There would be different perspectives, and requirements of the Information Security Policy for different group of employees in the Organisation. To accommodate all the perspectives and requirements, the employees can be categorised into various audience groups and their roles and responsibility may be defined accordingly in the Information Security Policy.

6.4.5 A Policy document may have an introduction, purpose, scope, roles and responsibilities, sanctions and violation etc. It must be understandable,

realistic, consistent and enforceable. There must be a periodic review of the policy so that it does not become obsolete. The policy must be known to all the stake holders such as employees, contractors, contractual workers, business associates etc.

6.4.6 Where required, relevant extracts may also be applied to sub contractors / vendors etc.

6.5 **PC 5: Integration Control**

This control deals with SCADA/Industrial Control Systems Interfacing with Cyber Security Systems

6.5.1 The significance of Cyber Security controls has only recently been recognised. It is therefore critical for any cyber security protection strategy for the CII sector to factor in existing systems / processes already deployed by industry.

6.5.2 This control aims to ensure that all systems deployed in the CII enterprise are adequately secured, and suitably incorporate the principle of defence in depth.

6.5.3 The CII must ensure that all interconnecting networks are suitably protected, with either adequate protections built in on both side (for enterprise owned networks), or, with adequate protection built in to withstand denial / disruption / damage from the interfacing network.

6.5.4 Impact analysis of failures / disruptions, either due to system outages, or, due to configuration changes or commissioning / decommissioning of new or updated equipment / systems must be considered at the planning stage itself.

6.6 **PC 6: Vulnerability/Threat/Risk (VTR) Assessment including Residual Risk Management (critical control/data plane identification) and Mitigation Controls**

6.6.1 Vulnerability/Threat/Risk assessment of enterprise wide cyber architecture must be part of the corporate planning/strategy. The resulting residual risk must have clear and unambiguous sign off from senior management.

6.6.2 Simply put, their inter relationship can be visualised as:

(a) Vulnerabilities are gaps/weaknesses in systems that allow an attacker to reduce the systems information assurance. Threats are actors / actions targeting the vulnerabilities in a system. Risks are the possibilities that a particular threat will successfully exploit vulnerability and the resultant impact of that exploitation on the information assurance of the system.

(b) This must include formalised VTR exercises supported by Senior most management in consultation with the CISO.

6.6.3 VTR assessment and management is an ongoing process and must be reviewed regularly. Additional triggers for VTR analysis could be:

(a) Upgrades/Induction/De-induction of systems / SCADA controls etc

(b) Configuration changes

(c) Security Alerts

6.6.4 This control provides an insight into the probabilistic implications or disruptions originated from the exploitation of the vulnerabilities by any threat. Risk analysis is a process used to evaluate the interlinking possibility of given threat source highlighting a particular potential vulnerability and its adverse impact. Risk assessment, analysis and management provide a decision making help to the management of any CII for preparing policies and plans for risk identification, categorisation, evaluation and its pro-active prevention. The entire process under this control can be divided into following categories:

(a) **CII categorization**: The inter se categorisation is based on business criticality as determined by the entity owner. The underlying criticality of the CII is thereby determined based ont the criticality of the supported business functions. This categorization is required as per IT Act 70 A and includes identification of all resources, assets (hardware and software) etc.

(b) **Threat Identification**: Threat categorisation can be broadly divided under three categories viz. Natural, Physical and environmental and Human threats. Natural threats covers floods, earthquake while physical and environmental threats covers power failure, physical intrusion and destruction. Human threats include all the attempts made by the malicious hackers to gain unauthorized access online or offline.

(c) **Vulnerability Identification**: Vulnerabilities of all aspects of the CII need to be examined in order to arrive at a considered view of the possibility of threat execution. Without the existence of vulnerability, threat can't be executed. Therefore the vulnerability should be properly identified under particular threat for the defined CII.

(d) **Risk evaluation**: Risk analysis involves the analysis of the controls for prevention of the hazards. It also includes the implication of the threats which arises out of the successful exploitation of the vulnerabilities. Risk evaluation provides the insight for the pro-active protection policy formation.

(e) **Quantitative and Qualitative analysis**: This analysis is must to assess the level of impact and damage that will be caused on successful exploitation of the vulnerabilities by the particular threat thereby increasing the risk level. Risk level qualitatively therefore can be categorized as high, Medium and Low whereas quantitatively the risk can be defined as the amount of damage that can occur.

(f) **Analysis of Implications**: This parameter analyse the implication which arise due to the successful exploitation attempt. Such impacts represent damaging challenges of different types, duration and levels. These impacts can be measured with the factors like asset impacted, severity and time duration. This parameter also has significance for the social, political, economical, national impacts after the exploitation.

(g) **Risk Prevention and Recovery**: This parameter deals with strategising the proper risk prevention policy and recovery process on successful threat exploitation. Risk prevention strategy is all about devising the plan which indicate, prioritize, evaluate and implement the low cost risk reducing controls suggested by the risk assessment process.

(h) **Compliance**: Compliance parameter deals with the proper checks and balances for properly and effectively implementing the risk assessment and management model. This parameter also deals with the checks and balances for preventing any violation in implementing the model because the purpose for risk assessment and management will be defeated without proper compliance.

(i) **Review and Feedback**: The fast pace of change of technologies is matched by a rapid change in the risk assessment and management model. It is therefore essential to regularly review the model and incorporate necessary amendments in policies periodically.

6.6.5 Residual risk is the component of risk which the Management is willing to accept either because the threat perception is extremely low, or because the mitigation cost is extremely high, or, as a combination of both these factors – i.e. Residual risk is the remaining risk that has been accepted by the CII owner after having addressed all vulnerabilities/ threats possible.

6.6.6 Residual risk must be the end product of a planned and systematic strategy to indentify and manage threats faced by the organisation, as part of a considered management decision.

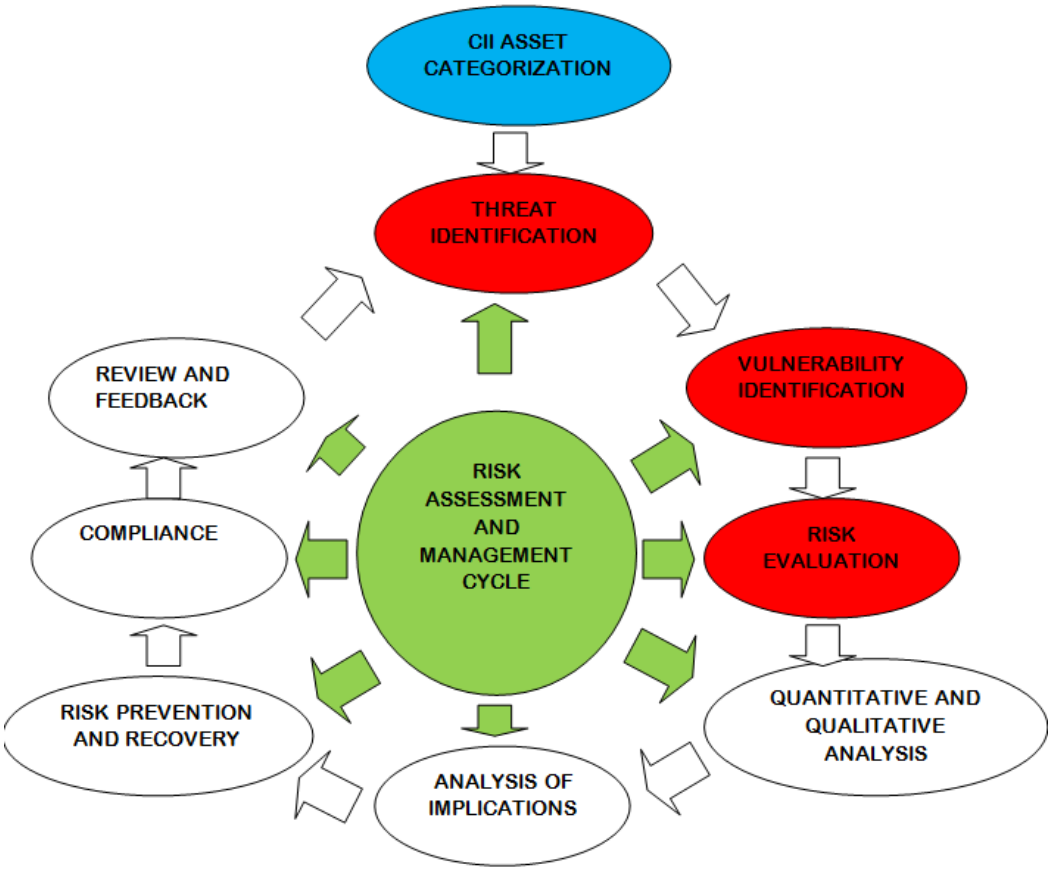

Figure 6: Risk Assessment

6.7 **PC 7**: **Security Architecture Control including configuration Management and mitigation control**

6.7.1 A significant aspect of the CII security mechanism is understanding and implementing a secure architecture as an organisational framework. This control works on the premise that the security infrastructure is meant to be an enabler and not a hindrance. This premise is achievable only when the security architecture, by means of imposing reasonable and cost effective controls, permits the transaction of organisational processes despite, attacks, attempted disruptions etc.

6.7.2 The security architecture control includes:

(a) Identification of services/controls/ interfaces and their exposure to threats

(b) System/ network components and their implementation

(c) Mitigation strategies as a result of V/T/R analysis including failover and graceful degradation

(d) Allocation of responsibilities, including at Senior management levels

(e) Identification/authorisation controls (Role Based Access Control)
(f) Limiting Administrative privileges

6.8 **PC 8 Redundancy Controls:**

6.8.1 Based on their own industrial / technical requirements, CII components, would, by design be fault tolerant and incorporate adequate redundancy to cater for system malfunctions / failover etc. It is the responsibility of the CISO to ensure that the CII security mechanisms understand and cater for these redundancies in their design and implementation.

6.8.2 A similar level of redundancy has to be catered for in the design and implementation of security controls as well.

6.8.3 Redundancy controls must ensure that failures do not lead to either choking / clogging of communication interfaces, or to cascading failures of other systems.

6.9 **PC 9: Legacy System integration**

6.9.1 Systems operating in NCII e.g. SCADA systems, typically will require specific skill sets very different from typical IT skill sets. In addition, these systems incorporate OEM specific Operating systems, protocols etc. Legacy systems may not have password protection/ encryption features. Also, these systems would typically be run by the relevant control systems specialists rather than IT specialists.

6.9.2 Organisations would also have to factor in warranty/AMC impacts, in consultation with the OEM system providers.

6.9.3 In such an environment, integration of legacy systems has to be a well thought out process taking into consideration disruptions/ downtime etc. Performance/impact analysis studies are essential to understand the implications/ effects of placing IT security controls as an overlay onto legacy Control Systems.

6.10 **PC 10: Supply Chain Management – NDA's, extensions and applicability**

6.10.1 Depending on the criticality of the control system / CII, sourcing of equipment and secure supply chain management gains importance.

6.10.2 For highly critical and sensitive deployments, it is advisable to obtain details of the supply chain and institute measures to ensure compliance to desired security standards / norms where possible.

6.10.3 Security precautions including Non Disclosure agreements, confidentiality clauses etc must be applicable to the supply chain where required.

6.11 **PC 11: Security Certifications**

6.11.1 Security certifications deals with the validation of the security measures or controls taken by the CII to protect the assets for smooth and error free operation. This validation is done by third party agencies which can be government or private empanelled agencies. The certifications must also deal with enforcing or implementing any international security standards available globally for the protection of critical assets working in the CII by respective organisations.

6.11.2 Each CII needs to devise a strategy to list the certifications which are needed to be implemented for the protection of their assets and in which areas.

6.11.3 Similar to certification of the CII facility, there is a requirement to ensure that personnel hold certifications relevant to their responsibilities. The currency of these certifications must be maintained. The security certification requirements of the employees engaged in the protection work at different levels and fields should be clearly chalked out.

6.11.4 Knowledge up gradations programs for the employees through new certifications, trainings, seminars, workshops etc should also be planned as per requirement of the respective CIIs.

6.11.5 Review and feedback process regarding the induction or deletion of security certifications for the assets and employees should be conducted periodically.

6.11.6 Implementation process of the security certifications should be properly monitored by the management so that the procedures may not affect the normal functioning of the CIIs.

6.12 **PC 12: Physical Security Controls**

6.12.1 The Physical Security tackles the threats, vulnerabilities, and countermeasures used to physically protect the CII's resources and sensitive information. These resources can be employee, work area, data, hardware and software equipments, support and back-up systems, storage media and supplies which are used in the smooth and efficient working of any CII. As per ISO 27001 physical security is to protect the organisation's assets by properly choosing a secure office location with a proper perimeter security through access control thus protecting the hardware and software equipments. The physical security in CIIs not only deals with the secure

software and hardware installation but it also deals with the personal background check of the employee with security clearance, proper backup facilities, Disaster recovery sites, office security etc.

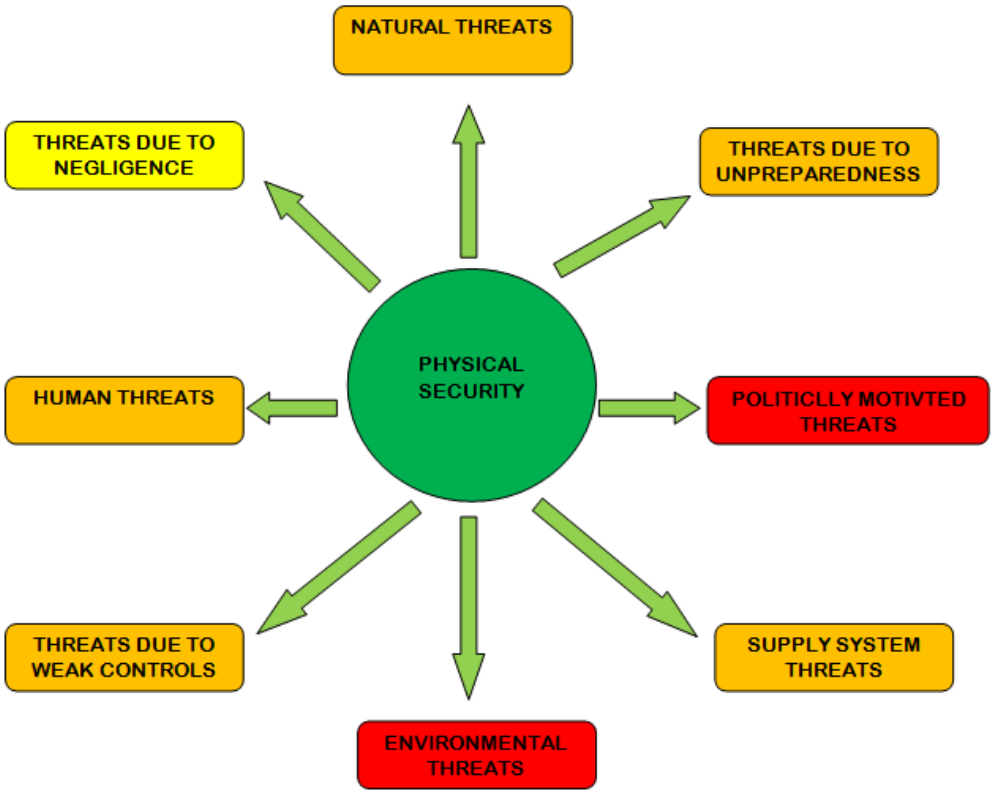

Figure 7: Physical and Environmental Security

6.12.2 Implication for not implementing the physical security control can lead to the debilitating effects of natural threats like floods, earthquakes or there can be environmental threats like extreme heat, lightning etc or human threats like explosions, disgruntled employees, trespassing etc. Supply system threats like power outages, communication interruption can also occur under physical security threats; weak implementation of physical security control mechanism can also lead to serious threats e.g. if fire alarm is faulty than the fire arising due to short circuit can go unnoticed; absence of audit and mock drills for checks and balances in physical control can lead to threats due to negligence.

6.12.3 **Best Practices**

(a) Proper plan with clear policies of how to implement physical security control should be devised.
(b) Proper Disaster Recovery site and back-up plans should be in place to deal with Natural and physical threats.

(c) For protecting the CII against environmental threats proper climate and precision control should be in place and proper protection against the negative effects of static electricity in the office place

(d) For fighting human threats security checks like CCTV cameras, swipe badges, access control policies, secure work area with strong building blocks and room construction should be in place.

(e) For supply system threats proper management is necessary e.g. use of UPS in case of power outage occurs or frequent power cuts. Back-up plans should also be there for supply system threats.

(f) Physical security plan should be properly implemented with proper guards deployed and good quality implementation of various security control gadgets for physical security with proper annual maintenance and service plan along urgent dealings with downtimes.

(g) Periodic audits and mock drills by the employees for addressing the issue of physical threats is must to deal with the situation. Audit and mock drills also provide insight in the lacuna existing in the implementation of the physical security control in the effective and strong manner.

(h) Many threats can only be addressed by strong management employee relationship and also with proper security guards guarding the situation on 24*7 basis monitoring for any suspicious behavior among some sections of employees.

(i) Devices would be placed in a controlled physical access environment with access only to authorized personnel.

7 Implementation Controls (IC)

7.1 IC 1: Asset and Inventory Control

7.1.1 Any strong security mechanism and especially security mechanisms for NCII must effectively implement Asset and Inventory control mechanisms. This is meant to correlate and track all physical and virtual assets owned by the CIIs. Asset inventory provides information that is important for day to day system management, CIIs asset tracking, and security incident response.

7.1.2 An asset inventory is also important for managing maintenance, servicing, theft prevention, controlling system builds, performing regular audits/reviews, replacing faulty systems and discarding/destroying/auctioning older/faulty systems. This control is essential to track unauthorized hardware or software. With this control in place every asset is assigned and issued to the employees / departments.

7.1.3 This control is also essential for formalising the access control list of the systems (software and hardware) used in the operation of the CII.

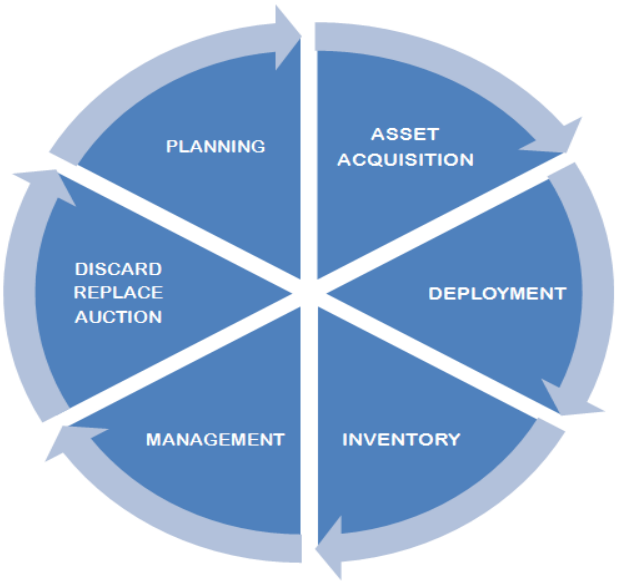

Figure 8: Asset and Inventory Management

7.1.4 Best Practices

(a) A dedicated team/department must be deployed for asset and inventory management, with clear roles and responsibilities.

(b) The entire hardware inventory must be clearly marked with uniquely identifying marks (e.g. serial no., model no.) for hardware devices like

servers, printers, laptops, desktops, fire alarms, access control devices etc.

(c) Similarly, software inventories can be made listing the product name, version, Serial Number, the device on which it is installed etc.

(d) Periodic review of the hardware and software inventory must be ensured.

(e) Movement of equipment / digital media etc from / to the CII, especially sensitive areas must be adequately controlled.

(f) For discarding/replacing/auctioning of the particular asset proper authorization from the management should be accorded and necessary updates be done in the inventory.

(g) Periodic audit of the asset and inventory management system should be conducted so as to unravel any flaws in the implementation of the asset and inventory management control. Status Reports of IT Devices may be verified periodically.

7.2 IC 2: Access Control Policies

7.2.1 Access control in the CIIs should follow a role based approach. Roles are containers defining specific access rights, responsibilities, approvals etc granted to specific classes / types of users.

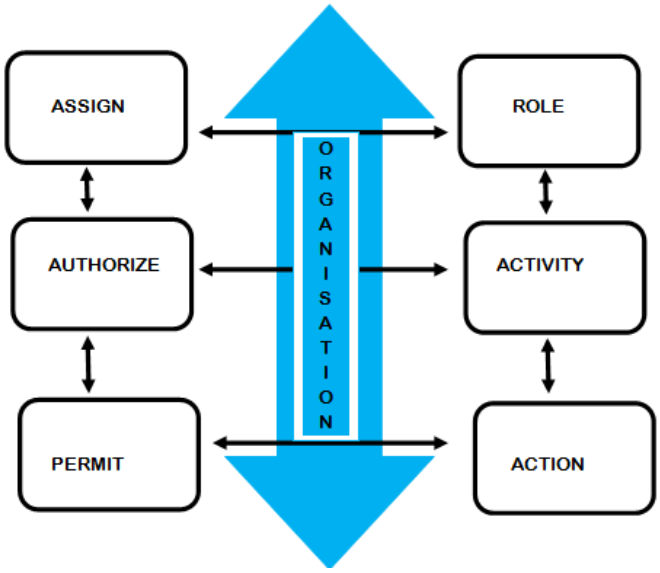

Figure 9: Access Control

7.2.2 **Best Practices**

(a) Segregation of responsibilities and corresponding roles is critical to avoid single point of failure where a single employee (or employees in collusion) may be empowered to assign, authorise and execute inimical actions.

(b) Assignment of roles and duties must be on an "As required" basis.

(c) Identify, prioritize and assign roles to all employees as per the policies, processes and systems

(d) Identification of Access controls required by the organisation based on systems etc in use, levels and types of access required etc.

(e) Identify and authorize the employees based on their roles and duties.

(f) Implement the proper access policies on the computer systems for physical authorization at the entry/exit of the CII area with further authorization at the sub-department and division level thereby implementing the multi-tier security access control.

(g) Implement the proper access control at the computer system level for authorizing the employee to do role based jobs in CII by creating proper user accounts with role defined and attached with it.

(h) Periodic check of the implementation of the proper access control policies at all the layers of the organisation network.

(i) Monitoring of the implementation of the access control policies.

(j) Checks and balances for violations or breaches in the implementation or working of the access control policies.

(k) Periodic review for audit and changes as per the organisational needs keeping in mind to increase the robustness of the access control policy implementation.

(l) Logical access to device configuration should be restricted to administrators.

7.3 **IC 3:Identification and Authentication Control:**

7.3.1 Proper implementation of the Identification and authentication control in the CII can check and trace the misuse of any asset belonging to CII, by an individual. Asset identification deals with providing the claimed identity to the system by any user whereas authentication checks the genuineness of the claimed identity. Identification of the person in relation to roles and responsibilities assigned in the organisation is essential to prevent impersonation attacks by attackers. This identification should always be

used in conjunction with the proper authorisation policies which will determine that whether the particular person is authorised to have an access to the restricted and role based facility in CII.

7.3.2 Absence of this control can lead to different types of threats which can hamper the popular CIA (confidentiality, Integrity and availability) model.

7.3.3 Proper session and token management should be in place with adequate encryption to avoid attacks such as impersonation /replay etc.

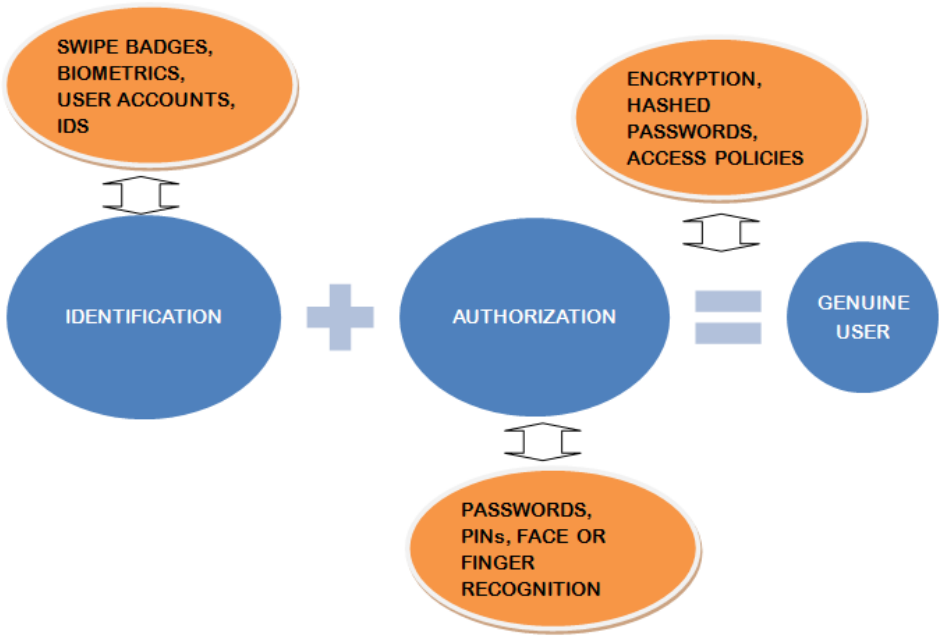

Figure 10 : Identification and Authentication

7.3.4 **Best Practices**

(a) Implement proper Identification and Authorization policies. Ensure all users are uniquely identified before permitting any task.

(b) Review all the access control for identification and authorization for disabling all those persons not associated with CII.

(c) There should be system access review mechanisms for terminated employees and contractors as also the employees and contractors leaving the organisation.

(d) Store the passwords in strong hash algorithms with salt.

(e) Authorization policies should be implemented by taking into consideration the role and assignments so that every action of the user can be mapped to its activities.

(f) There should be procedures to disable lost or stolen user identities including passwords.

(g) A reasonable cap on user failure attempts must be imposed.

(h) Effective monitoring of the accounts and access controls should be in place.

(i) Proper audit and feedback mechanism for strengthening the control should be implemented.

7.4 **IC 4: Perimeter Protection**

7.4.1 Perimeter zone of any CIIs will mostly comprise of Internet web servers, NIPS, NIDS, external routers, network, application and database firewall, proxy, Internet DNS servers. This perimeter zone is mostly prone to external threats and attacks originating from outside the organisational network. The defence points for the protection of perimeter zone includes routing security and redundancy with well designated ACL and routing design, hardening of the Firewalls, proxies, network and DNS servers. VPN and wireless security if used in the CIIs also plays a vital role in the protection of perimeter zone of the organisation's network.

7.4.2 In today's era of digitisation there are multi point entries to internet/other networks due to wide coverage of public mobile networks such as GPRS, 3G, WiMax etc. An end system can be connected to internet using USB based plug and play GPRS, 3G, WiMax devices, which can bypass many perimeter security measures and act as a backdoor entry into the network. Care is required to ensure that no such incidents occure in the organisation/enterprise.

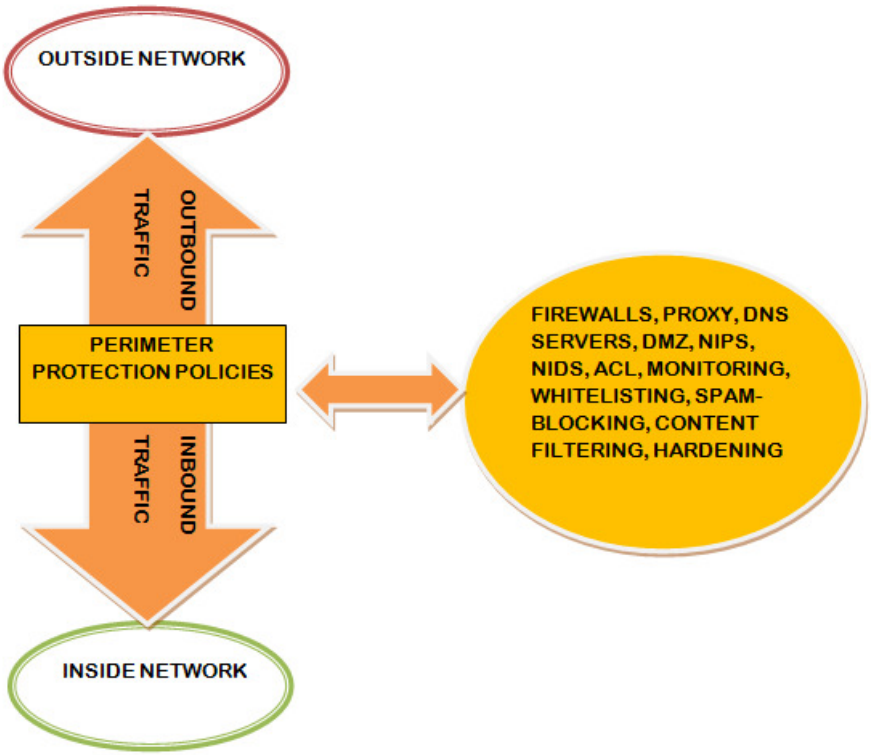

Figure11: Perimeter Protection

7.4.3 **Best Practices**

(a) Proper designing and implementation of the policies for protection of the perimeter zone.

(b) Deployment of NIDS and NIPS for all the intrusion detection and prevention by blocking on the basis of up-to-date signature database.

(c) Block all the connections (inbound and outbound) with proper ACL implementation following the white list approach – white list by definition allows only good IP's / calls / protocols etc

(d) Use Firewalls with proper protection policies as per functional requirements. Proper web content filtering of ingoing and outgoing traffic should be done.

(e) Sender policy framework for blocking spoofed emails should be devised.

(f) Websites should be allowed to access through domains instead of IP addresses.

(g) All the anti-virus, anti-spyware at the gateways and client machines should be up to date.

(h) All critical changes to the Security Device infrastructure would adhere to change management process.

(i) Access control, authorization, and auditing logging of all the devices under perimeter zone should be enforced.

(j) Implement system, application and database security to all internal infrastructure components.

(k) Clients should access the Internet through DNS server, e-mail server, or an authenticated web proxy for effective monitoring and auditing.

(l) DMZ web servers should be allowed to be accessed through proxy for proper tracking of incoming connection.

7.5 **IC 5: Physical and Environmental Security**

7.5.1 Implication for not implementing the physical security control can lead to the wide ranging of threats like there can be natural threats like floods, earthquake; there can be environmental threats like extreme heat, lightning etc; human threats like explosions, disgruntled employees, trespassing etc. are also prominent under physical security; Supply system threats like power outages, communication interruption can also occur under physical security threats; weak implementation of physical security control mechanism can also lead to serious threats e.g. if fire alarm is faulty than the fire arising due to short circuit can go unnoticed; absence of audit and mock drills for checks and balances in physical control can lead to threats due to negligence; threats like riots etc can also pose threat to physical security of the CII.

7.5.2 **Best Practices**

(a) Proper plan with clear policies of how to implement physical security control should be devised.

(b) Proper Disaster Recovery site and back-up plans should be in place to deal with Natural and physical threats.

(c) For protecting the CII against environmental threats proper climate and precision control should be in place and proper protection against the negative effects of static electricity in the office place

(d) For fighting human threats aequate security checks like CCTV cameras, swipe badges, access control policies, secure work area with strong building blocks and room construction should be in place.

(e) For supply system threats proper management is necessary e.g. use of UPS in case of power outage occurs or frequent power cuts. Back-up plans should also be there for supply system threats.

(f) Physical security plan should be properly implemented with proper guards deployed and good quality implementation of various security control gadgets for physical security with proper annual maintenance and service plan along urgent dealings with downtimes.

(g) Periodic audits and mock drills by the employees for addressing the issue of physical threats is a must. Audit and mock drills provide insight in the lacuna existing in the implementation of the physical security control.

(h) Many threats can only be addressed by strong management employee relationship and also with proper security guards guarding the situation on 24*7 basis monitoring for any suspicious behavior among some sections of employees.

(i) Proper checks and balances for the implementation of the physical security control with appointment of security officer. The security officer should look into the loopholes in the implementation process of physical security and also should be in touch with the management related to any physical security breach.

(j) Devices must be placed in a controlled physical access environment with access only to authorized personnel.

7.6 **IC 6: Testing and Evaluation of Hardware and Software**

7.6.1 This control highlights risks associated with inherent vulnerabilities of Commercial off-the Shelf (COTS) products and code appended with the Hardware/Software. These products may contain worms, malwares etc which can bypass security checks in the network.

7.6.2 Organisations need to be cautious in deploying possibly contaminated hardware or software products, especially in CII. After procurement and before deployment of hardware there should be an in depth testing and evaluation of systems. The Common Criteria Evaluation and Accreditation (CC EAL) approach could be followed if appropriate.

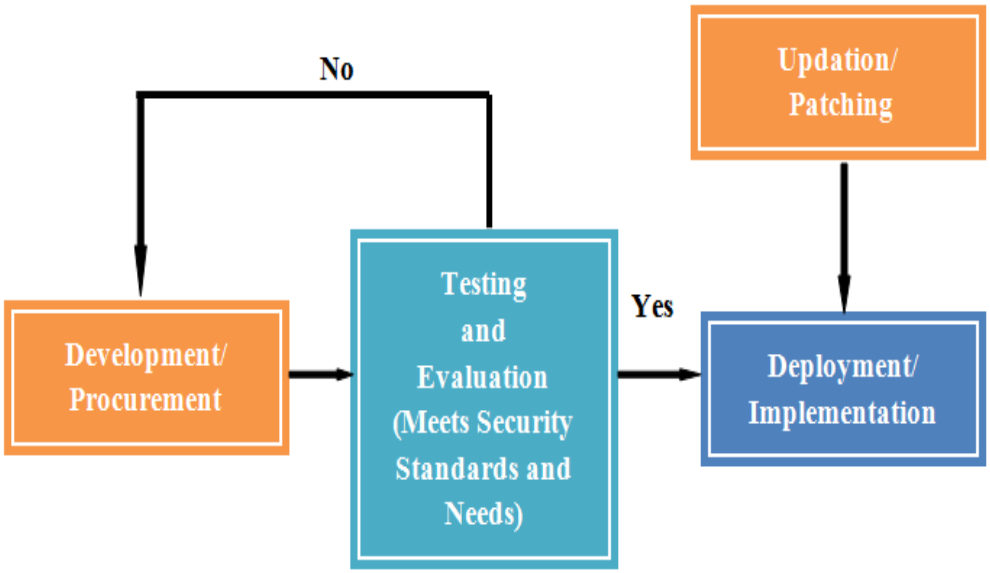

Figure 12: Testing and Evaluation of Hardware and Software

7.6.3 Best Practices

(a) An evaluation criterion should be decided for hardware and software procurement and use.

(b) Timely Equipments and software used in critical sectors should be tested and evaluated before installation. An evaluation chart, reflecting the security indices of equipments and softwares may also be prepared.

(c) Updation and patching of software and hardware should be ensured. Use of outdated or obsolete technology should be avoided as far as possible.

(d) Organisations should use robust hardware and software.

8 Operational Controls

8.1 OC 1: Data storage: Hashing and Encryption

8.1.1 Storage of data can be covered in different modules like regarding system configuration data, operational data copyright or classified information, user credentials, backup data etc. This data is critical for the proper functioning of any infrastructure, leave aside CII. Under this control data should be securely stored and preferable encrypted using strong encryption algorithm.

8.1.2 User credentials should be stored with strong hash algorithm with proper salt added to it.

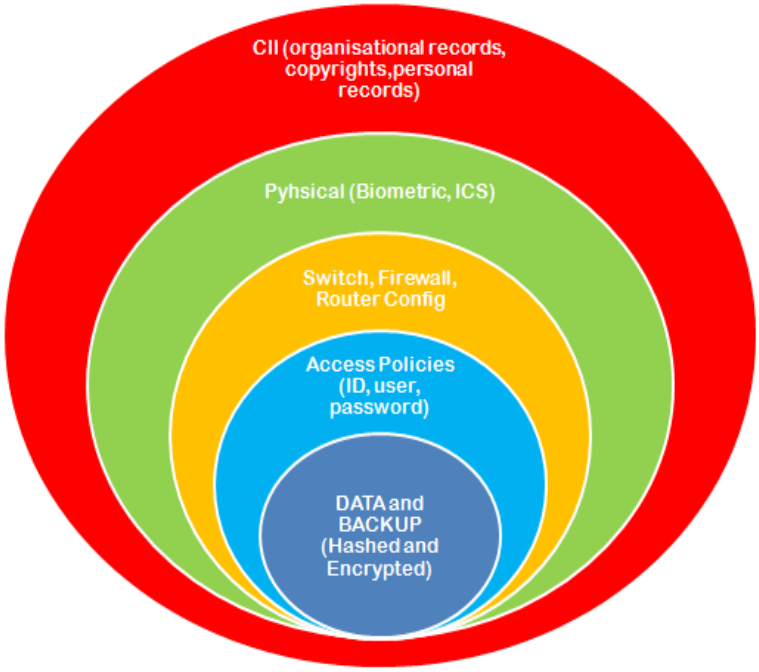

Figure 13: Data Storage

8.1.3 **Best Practices**

(a) Identify the classified and sensitive data to be protected through hashing and encryption.
(b) Proper hashing and encryption policy for the Critical data in CII issuing clear guidelines to all the employees of the organisation.
(c) Proper compliance of the policy guidelines regarding the hashing and encryption of the data.

(d) Checks and balances to pro-actively thwarting the violation of the policy guidelines regarding the encryption and hashing of stored data.
(e) Ensure the compliance of the encryption and hashing policy for back-up data also.
(f) Feedback and evaluation for checking the strength of the implemented algorithms for hash and encryption on periodic basis.
(g) Initiation to implement new algorithm for hashing and encryption of data if any flaws are reported in the already implemented algorithms.

8.2 OC 2 Incident Management - Response

8.2.1 There should be effective Incident Response strategy to deal with post incident damage handling which if not discovered or detected by the organisation or CII in the first place can lead to serious damage to the organisation. Incidents can be physical, environmental or computer attack related.

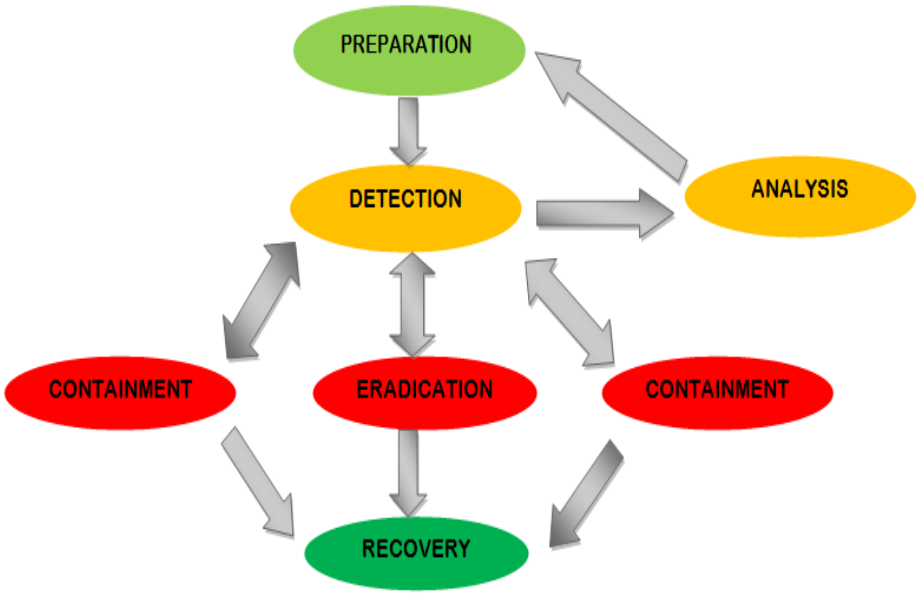

Figure 14: Incident Response

8.2.2 Physical incidents can be related to forced physical entries and destruction or stealing of resources in the CII areas. Environmental incidents can lead to hazards like earthquake, lightening, floods etc. Computer attacks as evident is related to any form of computer attacks which can lead to infiltrate and steal of classified data, exploitation of the CII

resources or altering the configuration or data leading to serious damage or implications.

8.2.3 **Best Practices**

(a) Develop an incident response plan with clear roles and responsibilities. This must include a clearly demarcated escalation matrix.

(b) Clear roles of management for their duties and decision making at the time of incidence.

(c) A containment and recovery plan must be clearly enunciated and promulgated amongst all concerned.

(d) The recovery mechanism must ensure that the original vulnerability is removed before making the system operational.

(e) Once recovered, systems should be analysed for the remains or traces of the cyber incidents to thwart and wipe the remaining cyber intrusions.

(f) An analysis of the incident including recommendations must be submitted to the management for increasing the effectiveness in handling similar incidents in future by incorporating any amendments in incident response plan.

8.3 OC 3: Training, Awareness and Skill up-gradation

8.3.1 Skills and knowledge are the driving forces for progress of any organisation. They have become even more important due to increasing intricate technological changes and consequent vulnerabilities.

8.3.2 A formal process to formulate and enforce training strategies, policies and automate compliance processes to facilitate the development of employees in the Organisation by prioritizing risks and vulnerabilities that span across locations and Organisations must be established. This may undertake, inter alia:

(a) Periodic review of the training strategies, plans and programs.

(b) Coordination with ISD in identification and evaluation of vulnerabilities and security threats.

(c) Evaluation of available resources and plan accordingly to examine and evaluate training and other skill programs in the Organisation.

(d) Identification and assessment of the skills development needs and ensure its implementation.

(e) Educating employees and the Organisation on skill development strategies and assocaited processes and procedures.

(f) Act as a committed leader in the skill development programs, strategies and their adequate implementation.

(g) Set up a training committee accountable for identification and facilitation of sophisticated trainings.

(h) Timely advise the Organisation on the trainings and other such skill development programs.

(i) Serve as an interface between the Organisation and the external service providers related to trainings and other such skill development programs.

(j) Ensure the compatibility of Organisation's training policies, programs, procedures and strategies in line with the rules and regulations as laid down by the Government.

(k) Create a skills performance system to examine and evaluate to ensure its' credibility for the Organisation, where no such system exists. Create a data record of evidence of trainings for all employees those have and shall receive training in the company.

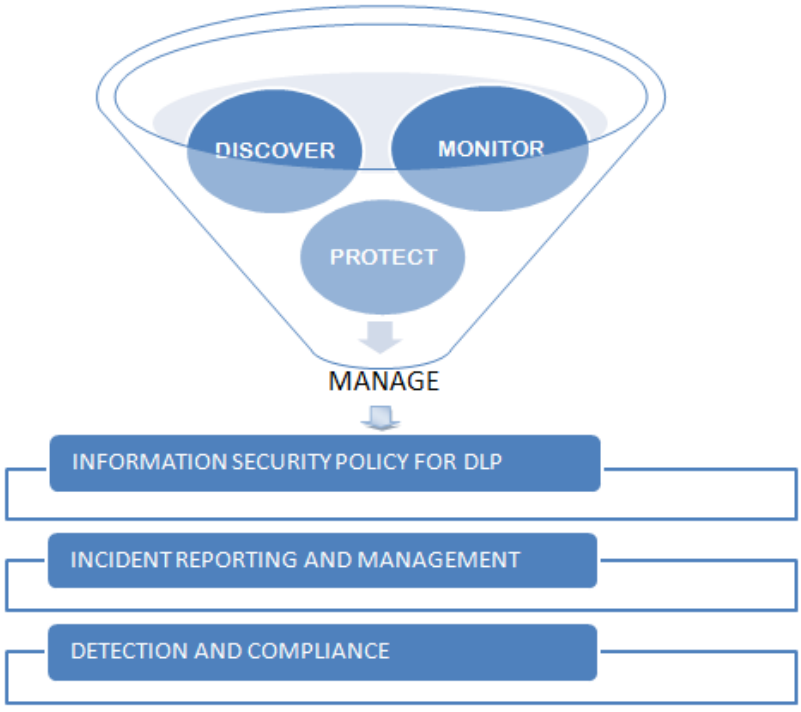

Figure15 : Data Loss Prevention

8.4 OC 4 Data Loss Prevention

8.4.1 Data loss prevention is a leading issue in the protection of CIIs. Data loss may lead to serious implications in the smooth and proper functioning of the CII. Data loss can be in the form of data leakage or in the form of data distortion, corruption, manipulation etc.

8.4.2 **Best Practices**

(a) Identification, authorisation and validation of the all the data storage devices.

(b) Sound Store Inventory procedure should be in place for different data storage mechanisms /media.

(c) Proper Backup plan and policy should be in place for the protection of all types of data on the regular basis.

(d) Network Monitoring tools for monitoring the unauthorized flow of data should be worked out by tracking sessions.

(e) Content filtering Perimeter protection devices to block the restricted or classified information by performing content-aware, deep packet inspection including email and other protocols.

(f) Dedicated Information security policy for the management and use of mobile storage devices like USB, CD/DVD, Floppy, and Smart phones etc should be controlled. The IS policy of CII should prevent the use of personal input devices in the office environment.

(g) Use of proper encryption algorithm for the protection of data in the storage devices.

(h) Information security policy curbing the information leakage attempts by Detecting, blocking or controlling the usage of specific content based on organisation's rules or policies.

(i) Proper checks and balances for the proper implementation of the data loss prevention policies.

(j) Ensure proper physical and environmental security along with proper identification and authorization for accessing the classified data.

(k) Only official email id to be used for official communication and correspondence alongwith digital signatures and encryptions wherever necessary.

(l) Control of PCs/Laptops in work places through End Point Protection

8.5 OC5 Penetration Testing

8.5.1 Assets, employees, processes and technology are the building blocks of any CII. “Penetration testing” evaluates and tests the preparedness of any organisation or CII in fighting threats originated from the weak or flawed implementation of the CIIP program. penetration testing is the methodology used to validate the overall security of the CII from all the different types of internal and external threats. The testing is aimed to uncover real time vulnerabilities or loopholes exiting in the infrastructure which can be exploited by malicious entities.

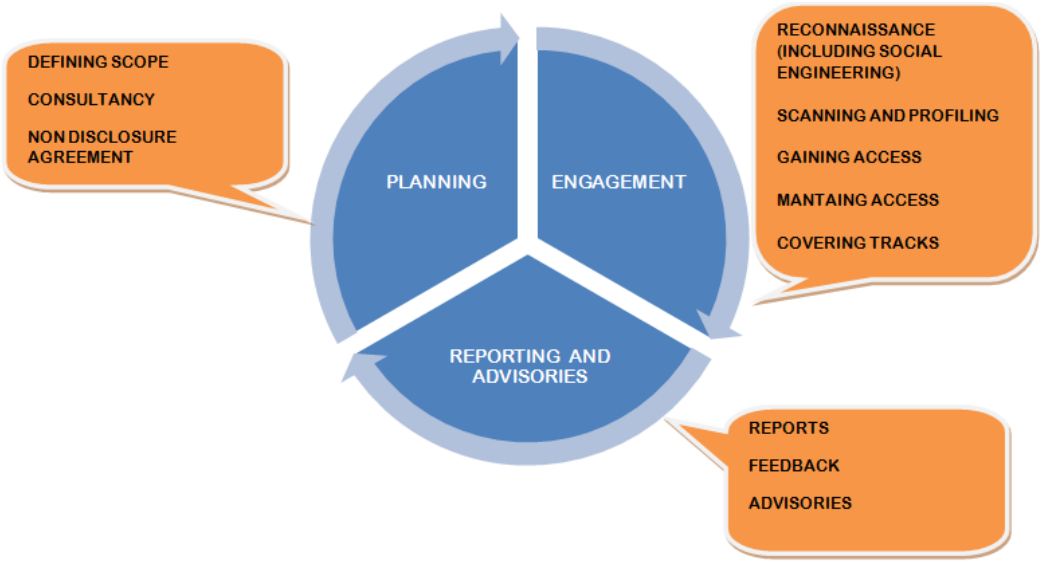

Figure 16: Penetration Testing

8.5.2 The absence of the control leads to oversight of some of the major flaws or vulnerabilities that could exist in the CII.

8.5.3 **Best Practices**

(a) Devise the mechanism involving the employees of the CII and external professional consultancy for the conduct of penetration testing for the assets of CII.

(b) If some outside professional bodies are involved for penetration testing Non Disclosure Agreement should be signed so that any restricted information gathered by the Pentesting Team during testing is not divulged.

(c) There should not be any damage to the operational sanctity of the CII while doing these tests. Vulnerability testing must not lead to system

collapse. The entire process of vulnerability trsting must be an elaborate, well thought out and calibrated exercise.

(d) Social engineering part is very important in the success of major attacks on any CIIP, therefore this element should be taken into consideration while performing the penetration testing.

(e) Review and implement the important feedback emanating from penetration testing and mock drills

(f) Penetration test should cover all the levels of security like physical, external, internal, web application, network, perimeter protection, client-side, hardware, software, data storage, access control, logging security into consideration.

(g) Test bed environments can be created for penetration tests related to Industrial control systems as the real time tests on these control systems might not be possible.

8.6 OC 6: Asset and Inventory Management

8.6.1 One of the most important steps in the critical assets management and security is asset and inventory management which correlates all the physical and virtual critical assets owned by the CIIs. Asset inventory provides information that is important for day to day system management, CIIs asset tracking, and security incident response. An asset inventory is also important for managing maintenance, servicing, theft prevention, controlling system builds, performing regular audits/reviews, replacing faulty systems and discarding/destroying/auctioning older/faulty systems.

8.6.2 Absence of the control can also make it difficult to formalise the access control list of the software and hardware to be used in the operation of the CII. Implementation of information security policies and security controls will also be difficult on each critical asset in the absence of proper inventory management.

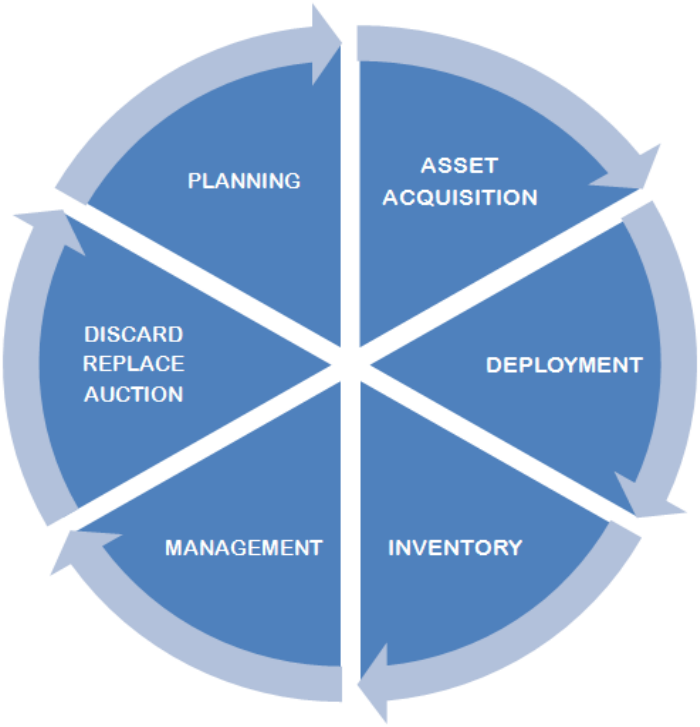

Figure 17: Asset and Inventory Management

8.6.3 **Best Practices**

(a) Complete asset and inventory management policy should be drafted and implemented strictly in the CIIs.

(b) The entire hardware inventory like serial no., model no., quantity etc for the hardware devices like servers, printers, laptops, desktops, fire alarms, access control devices etc must be managed.

(c) All the software inventories can be made listing the product name, version, the device on which it is installed etc.

(d) Periodic review of the hardware and software inventory should be made to update the records for better inventory management.

(e) Equipments taken out of the office e.g. laptops, CDs etc should be allowed by proper authorization from the management and receipt from the concerned employee.

(f) Inventory should be managed in accordance with the date of purchase and physical location of deployment.

(g) Each asset assigned to employee should have proper receipts with signatures.

(h) Periodic audit of the asset and inventory management system should be conducted so as to unravel any flaws in the implementation of the asset and inventory management control.

(i) Status Reports of IT Devices may be verified periodically.

8.7 OC 7: Network Device Protection

8.7.1 There are numerous sources viz. Configuration Violations, Weak Authentication, Obsolescence, and various kinds of attacks etc of the common loopholes in the network devices. Organisations must keep a vigil on the latest threats and prepare themselves to counter vulnerabilities and mitigate risks.

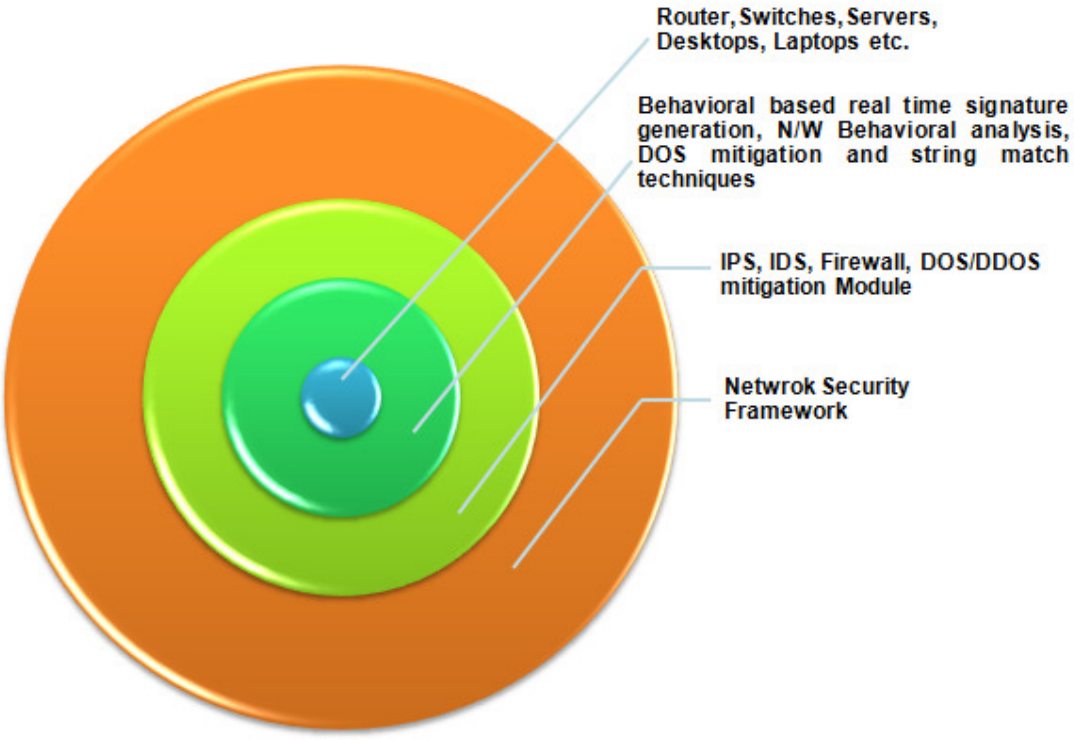

Figure18: Network Device Protection

8.7.2 **Best Practices**

(a) Change default authentication schemes and use strong passwords.

(b) Passwords should be changed periodically.

(c) All the Access Control lists must be implemented as per the requirement of security policy of organisation.

(d) Incoming and outgoing traffic must be monitored and analyzed.

(e) Security patches must be updated. If the support has expired, it must be renewed at earliest.

(f) Network topology and architecture should be in conscience with the sensitivity of organization.

8.8 OC 8: **Cloud Protection**

8.8.1 With the continuous expansion of digital world and ever rising dynamic complexities, shared services and resources have become one of the prime need of organisations and enterprises. In such direction, cloud computing has become a significant part of their infrastructure. The concept of cloud computing envisages use of computing resources that are delivered as a service over a network. The complex infrastructure of cloud entrusts remote services with a user's data, software and computation the information /data stored on remote servers which is accessed by remote users /client. Cloud providers manage the infrastructure and platform that run applications. There are different types of cloud like public cloud, private cloud, community cloud, hybrid cloud etc., which are used by organisations /enterprises on the basis of their needs. The control over the information /resources shared on cloud depends on the services provided e.g. Software as a Service (SaaS) Platforms as a Service (PaaS), Hardware as a Service (HaaS) and Infrastructure as a Service (IaaS) etc.

8.8.2 There are numerous benefits of all clouds in forms of services, cost, efficiency and reliability. However, clouds are best effort infrastructure, albeit with liabilities – they are not immune to threats /attacks. There is a lot critical information /data stored on computers, which is now being transferred to the cloud .It demands the need for timely security measures at the organisational, cloud provider, user and other such levels which are involved in this process. Some threats to cloud based computing are:

(a) Insecure applications stored on cloud.

(b) Insecure interfaces to access the cloud.

(c) Users with malicious intent.

(d) Technology vulnerabilities.

(e) Data loss, leakage or theft.

(f) Hacking or hijacking of user accounts, services or applications.

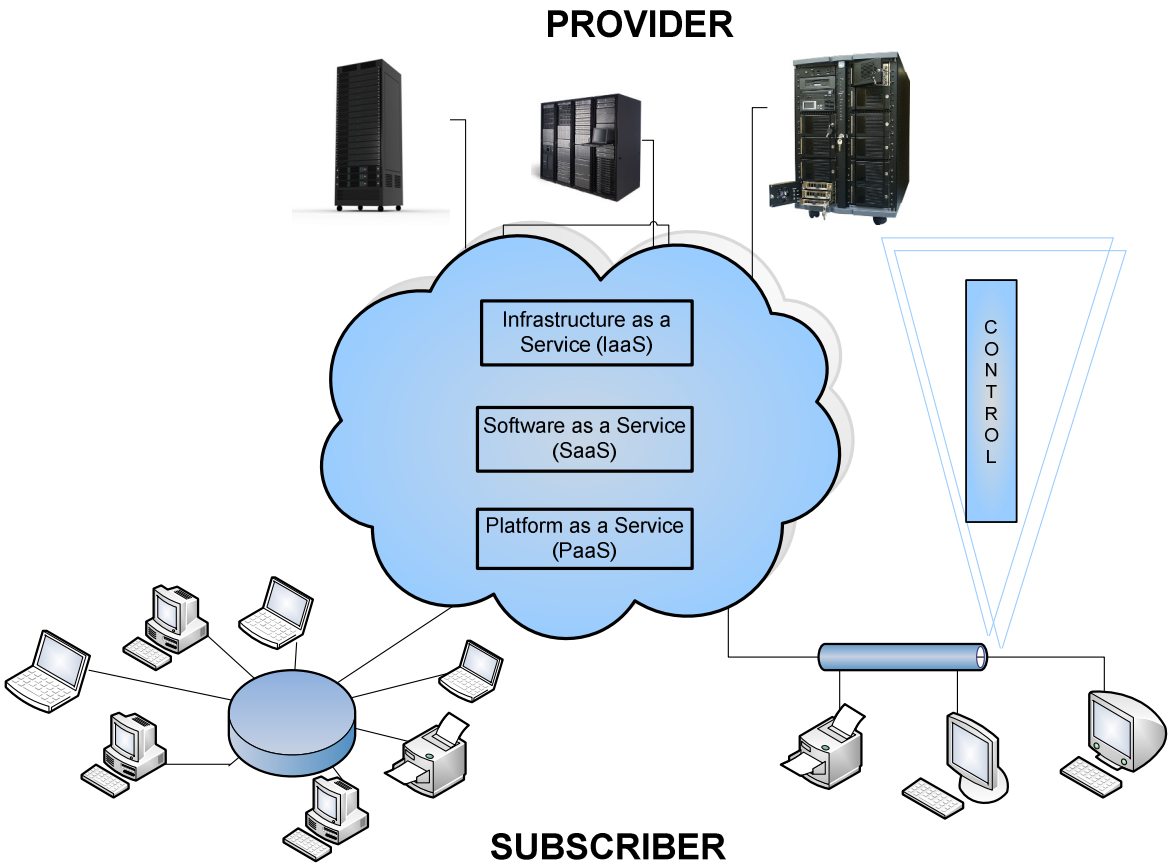

Figure 19: Cloud Protection

8.8.3 **Best Practices**

(a) Ensure that cloud provider is using strong encryption methods.

(b) Data backup must be managed by the organization /enterprise itself.

(c) There must be barriers to keep critical information separate from other information and organisations.

(d) Cloud-Organization and Cloud-Cloud interlinkages must be secured.

(e) It should be ensured that the information data is accessible to authorized users only.

(f) Logs at provider's end should be maintained .and stored in encrypted from. Access to logs must be limited to minimum persons.

(g) Security related issues /aspects may be covered under Service Level Agreements (SLA).

(h) As a rule, access to critical information should be minimum particularity from mobile endpoints. In cases, when it is required to

access the information from mobile endpoints, their access points, devices or end points must be secured. This is equally applicable to cloud connectivity as well.

(i) There should be adequate authentication mechanism to avoid any chances where an attacker can pose as a cloud subscriber.

(j) Threat/Risk management and mitigation strategy on cloud security should be part of IS Policy.

(k) There should be a breach reporting mechanism for any security related incident not only in the data that provider holds for subscriber but also the data it holds about the subscriber.

(l) Client side and server side systems must be protected by timely updating, patching etc.

(m) Access to information, network services, operation system, application and system should be controlled.

8.9 OC 9 Critical Information Disposal and Transfer:

8.9.1 The scope of this control encompasses all electronic hardware, digital media etc. capable of storing information handled by the CII. A secure disposal and transfer policy with appropriate safety measures for all the media storing the critical information should be in place. This must outline the detailed steps for the employees to be followed. This control covers media storing the information like hard disk drives (both internal and external to systems, desktops, servers etc.), optical devices (CD-R/RW, DVD-R/RW, MOs), Diskettes (floppies and floppy disks), solid state devices (flash media, USB or thumb drives etc.), PDA and cell phones, papers and files etc.

8.9.2 The absence of this control, or, improper implementation of this control can possibly compromise information security. The figure shown below illustrates the basic approach for handling transfer and disposal of various information storage media under any critical infrastructure. There are basically three methods for dealing with the disposals of the storage media viz. Wiping/cleaning/overwrite, degauss and physical destruction. Wiping deals with the formatting and overwriting of the information in the storage media for actually deleting the data stored which is not possible with simple delete. Degauss is process of wiping information in magnetic tapes, drives etc. whereas physical destruction is shredding, pulverising or complete burning etc.

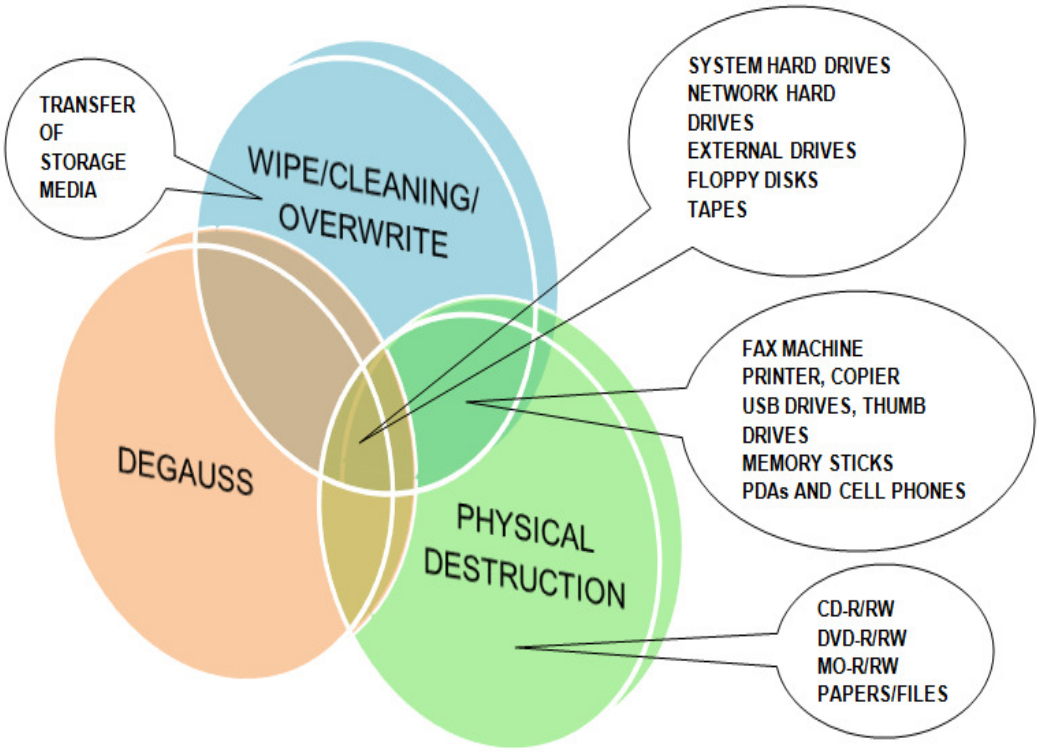

Figure 20: Critical Information Disposal And Transfer

8.9.3 **Best Practices**

(a) Information, storage media disposal and transfer policy should be drafted and enforced clearly indicating the administrative procedures and technical guidelines for all the employees dealing with information duly approved by the management.

(b) Policy should include the periodic board formation of the senior employees under the lead of CISO duly approved by the head of the organization for the disposal of storage media.

(c) Periodic audit should be in place to verify the storage media disposal process as drafted in the organization policy.

(d) Proper logs of the transfer and disposal of information storage media should be maintained.

(e) The transfer of media should also include the appropriate changes in the inventory management control along with proper gate pass approvals if media is leaving the premises of the organization.

(f) Returned storage media in the inventory or store should be securely and safely stored in the fireproof safes till the policy is enforced.

(g) Classified draft papers and files should be shredded if not in use. Till the information is in use before the finalization, papers should be stored in the fire safe storages instead of loosely storing them in desks as per the clean desk policy.

8.10 OC 10 Intranet Security

8.10.1 An intranet is an internal network system which is based on the existing internet protocol technologies and is owned by any single organisation to share its information and resources through communication between tits remote sites, where external network users have strong restricted access to this network. The basic components in the intranet are almost same in all the CIIs i.e servers, workstations, TCP/IP services, network protocols etc. Intranets can also consist of virtual networks based on the user groups, work allocation and assignments. There are numerous advantages prompting most of the CIIs to switch to intranet. Most common benefits being paperless work environment, drastic reduction in time for work completion, increased productivity through enhanced collaboration and common organization culture, centralised resources and fast updates etc. The content residing in the intranet can be classified in basic three categories: open source contents, CIIs content and restricted content. Open source content is openly or publically available which can be used as news, knowledge updation, jobs listing etc. for the employees. CIIs content is the content restricted for the employees of the CII only whereas restricted content is for particular user group working on particular tasks.

8.10.2 **Best Practices**

(a) The IS policy of the organisation should clearly mention the policies and procedures for intranet security and its implementation.

(b) The intranet access types can be classified by the respective organisation depending upon their functional and operational needs like employee access, restricted user access, restricted user editing access, administrative access. Biometric, smart cards, passwords etc can be used for all the user accounts

(c) There should be separate monitored and controlled permissions for viewing the folder.

(d) Content accessible on the intranet should be encrypted and password protected and only authorised user should be allowed to view or edit depending upon their user classification.

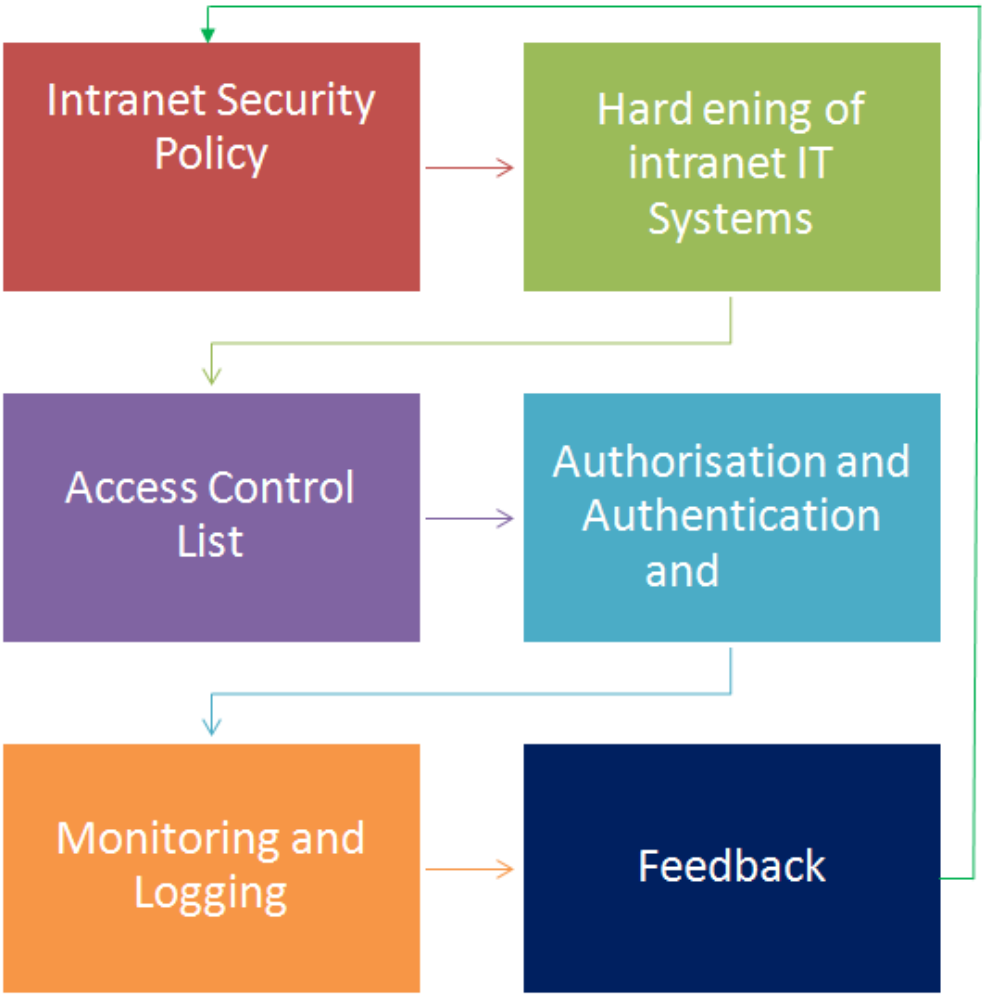

Figure 21: Intranet Security

(e) Complete isolation of the intranet from the public network should be maintained.

(f) All systems on the intranet should be regularly updated with latest patch, OS, anti-virus, anti-malware and security signatures etc.

(g) All the IT systems on the intranet should be hardened to perform only the minimum desired services.

(h) Complete logging of the traffic generated in the intranet should be logged and monitored regularly.

(i) Periodic audit and pentest of the intranet networks is essential.

(j) Movable devices e.g pen drives, hard drives etc. should be either prohibited in the intranet or should be assigned proper permissions after verification. Their usage should be monitored.

(k) E-mail filter should be there to block and track malicious traffic like spam, phishing, spyware, addware, malware etc.

(l) Confidential data in intranet can be protected from unauthorized access by the malicious attackers through use of SSL digital certificates.

8.11 OC 11: APT protection

8.11.1 Advanced Persistent Threat (APT) refers to the long-term pattern of targeted attacks. These sophisticated attacks are generally aimed at Governments, Financial Institutions and Political organisation's computer resources and websites.

8.11.2 These are unlikely to be detected by simple security methods for a reasonably long time. Defence capability acquisition and enhancement by and shoring up detection capabilities against APT has gathered great importance. Instead of relying on Cyber Firewalls, organisations are needed to equip themselves with the Human Firewalls i.e. employees should be trained enough to become security sensitive and aware.

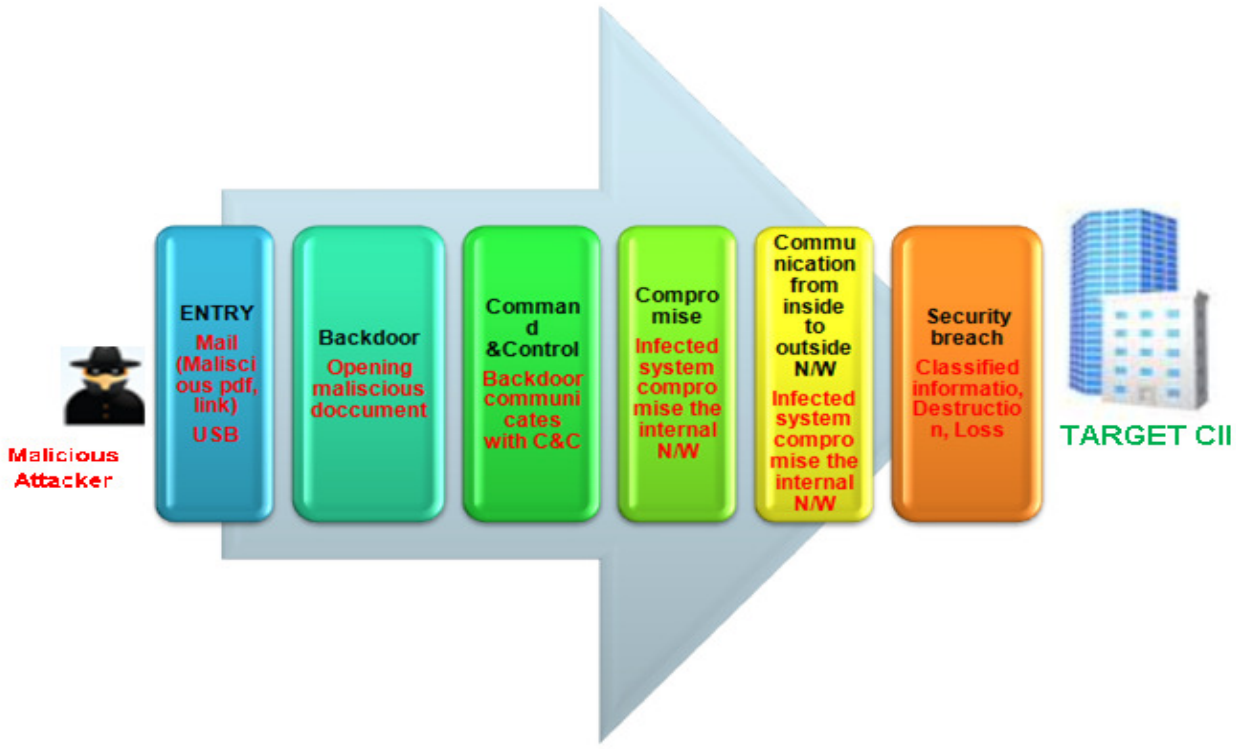

Figure 22: Apt Protection

8.11.3 **Best Practices**

(a) In case it is unavoidable to transmit information through internet, the technology and process used should be reasonably advanced that provide the best level of security and privacy available in the circumstances.

(b) Electronic Information should be password protected and guarded by multiple levels of electronic barriers.

(c) Permission to access the Computer accounts is crucial. System Administrators and users should be restricted with the minimum rights they need to do their job.

(d) Protection against computer intrusions that must include, at a minimum, current and regularly updated malware protection and prompt application of security-relevant software upgrades, such as patches, service packs and hot fixes.

(e) Any detection of APT attack must be reported with minimum time delay. The reporting should include date and time of attack and it's detection, methodology used and the system and information assessed along with the potential impact.

9 Disaster Recovery /Business Continuity Planning Controls (DR)

9.1 DR 1: Contingency Planning – graceful degradation

9.1.1 Contingency planning refers to a risk management perspective nurtured through proper assessment, policies, plans, procedures and technology involvement aimed at dealing with disruptions due to any disaster or major CII attack. This planning deals with alternate methods / sites of operating the CIIs in case of disruption. This control also deals with the restoration of effected services as soon as possible.

9.1.2 The entire aim of the Contingency planning is to reduce the impact of the disaster or any major CII outage to the minimum. Disruptions covered under Contingency planning can be due to natural, environmental or human threats. There are different plans covered under contingency planning e.g. continuity plans, recovery plans, communication plans, cyber incident response plan, disaster recovery plan, priority resource and manpower allocation plan, emergency plan etc.

Figure 23 : Contingency Planning

9.1.3 **Best Practices**

(a) Contingency planning statement of the CII should be conceptualized, formalized and implemented as soon as possible at the early stages of the formation of the organisation.

(b) Entire planning and policy formation should cover the continuity plans, recovery plans, communication plans, cyber incident response plan, disaster recovery plan, priority resource and manpower allocation plan and emergency plan in order to ensure integrity of the CII.

(c) Regularly update and analyse the contingency plans.

(d) Employees designated with the roles and responsibilities under contingency planning should be trained regularly.

(e) Impact analysis for different types of disruptions should be chalked out to strategise effective contingency planning.

(f) Proper tests and audit for the implementation of the contingency planning is a must to fill any detected gaps.

(g) Incorporate feedback and experience from the previous implementation of the contingency planning.

9.2 DR 2: Data Back-up and Recovery Plan, Disaster Recovery Site

9.2.1 One of the most important aspects of continuity management is to plan and implement disaster recovery site or backup sites. In the event of disaster the backup or the disaster recovery site will host the essential or bare minimum services to run the most critical part of the CIIs. Basically, disaster recovery sites can be broadly categorised into three categories:

(a) **Hot disaster recovery site**: This is the most expensive approach for implementing a disaster recovery site but the recovery time is barely a few hours as this hot disaster recovery site is the virtual mirror image of the original CII site.

(b) **Warm disaster recovery site**: The warm disaster recovery site is already housed with the appropriate hardware and software but it will take some time to commence operations as per the latest operating procedures and policies with latest data in usage.

(c) **Cold disaster recovery site**: This approach for the disaster recovery is least expensive but as the name suggests, has the least amount of systems configured / live data.

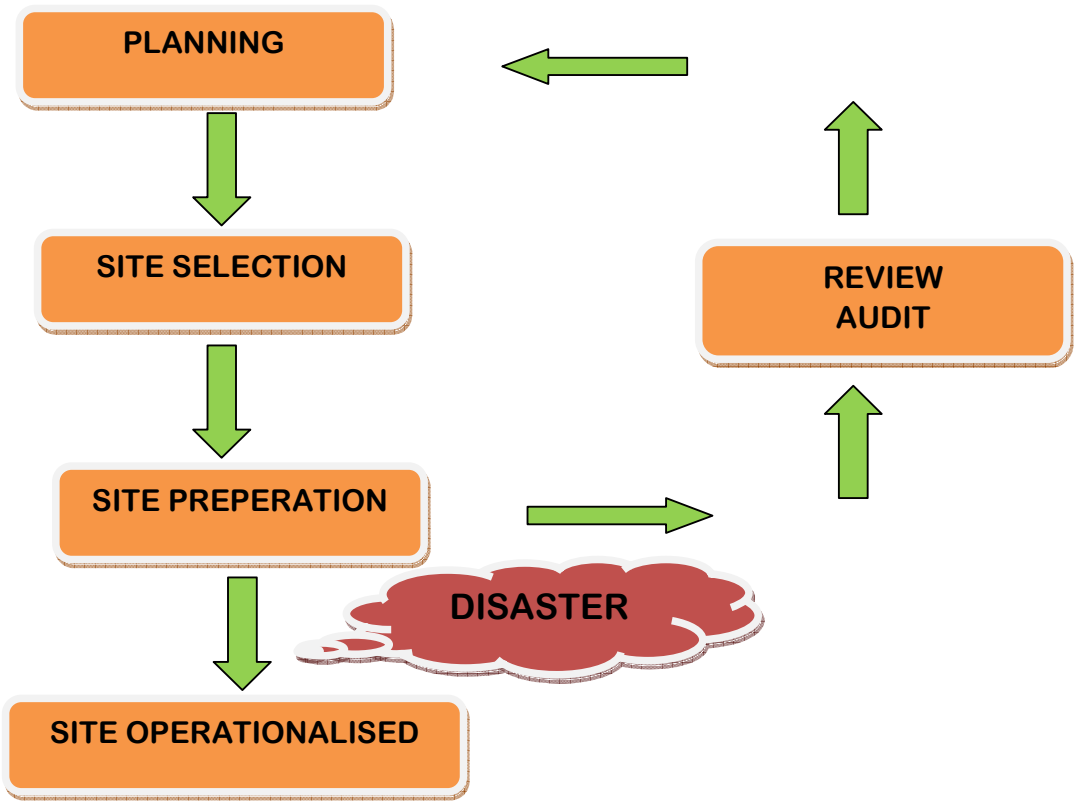

Figure 24: Disaster Recovery

9.2.2 In case of disasters like earthquake or heavy flood the actual site could be completely destroyed - at this time a properly selected and implemented disaster recovery site can allow the services to be resumed within the least amount of time, thereby reducing the impact of the disaster on the functioning of CII and its interdependencies. Effective choice and implementation of Disaster recovery site also includes resource and manpower allocation.

9.2.3 **Best Practices**

(a) Disaster recovery site selection policy, procedures and implementation should also be formalized at the early stage of formation of CII.

(b) Proper care of natural and environmental threats should be made before the selection of alternate site.

(c) Proper roles and responsibilities with resource allocation should be clearly defined if the need to work from the disaster recovery site arises.

(d) Basic amenities of water, electricity, transportation, internet connectivity etc. should also be checked before the selection of DR site as per the organisations need.

(e) Comparative assessment of other DR sites belonging to CIIs available domestically and internationally should be made to choose the right DR site for the recovery process.

(f) The review, audit and feedback of the disaster recovery site is a must for the smooth operationalisation of the same at the time of disaster.

(g) Thorough training process and mock drills of the employees charted with duties for resuming the operations at the time of disaster at the DR site should be accomplished periodically.

(h) Data back-up plan needs to be implemented in parallel at the DR site if the same is critical for normalising the operation in the event of disaster.

9.3 DR 3: Secure and Resilient Architecture Deployment

9.3.1 Secure architecture deployment refers to the safe and secure establishment and execution of the Information and network architecture in the organisation or CIIs in accordance with the IS policy of the concerned CIIs keeping in view the balance between the Business/Service, Information, Technology and security architectures. The basic idea is to attain the goal of information security keeping in view the functional needs of the organisation so as to avoid redundancy, over spending, inadaptability and over complexity in the process and architecture devised for the information security of the CIIs. Secure architecture deployment also includes the safe and secure deployment of the new technologies like Cloud computing, intelligent networks, and their interconnections for maintaining pace with the rapid change in technology to improve working culture and efficiency.

9.3.2 This secure architecture before finalisation should provide a rigorous taxonomy and ontology in clearly identifying the roles, responsibilities, processes and networks to be implemented that best suits the Information security requirement along with the functional needs of the CIIs keeping in view the Information, security, Service/ Business and technology architecture. Implementing organisation information security architecture generally deals with collating the organisation's strategy and other necessary details related to its operation.

9.3.3 In secure architecture deployment the Information technology components like process flows, Organisation timings, Applications and software inventories, events, messages, data flows, Intranet, Extranet,

Internet, e-Commerce, Data classifications, Databases , servers, network components , security devices, LAN, WAN etc. are related explicitly to the organisation's strategy, goals, and operations. Non implementation of this control can have major implication in the proper and successful implementation of the IS policy belonging to particular CII. Absence of this control leads to oversight of some of the modules requiring stringent protection mechanism, can also leads to improper visualisation of the design of information security policy, can leads to over complexity of the networks due to non mapping of the technology with CIIs goals and functions, improper upgrades and adaptability to new rapid changing technology.

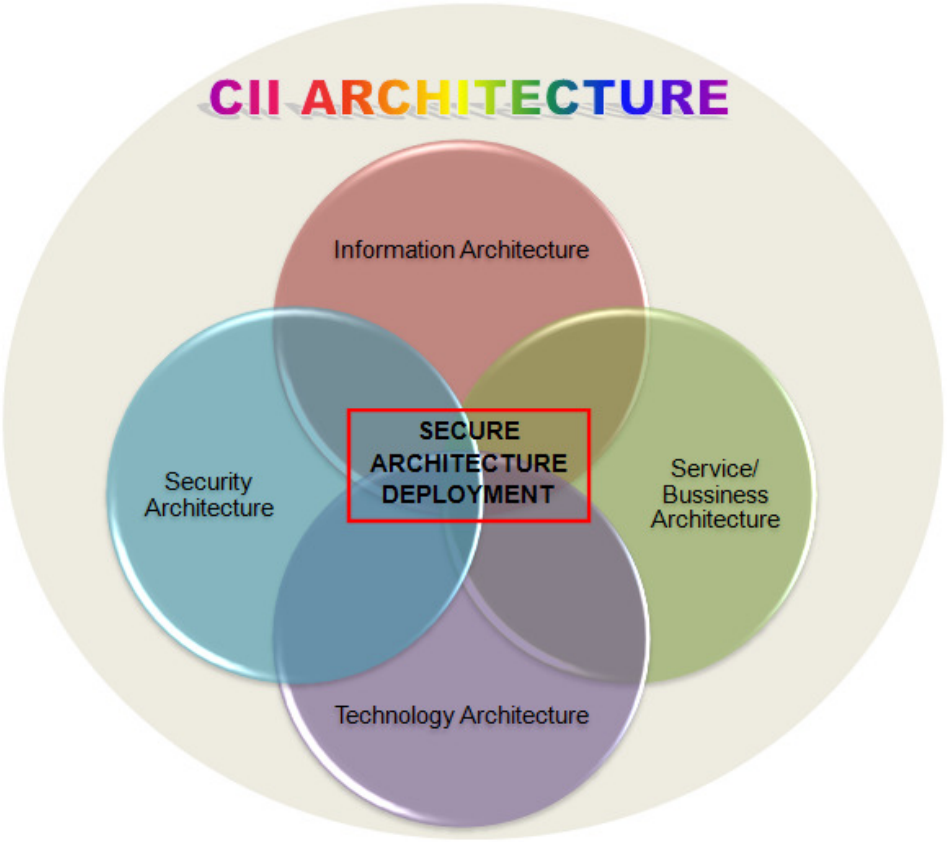

Figure 25: Secure and Resilient Architecture Deployment

9.3.4 **Best Practices**

(a) There should be secure and resilient architecture deployment plan in the IS policy specific to the CIIs needs and functions.

(b) Network architecture must incorporate security as a key design element.

(c) The overall architecture comprising of IT systems, products along with their selection and implementing conditions should be fully

analysed and vetted keeping in view the Information security of the CIIs.

(d) Architecture selection should strike a balance between security and business requirements.

(e) Automated upgrades and log monitoring should also be the part of secure architecture deployment.

(f) Testing and evaluation of Industrial Control, automation products and SCADA should be done before deploying in the architecture of the CIIs, keeping in mind the information security.

(g) Hardening of all the IT systems and products should also be covered under secure architecture deployment.

(h) Proper demarcation of MZ and DMZ from the internal network, designing of VLANs, maintenance of intranet, hardening and monitoring remote services, placement of perimeter protection devices, deployment of security products/solutions (like PKI, VPN, Cryptography etc.) should be considered while designing the secure architecture of the CIIs.

(i) Architecture should be easily adaptable and upgradable in tune with the rapid change in technology and information security trends.

(j) Architecture should be designed, considering security of deployed information systems through monitoring and analysis, regular audits and pentest which will help the systems to be resilient to cyber attacks.

(k) Critical communication systems and their communication channels should be protected to avoid eavesdropping which can be done by using SSL or https in URL.

10 Reporting and Accountability (RA)

10.1 RA 1: Mechanism for threat reporting to Govt. Agencies

10.1.1 Two-way exchange of information between CIIs and Government agencies regarding possible cyber threat or post attack analysis is essential. CIIs must always maintain strong communication channels with government agencies so as to get early information regarding emerging threats. This should include active participation of the CIIs in workshops, training or seminars conducted from time to time by government agencies.

10.1.2 Absence of proper feedback mechanism between the CIIs and government agencies can create a serious gap in the process of protection of critical assets of the country as separate islands cannot provide an overall, holistic view of the threat landscape. Neither the government will be able to take the holistic view of the seriousness and impact of the threats looming over the CIIs of the country nor the CIIs will be in the position to receive the intelligence regarding the large scale or State sponsored threats targeting the CIIs.

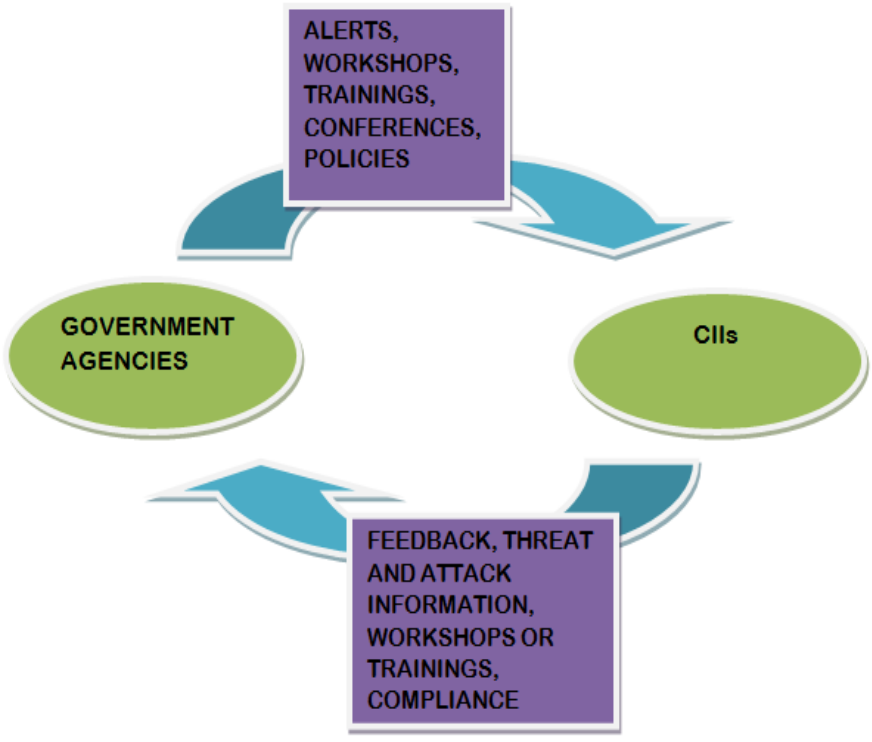

Figure 26: Feedback Mechanism

10.1.3 **Best Practices**

(a) Organisations must partner with government to devise a methodology for two way feedback mechanism.

(b) Proper Non Disclosure Agreement should be signed by the employees of the organisation under CII not to disclose the classified information received from the government in a process of feedback mechanism.

(c) Organisations should send their senior management for workshops, seminars and trainings regarding the protection of CII organised by the government from time to time.

(d) For any threat incident or intrusion in CII, government agencies should be taken into loop for their information and further actions.

(e) CIIs on receiving the information regarding the threat incident by the government agencies should ensure the compliance.

(f) Any advisories or feedback regarding the mock drills or penetration testing by the empanelled agencies by the government should be communicated to the government.

(g) Any major cyber incident reported in the CII should be immediately notified to the government agencies through the feedback channel without any delay.

(h) Policy making process regarding the protection of the CII by the government can be helped by suggesting appropriate suggestions or feedbacks through this feedback mechanism.

(i) CIIs should hold appropriate trainings or workshops relating to the security of their respective CIIs.

10.2 RA 2 : Periodic Audit and Vulnerability assessment

10.2.1 Everyday new attack trends are emerging in the field and the systems are being compromised or incapacitated. This increases the need to call for a periodic audit and vulnerability assessment.

10.2.2 Securing the Critical Information Infrastructure makes constant vigilance and review a necessary practice for the Organisations. The very dynamic nature of the digital world mandates that the underlying technology, policies, procedures and mechanisms put in place to secure the Information Infrastructure be periodically reviewed to validate their continued effectiveness.

10.2.3 A security audit and vulnerability assessment involves examination and evaluation of networks and other cyber/digital resources against the established security norms and best-practices to identify vulnerabilities, unnecessary exposures and subsequent risks. And then provide security recommendations.

Figure 27: Periodic Audit and Vulnerability Assessment

10.2.4 **Best Practices**

(a) A security assessment and audit policy may be devised.

(b) A comprehensive exercise to identify, prioritize before formulating an assessment schedule is required for vulnerability assessment and audit.

(c) A security culture is needed to evolve through awareness, trainings, audits, sanctions and sensitivity of employees to reduce vulnerability to its minimum level.

(d) Audit may include system information and log documentation and may recommend an assessment implementation plan to resolve vulnerabilities present if any, and to tackle upcoming threats.

(e) 'Security assessment and audit policy' and assessment implementation plan should apply to all the equipment, devices, softwares etc. engaged in critical services or deal/handle with critical information.

(f) Violations of established policies, procedures, programs or plans should be considered as a security breach and sanctions may be imposed as per norms of the organization.

10.3 RA 3: Compliance of security Recommendation

10.3.1 In accordance to the Information Security Policy and compliance of Security recommendations must be ensured by CISO and the allied departments or divisions.

10.3.2 Compliance of security Recommendations can be achieved through adequate planning and identification of requirements in accordance with the ascertain applicable laws and security standards. It's a huge task that includes risk analysis, findings and recommendations.

10.3.3 **Best Practices**

(a) A compliance committee may be formed for development of compliance policy, procedure and program considering risk analysis, and its effective implementation.

(b) A mechanism should be devised for periodic reporting of the compliance to the head of organisation through CISO.

(c) Review and monitoring of security recommendation should be there.

(d) Standard disciplinary/compliance guidelines may be developed and publicised among employees for their awareness and compliance assurance.

(e) Alongwith reporting an enquiry/investigation may also be initiated for non-compliance of security recommendation.

(f) Compliance of Security Recommendation may also be a part of organisation's Information Security Policy.

(g) Critical rule violations should be escalated and reported immediately.

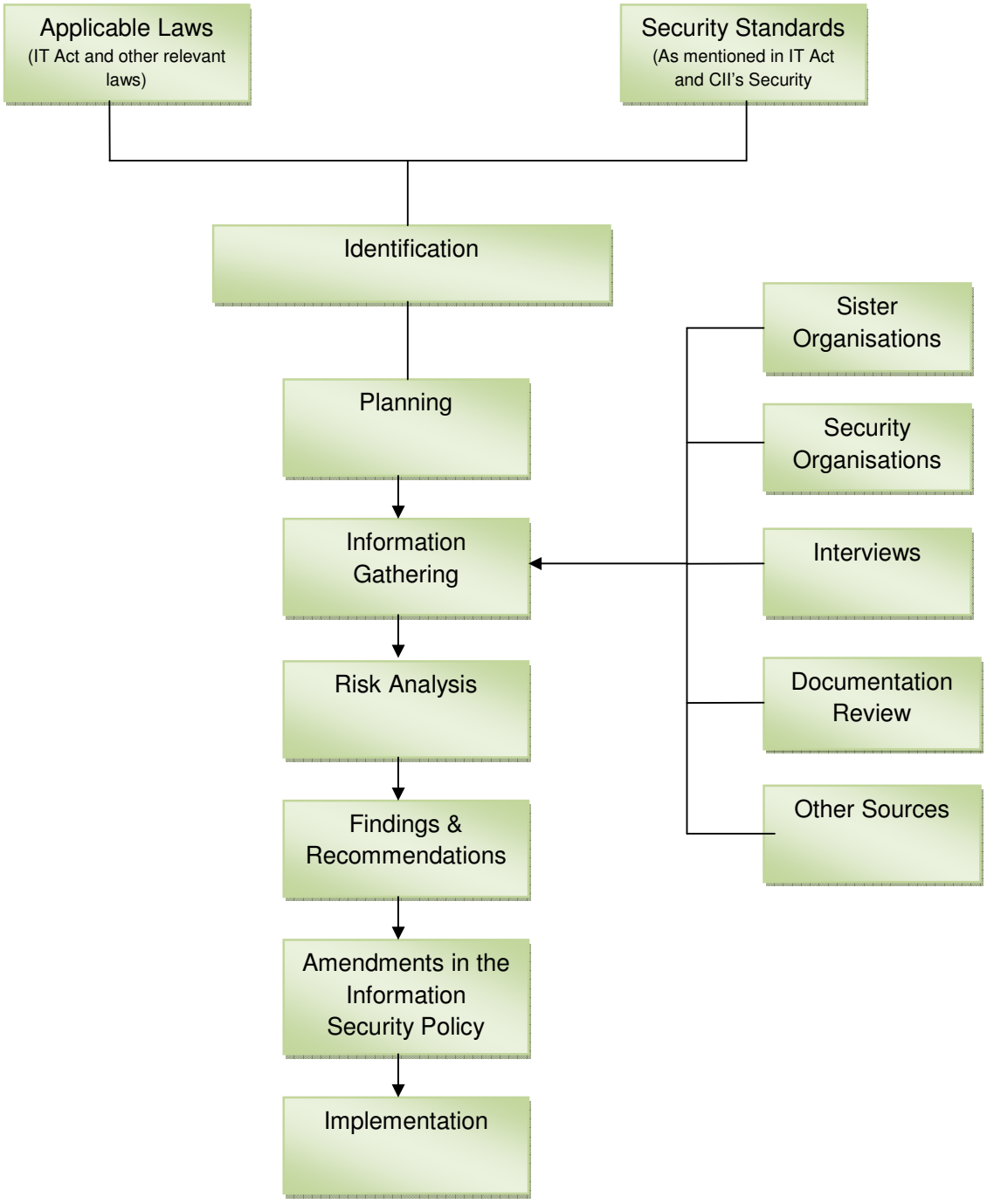

Figure 28: Compliance with Security Recommendation

11 Conclusion

11.1.1 Critical Information Infrastructure, by definition, is the backbone infrastructure supporting our National Security and Growth. This infrastructure is spread across multiple (Energy, Power, Finance etc) sectors and domains (Government, PSU, Indian Private entities, etc)

11.1.2 This document is meant to be an aid for Critical Information Infrastructure entities in their planning and approach to protecting their assets.

11.1.3 The document by no means claims to cover each and every aspect across all critical infrastructures. However, the document does aim to give serious practitioners charged with the responsibility of analyzing their organizational CII the basic tools and approaches to identifying the minimum set of controls and required to be put in place.

11.1.4 The document is very much a work in progress and needs to be updated on a regular basis, incorporating feedback and learning received from the multiple constituents of our Critical Information Infrastructure.

Designed & Printed by : NCIIPC, New Delhi