



Indian Manual for Cyber Security in Power Systems

Table of Contents

1. Abbreviations	2
2. Acknowledgements.....	3
3. Introduction and Scope.....	4
4. Threats and Attacks on Smart Grids	5
5. Mandatory Requirements (MR)	6
A) Security Control – Organisation	6
B) Security Control – System Protection	16
C) Security Control – Information Protection	26
D) Security Control – Audits, Assessments, Certification and Testing	27
E) Security Control – Personnel and Training	29
F) Security Control – Physical Security	30
G) Security Control – Operations.....	31
6. References	36

1. Abbreviations

The following abbreviations are used in this Manual:

Abbreviation	Full-Form	Abbreviation	Full-Form
ISGF	India Smart Grid Forum	IDS	Intrusion Detection Systems
NCIIPC	National Critical Information Infrastructure Protection Center	CA	Certification Authority
IT	Information Technology	LAN	Local Area Network
OT	Operation Technology	VLAN	Virtual Local Area Network
NERC	North American Electric Reliability Corporation	DMZ	De-Militarised Zone
CIP	Critical Information Protection	ICS	Industrial Control Systems
OEM	Original Equipment Manufacturer	SCADA	Supervisory Control and Data Acquisition
MR	Mandatory Requirement	VPN	Virtual Private Network
CISO	Chief Information Security Officer	SIEM	Security Information and Event Management
ISMS	Information Security Management System	RBAC	Role Based Access Control
BCP	Business Continuity Plan	HIPS	Host Intrusion Perversion System
ICT	Information and Communication Technologies	NAC	Network Access Control
ISD	Information Security Department	AD	Active Directory
SoD	Segregation of Duties	CDA	Critical Digital Assets
HR	Human Resource	VTR	Vulnerability, Threat, Risk
CII	Critical Information Infrastructure	PT	Penetration Testing
RRoI	Risk-based Return on Investment	NDA	Non-Disclosure Agreement
ESP	Electronic Security Perimeter	SLA	Service Level Agreements
EAP	Electronic Access Point	COTS	Commercial off-the Shelf
BPCS	Basic Process Control System	DR	Disaster Recovery
SIS	Safety Instrumented System	DC	Data Center
IPS	Intrusion Prevention Systems	RTO	Recovery Time Objective
SOP	Standard Operating Procedure	RPO	Recovery Point Objective

2. Acknowledgements

This manual is prepared by India Smart Grid Forum (Working Group 10 on Cyber Security) in coordination with National Critical Information Infrastructure Protection Center (NCIIPC). Following organisations contributed for the preparation of this Manual:

1. National Thermal Power Corporation (Mr R Sarangapani)
2. Tata Power Delhi Distribution Limited (Ms Satya Gupta)
3. Larsen & Toubro (Mr Abraham Samson & Ms Pallavi Mhatre)
4. Huawei (Dr Debu Nayak)
5. Schneider Electric (Mr Sandeep Pathak)
6. National Critical Information Infrastructure Protection Center (Mr Sachin Burman)
7. Microsoft (Mr Manish Tiwari)
8. Veermata Jijabai Technological Institute (Prof Faruk Kazi)
9. CESC, Kolkata (Mr Sumit Poddar and Ms Soma Basu)
10. Institute for Defence Studies and Analyses (Mr Munish Sharma)
11. Mr Arun Mane (in individual capacity)
12. ISGF (Mr Reji Kumar Pillai, Dr Shailendra Fuloria, Mr Samir Chaudhury, Mr Hem Thukral & Mr Sushant Chopra)

3. Introduction and Scope

In the current scenario in India, many directives and guidelines exist for cyber security. However, there are no guidelines for power systems-specific cyber security. The North American Electric Reliability Corporation (NERC) Critical Information Protection (CIP) Standards are generally followed by Utilities in the USA and several other countries. However, Indian utilities are at the threshold of adopting communications, automation and IT systems for their power systems and NERC CIP Version 5 is way beyond their preparedness. This prevents us from adopting such standards for India.

This Manual on cyber security for power systems in India will provide actionable inputs to the stakeholders in the power sector. This Manual is applicable to the following stakeholders:

- Generation Companies
- Transmission Companies
- Distribution Companies
- Load Dispatch Centers
- Equipment Manufacturers
- IT Hardware and Software OEMs
- System Integrators
- Service Providers (including communication system providers and agencies implementing microgrids)

4. Threats and Attacks on Smart Grids

With the superposition of the information infrastructure over the electrical infrastructure, confidentiality, integrity, accountability and denial of service have become critically important in today's scenario. Recent attacks on the industrial control systems have shown that there is an urgent need for building resilience and robustness into the electricity grid.

Protection of the critical infrastructure (encompassing energy, transportation, banking and finance, communication and IT, defence, space, law enforcement, sensitive government organisations, critical manufacturing, e-governance etc.) is the primary objective of any nation and the power sector assumes top priority. With this convergence of the electrical technologies, communication technologies, information technologies and automation technologies in a smart grid, security of industrial control systems has become extremely important. The security of the information infrastructure directly decides the reliability of the power system infrastructure.

Before the advent of smart grids, security of industrial control systems was limited to prevention of online attacks. However, today's scenario mandates protection of critical cyber assets that include (but are not limited to) substations and control centres of the electric utilities (Generation, Transmission and Distribution), and load dispatch centres. Hence 'cyber- physical security' completely signifies the need of the hour. In this Manual, we have used 'cyber security' and 'cyber-physical security' synonymously.

In today's scenario of regular attacks on electric utilities, it is very important to have defence in depth in the utility's day to day functioning. That is, a layered security approach will strengthen its cyber security posture as illustrated in the diagram below. This provides a redundancy in the system with respect to cyber security.

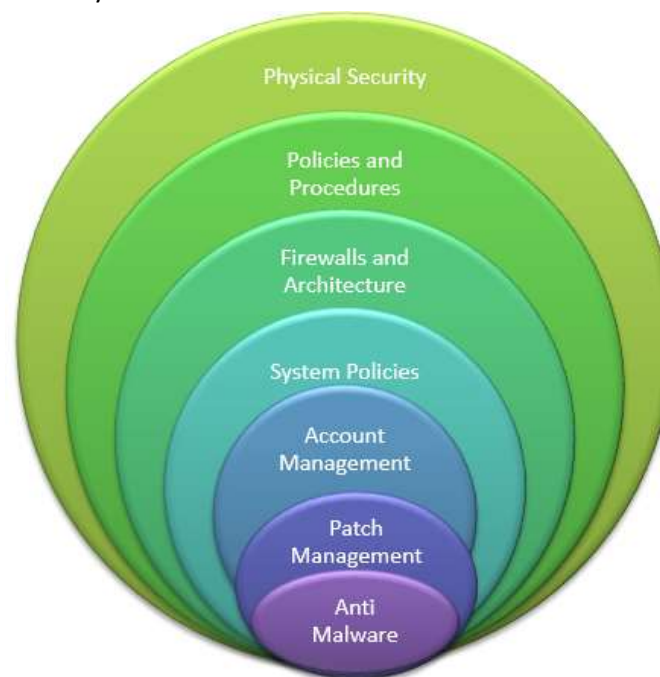


Figure 1: Defense In-Depth Approach for Cyber Security

This approach consists of people, processes and technology. At the outset there is physical security, procedures, policies and firewalls. Then we have system policies, account management, patch management and anti-malware as the central part.

5. Mandatory Requirements (MR)

In this Manual, the term 'Organisation' has been defined as an electricity generation company, transmission company, distribution company or a load dispatch center. Also, 'IT system' may need to be treated as 'IT and OT (Operational technology) systems' wherever applicable.

This section describes the Mandatory Requirements (MR) that the Organisation needs to adhere with.

A) Security Control – Organisation

MR 1 – Appointment of CISO

A Chief Information Security Officer (CISO) is a senior-level officer within the Organisation responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the Organisation to reduce risk. The CISO must understand the importance of establishing cyber security controls and the implications of not having them.

Requirements:

The Chief Information Security Officer (CISO) must:

1. Seek top management support and direction for implementing information security measures in the Organisation
2. Identify information security goals and objectives consistent with Organisation business need/objectives of the Organisation
3. Define the scope and boundaries of the information security program
4. Understand legal and regulatory requirements
5. Define information security implementation strategies
6. Estimate budget and resources required to develop and maintain a resilient and robust cyber system
7. Plan and establish Organisation-wide Information security Management System (ISMS) in accordance with ISO/IEC 27001 Standard, directions and advice of National Critical Information Infrastructure Protection Centre (NCIIPC) and other relevant security standards
8. Define a risk management framework
9. Define information security measurement metrics and other key performance indicators
10. Obtain approval for the information security policies, procedures, plans, guidelines and budget and resources from the senior management
11. Identify information security policies, standards, procedures, plans, guidelines and processes
12. Define a formal process for creating, documenting, reviewing, updating, and implementing security policies, procedures, plans, guidelines and processes
13. Define an information security policy
14. Define a policy for identification and classification of information and information assets
15. Lead and coordinate the development of Organisation specific information security policies, procedures, guideline and processes in consultation with various stake holders including NCIIPC
16. Assist in developing, maintaining, reviewing and improving strategic Organisation wide information security and risk management plans
17. Disseminate information security policies, procedures and guidelines to all concerned personnel including management, employees, contractors, sub-contractors and other stakeholders
18. Enforce and oversee implementation of approved information security policies, procedures, plans, guidelines and ISMS etc.

19. Integrate information security procedures with Organisation's business processes
20. Ensure that information security considerations are integrated with IT system planning, development & acquisition life cycle
21. Periodically evaluate and review effectiveness of information security policies, procedures, standards, plans, guidelines and processes etc.
22. Issue alerts and advisories with respect to new vulnerabilities/threats to all concerned personnel, departments, and inform other related organisations
23. Perform risk assessment steps such as:
 - (a) identify and prepare inventory of assets within the scope of information security plan
 - (b) identify and document threats to those assets
 - (c) perform vulnerability analysis
 - (d) perform penetration testing
 - (e) perform impact analysis
 - (f) evaluate level of risk
 - (g) determine acceptability or treatment of risk based on risk acceptance criteria
24. Perform risk treatment such as:
 - (a) identify appropriate security controls for treatment of risk
 - (b) take approval from senior management for implementation of identified security controls
 - (c) oversee implementation of information security controls
 - (d) evaluate residual risk
 - (e) take approval from senior management for residual risk
25. Implement automated and continuous monitoring of security incidents
26. Maintain a record of information security incidents and breaches
27. Take remedial action to mitigate and reduce/diminish the impact of information security incidents and breaches
28. Share information related to critical information security incidents and breaches with NCIIPC
29. Ensure compliance with legal and regulatory requirements for information security
30. Raise information security awareness among management, employees, contractors, sub-contractors and other stakeholders
31. Provide role-based training on information security to the workforce
32. Evaluate effectiveness of training & awareness programs and continuously upgrade them.
33. Coordinate and ensure implementation of a Business Continuity Plan (BCP)
34. Periodically conduct mock drills to evaluate the effectiveness of the Business Continuity Plan
35. Define and implement a change management plan for both, change in information systems and the change in Information Security Management System (ISMS) itself
36. Ensure compliance of information security by contractors/suppliers/sub-contractors etc.
37. Ensure that before issuing a No Objection Certificate to the employee who has resigned or has been terminated or is leaving the Organisation, all equipment have been taken back and all his accounts either have been deleted or their passwords have been changed
38. Maintain the Information and Communication Technologies (ICT) as a register containing details of asset, its owner and its security classification
39. Ensure that all storage media, when no longer required, are disposed securely and safely as per the procedures established by the Organisation
40. Ensure safety and security of portable computing devices/storage media when they are taken outside the Organisation
41. Ensure all information systems with the Organisation are adequately patched and updated
42. Evaluate compliance with respect to legal and regulatory requirements for information security
43. Evaluate compliance with respect to Organisation-specific information security policies, procedures, plans, standards, guidelines and directives & advice of NCIIPC
44. Perform information security audit at least annually

45. Prepare an information security audit report along with recommendations for improving information security and present to senior management
46. Ensure closure of reported audit observations
47. Send a copy of the audit report periodically to NCIIPC

MR 2 - Creation of Information Security Department (ISD)

Information Security Department (ISD) is an integral part of an Organisation. Every Organisation must house an independent and competent ISD. This department must be accountable for safeguarding the security and protection of the critical IT assets of the Organisation. The ISD is involved in 4 broad activities viz. Planning, Development, Management and Oversight of the security posture of the Organisation.

The Organisation may employ experts in the ISD that work on securing its cyberspace. The ISD also performs threat, risk and vulnerability assessment and develops solutions for ensuring sustained cyber security of the Organisation. The ISD of the Organisation must function continuously **on a 24x7x365 basis**.

The ISD should have a hierarchical structure and should report to CISO who functionally reports to the head of the Organisation in order to make sure that the senior management is well informed and involved.

Requirements:

The ISD must:

1. Formulate an annual work plan in order to realise the security objectives of the Organisation
2. Specify the scope of the information security program and its implementation strategy
3. Revise and update the existing plans to stay secure while incorporating new technologies
4. Estimate the monetary and logistics requirements and to ensure that there are sufficient funds for the planning, maintenance and management of information security
5. Outline the 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
6. Coordinate the development of Organisation-specific information security policies, procedures, plans, guidelines and processes in consultation with various stake holders including NCIIPC
7. Establish a formal process for creating, documenting, reviewing, updating and implementing security policies
8. Design and develop an information and asset classification policy
9. Circulate information security procedures, plans, policies and guidelines to all the concerned departments
10. Manage incidents, conduct risk assessments & security awareness training
11. Incorporate information security processes in the Organisation's business processes
12. Define roles and responsibilities of the key personnel of the Organisation for ensuring implementation of policies and guidelines of information security
13. Implement Segregation of Duties (SoD) to reduce conflicts of duties and interests
14. Periodically evaluate and review the effectiveness of information security policies, procedures, plans, standards, guidelines and processes
15. Keep a record of information security incidents and breaches
16. Perform internal security audits and coordinate for external audit. Also implement mock drills on a regular basis and after major reconfigurations or updations
17. Ensure Human Resource (HR) policies adequately incorporate information security guidelines.
18. Develop policies or procedures for disposal of critical digital assets

19. Ensure that all information systems within the Organisation are adequately patched and updated
20. Monitor compliance to the Organisation's security policies, procedures, plans, processes, standards, guidelines etc.
21. Evaluate compliance with respect to legal and regulatory requirements for information security.
22. Perform information security audit at least annually
23. Ensure that the respective departments provide the necessary inputs to the ISD at every stage to ensure continuous, comprehensive protection of the Organisation's cyber space

MR 3 - Framework for Identification of Critical Information Infrastructure (CII)

Each Organisation has a number of critical cyber assets which enable its seamless operation. It is the responsibility of the Organisation to identify and classify the Critical Information Infrastructure (CII) present in their systems on the basis of (functionality, criticality scale, degree of complementarities political, economic, social and strategic values, degree of dependence, sensitivity etc.).

Requirements:

The Organisation may use the following parameters for identification of Critical Information Infrastructure:

1. **Functionality:** It is an active concept which includes a 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.
2. **Criticality Scale:** It is a rule for evaluating the criticality of various cyber assets in the Organisation. It can be a compound approach which can involve a number of factors such as the availability, delivery, access and consummation of essential services.
3. **Degree of Complementarities:** It is a very important characteristic as it takes into account that how various systems in an Organisation are complementing each other i.e. their dependency over one another. For example, number of affected parallel systems if a particular system fails.
4. **Political, Economic, Social and Strategic Values:** It comprises of the values that are important for the fraternity, integrity, unity, political stability and economic prosperity of the nation.
5. **Time Duration:** It is also a very important factor in deciding critical information infrastructure. It is important because not all systems may be critical at all times and other all circumstances and there may be time slots in which they are critical or not.

This critical information identification is a dynamic process and must be reviewed periodically atleast once a year by all stakeholders to identify changes in functional dependencies, protocols and technologies.

MR 4 - Listing of Dependencies

The complex interaction and information exchange among various functions of critical infrastructure lead to interdependencies which may be inter-Organisational (Horizontal) or intra-Organisational (Vertical) in nature. The Organisation must not view its CII in isolation, but in conjunction to all interdependencies.

Requirements:

1. The Organisation should identify its core business processes.
2. The Organisation should identify all horizontal (both incoming and outgoing) & vertical dependencies.
3. The Organisation should review these dependencies on a regular basis, atleast once in 6 months.
4. The Organisation should apply appropriate security controls to make sure that the dependencies do not increase the attack surface.
5. The Organisation should list the dependencies for which security controls have not been implemented and subsequently take sign off from the senior management.

MR 5 – Coordination with NCIIPC

The National Critical Information Infrastructure Protection Centre (NCIIPC) is the national nodal agency designated under section 70A of the IT Act for all measures to protect the critical information infrastructure of India. In accordance with its mandate, to protect the critical information infrastructure against cyber terrorism, cyber warfare and other threats, and to maintain situational awareness, NCIIPC would need periodical information from all the entities operating the critical information infrastructure.

Requirements:

1. The Organisation should periodically share the following information with NCIIPC:
 - a. Logs of successful attacking IPs and compromised accounts
 - b. Critical incident response reports
 - c. Targeted malware samples
 - d. Information security periodic surveillance audit report
2. The Organisation would receive advisories, guidelines and directives from NCIIPC and in turn should take action

MR 6 - Formulation of Risk-Based Cyber Security Policy

In the power sector, cyber space security is the protection of data, systems, and infrastructure vital for the Organisation's operation and to stability and livelihood of people associated with the Organisation. Organisations are increasingly depending on Information and Communication Technology (ICT). Along with the growing economic value of ICT for Organisations, threats to it are all growing because of the increased connectivity. A secure Organisation can be confident that it is better positioned for opportunity and growth. To ensure a secure environment, a strategy to protect the Organisation's cyber space is required for managing risks and boosting resilience. Organisations must build and implement a risk based cyber security policy with clear priorities, minimum ICT security baseline with threat and vulnerability information, build incident response capabilities and create awareness, educating and training opportunities.

Establishing an Organisation's risk-based cyber security policy is an important element in maintaining an Organisation's resilience to disruptions while mapping a path to future. By creating a structured approach, thinking holistically about threats and vulnerabilities, and deploying strong practices to detect, mitigate, and communicate threats, the Organisation can protect its stakeholders and safeguard its resources.

Requirements:

1. The Organisation should formulate a cyber security policy
2. The Organisation should develop a clear structure for identifying, analysing, and evaluating the risks to be managed
3. The Organisation should assess threats to the Organisation's cyber security using threat modelling
4. The Organisation should document and review risk acceptance and exceptions
5. The Organisation should conduct assessment, management and monitoring of risk as an on-going process
6. The Organisation should establish minimum security baselines
7. The Organisation should define clear roles and responsibilities for the personnel supporting a security baseline

MR 7 - Formulation of Information and Document Management Policy

To comply with the sections 7 (Retention of Electronic Records) and 43A (Compensation for failure to protect data) of IT Act, 2008, the Organisations should formulate a cyber system information (including storage, transit, and use) and document management policy.

The document management policy should provide guidance for handling, storing, and managing documents so as to ensure that they remain accessible, authentic, and reliable as long as needed, transferring when required, and disposing at the end of their scheduled life cycle.

Requirements:

1. The Organisation may classify all documents as 'Top Secret', 'Confidential', 'Restricted' and 'Public'. A document which has been classified as 'Top Secret' is to be treated as the most critical document in the Organisation. Also, the appropriate documents must be stored in a secure manner.
2. The Organisation should take action to prevent the unauthorized retrieval of information from workstations, laptops, tablets, smart phones etc. For USB drives, vendor identification and/or product identification may be employed.
3. Prior to the disposal of cyber assets, the Organisation should take necessary actions to prevent unauthorized retrieval of information.
4. The Organisation should manage information and documents in accordance with IT Act, 2008 (Amendment).
5. The Organisation should ensure that Non-Disclosure Agreements (NDAs) are signed by both internal staff and external agencies (while dealing with external agencies).

MR 8 - Conversion of Cyber Risk to Financial risk

In view of increasing need of integration of IT and OT systems, unified and interoperable security solutions have become essential for seamless operation of varied systems using different communication media and topologies. 'Cyber Risk' is defined as any risk of financial loss, disruption of services or damage to the reputation of the Organisation from a failure of its information and communication technology systems.

Conversion of cyber risk into financial risks having a common denominator in Indian rupees (INR) helps in defining acceptable limits, allowing monitoring and enabling mitigation of risk. These financial risks are assessed from the perspectives of its *Impact and Likelihood of occurrence*.

$$\text{Significance} \times \text{Likelihood} = \text{Inherent Value of Risk (Probability)}$$

In view of the evolving and emergent nature of the vulnerabilities and risks facing the power sector operations, appropriate risk management frameworks and security blueprints need to be implemented to secure the Organisation against deliberate attacks, equipment failures, inadvertent errors or natural disasters.

Requirements

1. The Organisation may consider the following for determining the cost of the compromise:
 - Value of data lost
 - Brand damage
 - Shareholder value
 - Cost of incident response and recovery
 - Fines, penalties, and potential litigation for damages
2. Based on the estimated value derived from the above parameters, the risks may be ranked according to their significance and likelihood of occurrence

MR 9 - Calculation of Residual Risk

Residual risk is a risk that remains after all efforts have been made to mitigate or eliminate risks associated with a business process or investment. After a risk assessment, a residual risk may be known but not completely controllable, or, in some cases, it may not be known. Hence, the residual risk is calculated or assumed by the Organisation.

The effectiveness of security controls for mitigating the identified risks will enable the Organisation to measure its residual risk exposure. All identified risks need to be mapped to the existing security controls/practices. The strength of the security control can be assessed for its effectiveness to mitigate the identified risks by carrying out process walk through, observation, exception monitoring, etc. The security controls need to be mapped at the likelihood stage to ensure that risk vulnerability is addressed.

All risks and the existing security controls are measured to get a residual risk exposure.

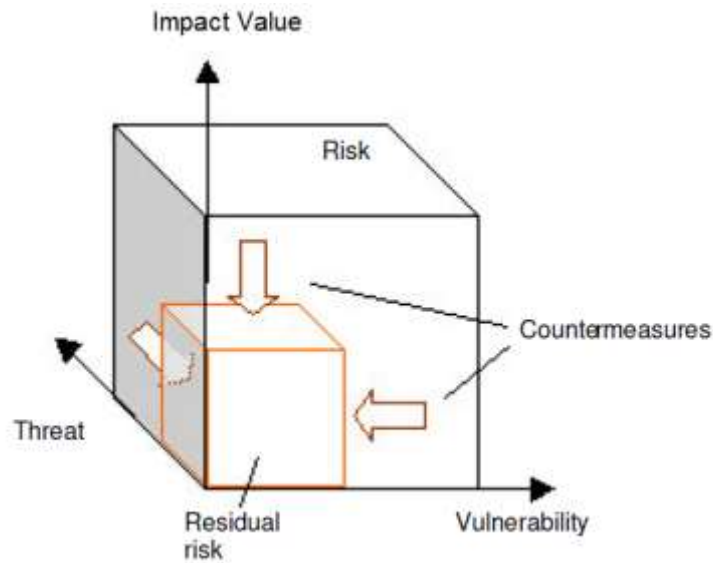


Figure 2: Illustration of residual risk

As depicted from the above figure, risks that remain after applying countermeasures are called “residual risks”. Residual risks have to be considered by the management and be accepted or rejected (in the latter case the risks have to be treated again). In some cases, the cost required to mitigate the residual risk may be very high as compared to the financial impact of that risk or the residual risk may be of least criticality. Hence the Organisation may decide not to apply security controls for such cases.

Requirements:

1. The Organisation should calculate the net bypass rate for all security solutions which is the rate at which an attack results in actual damage to the Organisation
2. The Organisation should calculate the total damage from all possible risks and the baseline scenario (if no security controls were in place) using the below figure. This is the damage sustained in a given time period for each incident type and can be approximated by assigning an average cost per incident and multiplying by the number of incidents
3. The Organisation should calculate the residual risk using the baseline scenario and total damages from all incidents
4. The Organisation should calculate the Risk-based Return on Investment (RRoI) using the residual risk and implementation cost for all countermeasures

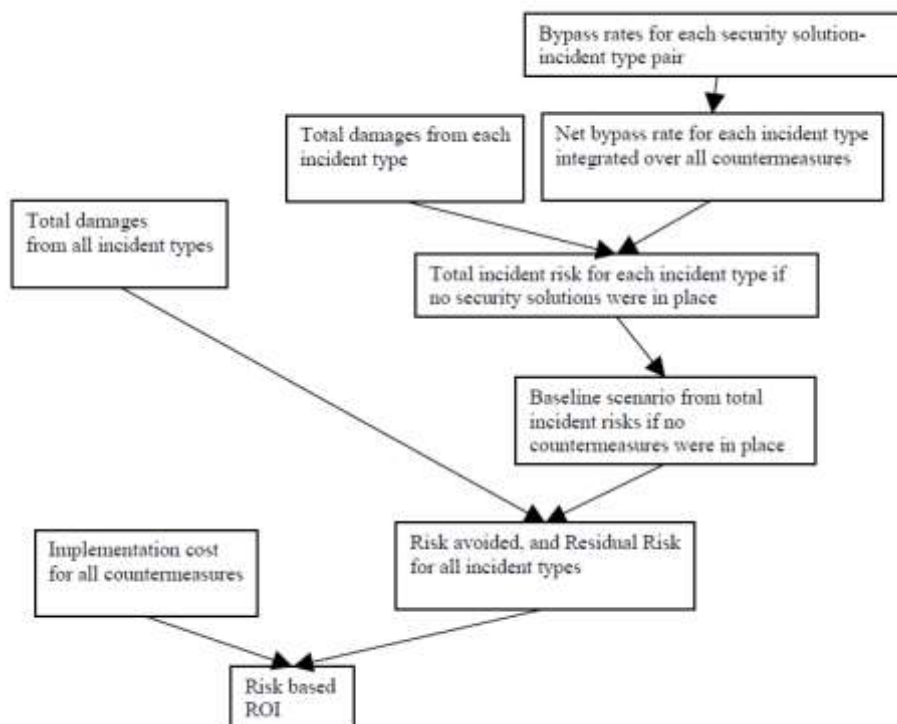


Figure 3: Outline of the framework to calculate residual risk

MR 10 – Cyber Security for Budgetary Allocation

Often, many security controls are not implemented due to lack of funds and/or resources. The prime reason for this is the difficulty to show a return on investment made on cyber security. The senior management of the Organisation must understand the implications of not implementing security controls, that is, their systems being attacked or misused, financial losses, poor quality of life to the citizens etc.

It is a common but wrong practice that dedicated funds are not allocated for cyber security. This often leads inadequate allocation of funds and hence insufficient implementation of security controls thus leading to limited planning and development. The Organisation can secure its cyber space in a more comprehensive manner if funds are allocated for cyber security in a dedicated manner.

Requirements:

1. The Organisation to separately allocate funds for cyber security
2. The CISO to be involved in the process of allocation of funds for cyber security
3. The Organisation to set aside a suitable portion of the total budget allocated to cyber security for capacity building exercises (including but not limited to) conferences, workshops, seminars, practical exercises such as mock attacks et.

MR 11 – Exception Management

At times, it is not possible to completely adhere to all the clauses mentioned in the cyber security policies, plans, procedures, guidelines, standards, processes etc. due to manpower and budgetary constraints and/or inconsistencies in these directives. Hence it is extremely important to document such exceptions and subsequently take signoff from the senior management.

Requirements:

1. The Organisation should document any non-compliance within a stipulated time frame as deemed fit by the Organisation
2. The Organisation should include a valid reason in the documentation for not complying with cyber security policies, plans, procedures, guidelines, standards, processes etc.
3. The CISO should approve the document mentioning non-compliance before submitting to the senior management
4. The Organisation should review this document (that contains exceptions) regularly in order to make sure that the exceptions hold valid and true over the time

MR 12 – Critical Asset Inventory Control

This is meant to correlate and track all physical and virtual assets owned by the Organisation. Asset inventory provides information that is important for day to day system management, 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. This control is essential to track unauthorized hardware or software. With this control in place, every asset is assigned and subsequently issued to the employees/departments.

This control is also essential for formalising the access control list of the systems (software and hardware) used in the operation of critical information infrastructure of the Organisation.

Requirements:

1. The Organisation should identify and allocate a dedicated team for asset and inventory management, with clear roles and responsibilities
2. The entire hardware inventory should be clearly marked with uniquely identifying marks (e.g. serial no., model no., asset no.) for devices like servers, printers, laptops, desktops etc.
3. Similarly, software inventories should be made listing the product name, version, serial number, the device on which it is installed etc.
4. Periodic review of the hardware and software inventory should be ensured
5. Movement of equipment/digital media etc. from/to the Organisation should be adequately controlled
6. For discarding/replacing/auctioning of the particular asset, proper authorization from the management should be accorded and necessary updates be done in the inventory
7. 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

B) Security Control – System Protection

MR 13 - Protection of Portable/Wireless/Removable Media

This security control defines a formal procedure to prevent the use of unnecessary logical and physical input/output ports used for network connectivity, console commands, or removable media. It is required to minimize the attack surface through disabling or limiting access to unnecessary physical and logical access ports and services.

Requirements:

1. The Organisation to maintain documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage
2. Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Organisation
3. If a device has no provision for disabling or restricting logical ports, then those ports that are open, should be deemed needed
4. The Organisation to maintain documentation of the need for all enabled ports on all applicable cyber assets and electronic access points, individually or by group
5. The Organisation to list the listening ports on the cyber assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports, or; configuration files of host based firewalls or other device level mechanisms that only allow needed ports and deny all others
6. The Organisation to identify portable, mobile and removable media via vendor identification and/or product identification methods

MR 14 – White/Black/Grey Listing

Automation solution systems now a days comprises of a wide range of equipment with wide variety of vulnerabilities and constantly evolving threats. This has resulted in constant evolution of tools and controls.

However, of the numerous solutions available for prevention of malware intrusions/attacks viz. network isolation techniques, portable storage media policies, intrusion detection/prevention solutions, whitelisting solutions, traditional anti-virus solutions etc., whitelisting has been discussed in this Mandatory Requirement.

If a malicious code is detected on an equipment, then the threat posed by that code must be mitigated. However, the traditional solution of using antivirus products to remove or quarantine the malicious code can be augmented through the use of whitelisting which will not allow the code to execute.

Further, whitelisting serves as another tool for ensuring the access controls between the network segments with an automation solution and between the automation solution and the external network/communication links by restricting the traffic flows between them through restrictions placed on the execution of the malicious software/code that tries to generate the prohibited traffic. Restrictions are generally defined by rules that whitelist and/or blacklist traffic based on a number of factors including source addresses, destination addresses, and content (e.g. deep packet inspection). Whitelisting/Blacklisting becomes important in the scenarios where other malware protection tools are not recommended for use in the offered automation solution for various reasons.

Requirements:

1. The Organisation should identify equipment susceptible to malware and document it. The automation solution provider shall be capable of identifying the equipment, part of the automation solution being provided, that are susceptible to malware intrusions and provide to asset owner proper documented plans and processes for addressing those risks. This malware document shall also include the corresponding documentation for the plans and processes related to whitelisting/blacklisting solution to malware attacks.

If whitelisting/blacklisting software is used, then the documentation shall clearly indicate the process for installing, updating and configuring the used software on all the relevant hardware platforms in the automation solution, with an intent as to how to ensure that the latest data, configuration and software patches are deployed.

Moreover, any equipment that has no updateable software and its executing code cannot be altered, then that equipment can be considered of having its own internal method of deterring malicious code.

2. Further, the automation solution provider should also provide the asset owner with the evidence that these plans and processes have been followed during all applicable stages of automation solution system engineering and commissioning. If the control system manufacturer/supplier is different from automation solution provider and control system manufacturer/supplier does not undertake the above exercise, then the automation solution provider is responsible for ensuring the above and other necessary activities related to whitelisting/blacklisting.
3. The Organisation should implement whitelisting/blacklisting. Whitelisting/Blacklisting can be implemented through any of the available methods viz. tools available with the operating system of the equipment or through the available whitelisting/blacklisting software. The automation solution provider is responsible to ensure that in the finally delivered automation solution, whitelisting/blacklisting has been configured as per the agreed procedures mentioned above. If a whitelisting/blacklisting software is used then the patches/updates for the same will be managed as per the procedures laid down under the Mandatory Requirement on Patch Management mentioned in this Manual.
4. On completion of implementation of whitelisting/blacklisting, the automation solution provider should provide the documentation specifying the following:
 - a) The state of implementation of whitelisting/blacklisting for use as malware protection mechanism
 - b) Clearly specifying the automation solution components on which it is technically possible to install/configure whitelisting/blacklisting with the applicable reasons for each component
 - c) The current configuration settings for whitelisting/blacklisting. If a software is used for whitelisting/blacklisting then the patches/updates/release of the software installed should also be furnished as a part such documentation
 - d) Any other features/functions/software (e.g. for isolating and reporting infections/malicious code) used to augment the whitelisting/blacklisting functionality and its necessary details as per the relevant sections of this Manual
5. Centralized anti-malware solution should be promoted to ease the configuration and deployment of the security policy regarding protection against malware, as well as to ease

its maintenance during the Critical Information Infrastructure (CII) lifetime, thus raising and maintaining the security level of the solution.

MR 15 – Electronic Security Perimeter (ESP)

The capabilities specified by this security control are used to ensure the use of access controlled routable protocol through an identified and documented Electronic Access Point (EAP) between network segments within the automation solution and between the automation solution and external networks/communication links.

Requirements:

1. All applicable CII connected to a network via an access controlled routable protocol shall reside within a defined ESP
 - This will enable the asset owner/service provider to have an identifiable process for identifying and documenting all network segments of the automation solution, how they are interconnected, which of them provide external access to the automation solution, and for designating each connection point (interface to/from a segment) as trusted or untrusted. Untrusted interfaces are those that allow connections with untrusted devices in other segments/systems.
 - This will also enable the asset owner/ service provider to have an identifiable process for protecting interfaces of the automation solution, that have been identified as untrusted, by network security devices or equivalent mechanisms, and for providing the information necessary to create security rules that are used to grant/deny access to Basic Process Control System (BPCS) ports and applications, with documented and maintained security rules. At a minimum, the following shall be protected:
 - 1) External interfaces
 - 2) Level 2/Level 3 interfaces (Depending on the automation solution, Level 2/Level 3 interfaces may be “External” interfaces.)
 - 3) Interfaces between the BPCS and the Safety Instrumented System (SIS)
 - 4) Interfaces connecting wired and wireless BPCS networks
 - 5) Interfaces connecting the BPCS to data warehouses (e.g. enterprise historians)
2. All External Routable Connectivity must be through an identified and documented Electronic Access Point (EAP)
 - This will enable the asset owner/service provider to have an identifiable process for reducing the attack surface of the automation solution, for limiting access to the listed interfaces/ports to authorized users, and for maintaining the hardened state of the automation solution.
 - Limiting the software applications and their associated communication access points, USB devices such as mass storage devices, and wireless communications capabilities to only those necessary to perform the functions of a device used in both normal and emergency operations reduces the number of avenues into the device for an attack. Identifying unnecessary and/or unauthorized access points (e.g. using network scanning tools) is one technique that can be used to discover unnecessary software programs.

Identifying network addresses that are unauthorized, for example using network scans, and removing them (e.g. by disconnecting the devices to which they are assigned) limits the source of passive and active attacks.

- Controlling access to physical configuration ports of devices, such as serial ports is intended to prevent or reduce the risk of having the network configuration (network devices) or the operation of other devices changed without proper authorization. Different methods for controlling access include installing a device in a locked cabinet, being able to physically lock the configuration port, or otherwise disabling use of the port when its use is not authorized (e.g. through a software lock).
 - Locking down network device ports (switches and routers) reduces the possibility that an unauthorized device will be able to connect to the network and launch attacks or sniff the network.
- Control system products may have already removed capabilities unused by them prior to or during installation, making it necessary for the service provider to ensure that they are added/enabled only if they are required and approved by the asset owner.
- Maintenance processes provide the possibility that previously hardened components of the automation solution are reset or reconfigured to lose some aspect of their hardening. Controlling these processes reduce this possibility.
3. The Organisation should ensure that inbound and outbound communications require access permissions, and it is able to detect known or suspected malicious communications for both inbound and outbound communications via Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)
 - Access controls protect network segments by restricting traffic flows between them by architectural and configuration considerations, such as firewall, data diode placement (architectural) and firewall rules (configuration). Restrictions are generally defined by rules that whitelist, blacklist and/or grey list traffic based on a number of factors including source addresses, destination addresses, and content (e.g. deep packet inspection).
 4. The Organisation should have one or more methods for hardening of devices within the ESP
 - This will enable the asset owner/ service provider to have an identifiable process for determining which Certification Authority (CA) certificates are installed and removing those that are not used/authorized. Limiting which CA certificates are installed to only those that are necessary to prevent authentication of unwanted, undesirable, or unnecessary applications.
 - This will enable the asset owner/service provider to have an identifiable process for handling vulnerabilities that affect the automation solution, including its related policies and procedures. These capabilities shall address:
 - 1) The handling of vulnerabilities newly discovered in the automation solution or in its related policies and procedures for which the service provider is responsible
 - 2) The handling of publically disclosed vulnerabilities affecting the automation solution
 - This will further enable the asset owner/service provider to have an identifiable process to get/provide to the asset owner, documentation that describes how to mitigate security weaknesses inherent in the design and/or implementation of communication protocols used in the automation solution that were known prior to

automation solution integration or are revealed during the tenure of maintenance activities.

5. The Organisation should use cryptography to ensure protection of data
 - This will enable the asset owner/service provider to have an identifiable process for ensuring that data used for the administration of network device is protected by encryption within the device and on communication links. Encryption used on communications links can be performed at the network layer, on the transport layer connection, or at the message level to protect the data “on the wire”.
 - Encryption within network devices is used to prevent attacks on the configuration by malicious software in the device (e.g. as a result of hacking). The use of encryption mechanisms that provide integrity protection should be considered, such as AES_GCM.
6. The Organisation should use mutual multi-factor authentication for administration of network devices and all interactive remote access sessions
 - This will enable the asset owner/ service provider to have an identifiable process for configuring network devices to use mutual authentication. Mutual authentication validates the identity of the user and the network device, and results in the ability of the network device to determine whether the user is authorized to access the device, and in the ability for the user to ensure the device is the intended device and is not being spoofed. Challenge/response, user password/device certificate, and Kerberos (RFC 1510), are examples of techniques used to provide mutual authentication.
7. The Organisation should physically or logically segregate the IT and OT networks
8. The Organisation should implement Virtual LANs (VLANs) to isolate different traffics which are using common transport channel
9. The Organisation should implement SCADA-aware threat detection and prevention devices. These devices detect and prevent exploits of Industrial Control Systems (ICS) vulnerabilities with SCADA IPS signatures
10. The Organisation should segregate its cyber space into zones and apply perimeter protection as per this Mandatory Requirement on Electronic Security Perimeter
11. The Organisation should create a De-Militarised Zone (DMZ) which separates the internal LAN from other untrusted networks. Typically, external-facing servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable. This provides an additional level of security to the LAN as it prevents the attackers from directly accessing internal servers and data via the internet. Any service that is being provided to the users is typically placed in the DMZ

MR 16 - Access Control (including Remote Access)

This MR addresses the requirement of a management process for controls in order to ensure effective and secure access control. These controls apply to local or remote access to system hardware or devices as well as remote access to the same. It also includes restrictions on the user access which has been covered in the MR on Account Management. For clarity, the same has been cross referred and not repeated.

Requirements:

1. The Organisation should perform the following:
 - a) All unused ports shall be disabled. There should be a clear documentation on the network ports that are used in the system
 - b) Mirror ports, if used, shall be clearly documented in terms of usage. These should be kept open only for the intended period of usage. Work permits shall be taken for such restricted usage
 - c) Laptops and mobiles shall not be allowed to be connected on the network devices. If absolutely necessary, special permissions should be taken from the CISO and the usage should be clearly documented along with the intended period of usage

NOTE: In many systems, laptops are used in lieu of engineer stations for modifying control logic, as they are handy and can save permanently installed hardware. Such devices are potential entry points of malicious code in the network and hence, must be avoided.

2. For the servers /workstations of the system, following controls should be enforced by the Organisation:
 - a) Access to USB ports shall be restricted for connection of keyboards , mouse & authorized storage devices
 - b) Network access measures shall follow the requirements stated in Mandatory Requirement (MR) on 'Account Management'
3. Wherever access to third party devices is provided, necessary rules shall be included in the firewall to :
 - a) Allow only desired ports (TCP ports) and disallow the rest
 - b) Allow only desired services and disallow the rest
 - c) Allow only desired protocols and disallow the rest
 - d) Two way authentication for network traffic

NOTE: Some of the systems use proprietary protocols for which the firewall rules are opened to allow any protocol. Such measures are potential security compromises and should not be encouraged.

4. The Organisation should implement two firewall devices connected in series from different OEMs. Common and uncommon IPS signatures from disparate OEMs will enforce tighter security regime.
5. The following controls to be applied for remote access:
 - a) If the remote access is provided through a public network, then encrypted transmission shall be used such as Virtual Private Network (VPN)
 - b) If the remote access is only for diagnostic services or repair, the same shall be provided after taking work permit. Further, the remote access shall be disabled including physical disconnection of the communication devices after the intended period of usage, in which case the work permit shall be closed. Firewall rules should also be modified immediately restricting remote access, after the intended period of usage
 - c) All remote access to the system/devices shall be request controlled. i.e. initiated from the local end and not from the remote end

- d) If the remote access is provided on permanent basis, say for remote operation, then additional security measures shall be provided. Eg. Point to point link, Leased line, Creation of DMZ (De-militarized zone) etc.
 - e) All remote access (permanent or restricted time) shall be allowed only after a clear documented procedure of usage
 - f) For certificate-based VPN access clients, the certificates must be installed by authorized personnel. The certificates must be kept secured enough and any incident of theft must be succeeded by regenerating and redeploying of certificates
6. Firewall, routers and bandwidth manager in the perimeter zone, core switches with built-in firewalls, application servers, field equipment (RTUs, PLCs etc.) generate a huge number of logs. The Organisation should generate and maintain logs of sufficient detail to create historical audit trails of firewall activity for a user defined period. Manual analysis of logs and taking instant corrective actions is not always possible. To automate this, Security Information and Event Management (SIEM) software may be deployed for real time collection of logs from different critical devices/servers for correlating, final analysis and quick corrective actions. Organisational policies must ensure restricted access to these logs.
7. The Organisation should document the above measures as evidence of enforcement with revision control and screen shots of the system enforced parameters
8. Wherever possible, the system must detect unauthorized access attempts and alert specified personnel through automated SMS, email etc.
9. Alarms acknowledgement should be by authorized users only

MR 17 – Account Management

This MR addresses the requirement of a management process for controls in order to ensure effective and secure account management. The account management controls shall support enforcement of security policies either as a whole or selectively. i.e. account management controls shall include authentication as well as authorization.

Requirements:

1. Default passwords should be changed at the time of system or device deployment unless these are pseudo-randomly generated and are unique to the system or device. Similarly, unused default system accounts (eg, Guest, "Super User") should be removed or disabled at the time of system/ device deployment
2. For the systems or devices with password-only authentication, following controls are to be enforced:
 - a. Password length shall be at least eight characters. Password shall consist of a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special character (%, #, etc.)
 - b. Password shall be changed every [user defined] days prior to expiration with a default of 30 days. Users should be prompted to change their passwords on the system or devices according to this defined setting

- c. The account management controls shall prohibit reuse of the three previously used passwords
 - d. The account management controls shall limit the number of unsuccessful authentication attempts. Alternatively, alerts should be generated after the defined limit of unsuccessful attempts are exceeded
3. Wherever considered critical to the health, safety of personnel and equipment and environment, enhanced controls for authentication should be provided, subject to technical feasibility. These controls shall include but not be limited to:
 - a. Password encryption
 - b. Encryption for device administration
 - c. Multi factor access control
 - d. Two way authentication for network traffic

NOTE: Some of the above measures can be used in network devices for enhanced security. In safety systems, the device used for control logic changes could be authenticated through a combination of password and an external physical device like dongle. (i.e. Multifactor authentication).

4. The account management controls shall be used for enforcing security controls through a centralized policy. For this purpose, account groups or roles could be created, thereby implementing Role Based Access Control (RBAC), in which a role is assigned a specific role in the CII (guest, operator, maintenance engineer, security administrator etc.).
5. The Organisation to perform the following:
 - a) Special accounts like no login or application specific logins shall be configured such that they never expire or never get disabled automatically.
 - b) Workstations which are in unmanned areas shall have an automatic locking and disconnection mechanism.
 - c) All users of shared accounts shall be listed.
6. The Organisation to document the above measures as evidence of enforcement with revision control and screen shots of the system enforced parameters.

MR 18 - Patch Management

This MR addresses the requirement of a management process for tracking, evaluating and installing patch updates for the applicable assets. This may even include identification of a source(sources) releasing the patches.

Requirements:

1. The automation solution provider shall be capable of providing documentation to the asset owner describing how the security patches for automation solution software are evaluated and approved. This shall include security patches for the control system and component software, operating system software, and 3rd party software applications integrate into or with the automation solution, the control system, and components. It is to be noted that the firmware upgrades shall also be regarded as software patches.

Further, the automation solution provider shall, as a result of the changes in security risks, be capable to review and update as to how it evaluates and approves security patches for automation solution software for which it is responsible. This review needs to be performed periodically or explicitly in response to the changes in the risk environment that are recognized to have a potential impact in the process. Changes to the risk environment generally includes new threats and vulnerabilities as well as the development of new security technologies.

NOTE: 'Approved' means that the patch has been tested and validated by the automation solution software provider against a known configuration and no issues were found.

2. The Organisation should formulate a plan for upgrading/updating the firmware versions of networking/telecom and OT devices for addressing all operational issues. There shall be an agreement between the Organisation and OEMs so that the new version/releases are immediately communicated to the users.
3. The automation solution provider shall make available to the asset owner document containing the following details about the security patches within an agreed time frame after the release of the patch by the manufacturer:
 - a. Applicability of the patch for the asset owner's systems including the version nos. of the software to which the approved patches are applicable
 - b. The result of patch qualification process, that is, whether the patches have been approved, not approved, not applicable, in test, etc. and the reason for those that are not approved or not applicable
 - c. A remediation plan for those that are not approved or not applicable
 - d. Whether the software libraries for the patches used by automation solution software provider are enhanced or different from those provide by the manufacturer(s), i.e. whether the automation solution software provider has altered the software patch package or not
 - e. Whether the installation of the approved patch requires system shutdown or re-start
 - f. Recommendations to mitigate the vulnerabilities for the patches that the asset owner choose not to install

The above documentation for the patch list shall be made available to the asset owner through an interface commonly accepted by the industrial and security committees. This interface may be with the control system product supplier, with the automation solution software provider or with another agent as identified by automation solution software provider.

4. The automation solution provider shall install patches to the asset owner's systems only after the approval of the same from asset owner. Further, the automation solution software provider shall recommend a mitigation plan to the asset owner for the approved applicable patches that were not approved by the asset owner for various reasons like impact on operations or performance. This mitigating plan shall include compensating mechanisms or other means to reduce the vulnerabilities addressed by that security patch and will be subject to asset owner's approval for implementation by automation solution software provider.

5. The automation solution provider, as a part of patch management plan, shall clearly inform the asset owner about the patches that are to be directly obtained by the asset owner from the patch's manufacturer and, if the licensing agreements with the patch manufacturer allows and has been requested/permitted by the asset owner, the patches that are to be distributed to asset owner by automation solution provider. If the patches are to be delivered by the automation solution provider, then the automation solution provider and the asset owner has to jointly decide on the protocol as to how this will occur (e.g. through DVD, secure connection, etc.). This ensures that the patches are obtained through an authorized channel from an appropriate source to reduce the possibility that they could be invalid/infected.
6. The automation solution provider shall furnish the documentation to the asset owner clearly describing the process as to how patching is to be done through one or more of the following applicable ways and obtain the patching status reports:
 - a. Manual patching using portable media (e.g. CDs, DVDs, etc.)
 - b. Using patch management server

For the devices that support installation of software/firmware over the network, the automation solution provider shall have a well-defined process for securely updating the software/firmware in such devices which shall include but not limited to ensuring that the patches installed over the network are authentic and not corrupted during the patching process i.e. the update images sent to the device are protected during transmission against modification, allowing only the authorized users to perform updates, etc.

Also, only the security patches that have been approved by the asset owner are to be installed by the automation solution provider and obtaining such necessary approvals shall form a part of the automation solution provider's policy.

Further, if the automation solution provider is to install the software security patches in order to prevent process upset (if a device has to reboot after the installation), the time of installation of patches shall be as specified/decided by the asset owner. The automation solution provider shall have a well-defined procedure for the same.

7. The automation solution provider shall have measures to ensure that the security hardening level of the automation solution is retained after the patch installation through various suited activities like re-installing software or changing system configuration settings, etc., irrespective of who installs the patches. The automation solution provider has to have a process to determine if the removal of or degradation of system hardening has occurred due to patch installation and whether it has to restore the same.
8. Automation solution provider shall have a well defined process (manual procedures or automated tools) for tracking whether the patches approved for the automation solution have been installed or not and shall clearly bring out the patches that are missing/not installed.

MR 19 - Legacy System Integration

This security control defines a formal procedure for legacy system integration for cyber security. In some cases, these systems installed before there was concern about system security, and hence

security mitigation measures were not included. Typically, the Organisation should determine the current security configuration of legacy components and updates.

Requirements:

1. The Organisation should develop policies and procedures to integrate and upgrade all legacy components of the smart grid systems to include security mitigating measures needed to bring all elements of the smart grid systems into compliance with current security requirement commensurate with the Organisation's risk tolerance for those components.
2. The Organisation should ensure that the identity should be verified through strong authentication mechanisms. Organisations should implement an implicit deny policy such that access to the network is granted only through explicit access permissions.
3. In order to protect the hosts from intrusion, Host Intrusion Perversion System (HIPS) should be integrated with servers and core networking devices. Depending on the situation, appliance or software based HIPS may be deployed. To ensure better end-point security, hardware or software-based Network Access Control (NAC) mechanism has to be deployed along with Active Directory (AD) services. NAC shall cover all the desktops/laptops etc. connected to the corporate network.
4. The Organisation to formulate security portion of the smart grid from the designing stage itself. Otherwise, security of devices becomes vendor specific; the fact that might produce many vulnerabilities because of incompatibility issues.
5. As the life cycle of the smart grid is longer than that of the IT systems involved, the Organisation to ensure that all IT technologies should have the ability to be upgraded.

C) Security Control – Information Protection

MR 20 – Formulation of Policy for Disposal of Critical Digital Assets (CDA)

This Security Control defines a procedure for policy formulation of identified Critical Digital Assets (CDA). CDA are cyber assets that are essential for the reliable operation of various systems. This is a formal documented policy that addresses the purpose, scope, roles and responsibilities, management commitments and internal coordination of security controls. The first focus area in this policy is the identification of digital assets as a CDA and then identifying potential cyber security risks to CDA with categorization and implementing mitigation strategies for the identified risks.

Requirements:

1. The Organisation should specify the process for identification and disposal of critical digital assets
2. The Organisation should identify potential cyber risks associated with categorization of CDA
3. The Organisation should undertake regular review and validation/modification/addition of a CDA
4. The Organisation should maintain an effective cyber security plan for all the critical digital assets
5. The Organisation should maintain a multi-layered system and all CDAs relevant to safety, and security should be placed directly in inner most secured layer

MR 21 – Information Protection (including Data Storage)

This security control defines a formal procedure for information protection mechanism including data residing on storage, disk drives (both internal / external), desktops / laptops, Servers, LTOs, etc. The value of the data that requires protection and the system storing the data need to be considered carefully. An in-depth approach is recommended when evaluating and deploying encryption methods. This approach applies to both data at rest and in transit.

Requirements:

1. The Organisation should formulate strategies, plans and programs for data protection
2. The Organisation should adhere to manageable set of encryption policies which meets the Organisational requirement
3. The Organisation should take adequate measures to protect against information loss or leakage by implementing data loss prevention solutions
4. Information protection is a continuous process and data protection strategies to be reviewed regularly
5. Wherever possible, communication between devices and/server shall be using digital signatures

D) Security Control – Audits, Assessments, Certification and Testing

MR 22 - Internal and External Audit (including VTR Assessment and Penetration Testing)

Regular internal and external audit for the cyber security must be conducted by the Organisation. It is advisable to change the auditors on a regular basis.

Vulnerability, Threat, Risk (VTR) assessment and Penetration Testing (PT) need to be integrated as part of internal and external cyber security audits. VTR assessment and management is an ongoing process and must be reviewed regularly. Penetration Testing for communication network and public facing web portal / services should be carried out at regular intervals.

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 a given threat source highlighting a particular potential vulnerability and its adverse impact.

Penetration Testing evaluates and tests the preparedness of the Organisation fighting threats originated from the weak or flawed implementation of a security framework. The testing is aimed to uncover real time vulnerabilities or loopholes existing in the infrastructure which can be exploited by malicious entities.

Requirements:

1. The Organisation should conduct internal and external cyber security audits once a year by CERT-empanelled agencies

2. The Organisation should change the auditors on a regular basis
3. The Organisation should devise a mechanism involving its employees and external professional consultants for the conduct of VTR assessment and Penetration Testing
4. The Organisation should arrange a Non-Disclosure Agreement (NDA) in case external agencies are employed to perform VTR assessment and penetration testing
5. The Organisation should maintain the operational sanctity of the critical processes while doing these tests and ensure that the vulnerability testing is not leading to the system collapse
6. The Organisation should undertake review and implement the important feedback emanating from Penetration Testing and occasional internal/external audits

MR 23 – Cyber Security SLAs

Smart grid has made traditional grid operations to be more reliant on IT infrastructure for system monitoring, control, computing and communication requirements. Third party IT services like data backup, cloud computing and communication infrastructure support are being outsourced. Cyber security Service Level Agreements (SLAs) can help reduce risk to the Organisation while outsourcing such operational requirements. Also, well negotiated SLAs are of great help in post-incident legal combat.

Organisation must insist on specific and enforceable stipulations in SLAs in compliance with controls and standards to which the Organisation is committed. A management level framework is needed to monitor compliance of SLAs.

Requirements:

1. The Organisation should identify and communicate its specific cyber security objectives to outside agencies in a well-documented SLA
2. The Organisation should implement a management framework to monitor compliance with security objectives in SLAs with third parties
3. The Organisation should specify measures of security performance in SLAs
4. The Organisation should specify responsibilities of the outsourced agency for end user violations and end user support
5. The Organisation should specify confidentiality, integrity and availability obligations with exceptions, if any, in SLAs

MR 24 - Testing and Evaluation of Equipment and Software before Procurement

Security of interconnected systems like electric grid depends on the weakest link in the network. The entire Organisation may get exposed due to a vulnerability in any one equipment or software. Hence due care is needed while procuring such equipment or software.

The inherent vulnerabilities of Commercial off-the Shelf (COTS) products and code appended with the hardware/software needs to be thoroughly evaluated. These products may contain malware which can bypass security checks in the network. Organisations need to be cautious in deploying possibly contaminated hardware or software products.

After procurement and before deployment of hardware there should be procedures/framework for an in-depth testing and evaluation of systems.

Requirements:

1. The Organisation should specify security requirements and evaluation criteria during procurement process

2. The Organisation should undertake upgradation and patching of its existing critical assets on a regular basis
3. The Organisation should make sure that the equipment and software is deployed only after appropriate testing of their security features and the test reports to be maintained till the life cycle of the product
4. The Organisation should set up a training curriculum with national laboratories/testing centres to train their employees and vendors about the risk involved in procuring COTS products
5. The Organisation should maintain in house testing facility/personnel atleast to the extent of functional testing capabilities

MR 25 - Security Certification

Third party security certification is needed to validate the security measures adopted by the Organisation for protecting its IT and OT infrastructure. The third party certifying agency may be a government agency, or an agency empanelled/recommended by the competent government authority.

Process of security certification needs to be carried out according to national/international standards as specified by the competent authority and need to be reviewed on a regular basis to incorporate new controls released from time to time. The recommendations of the certifying agency need to be implemented and a mechanism needs to be evolved at the Organisation level to monitor its impact on the security enhancement.

Security certification shall be applicable to the Organisation, its employee and its vendors/contractors and sub-contractors. Individuals holding key positions in the security framework of the Organisation needs to undergo suitable security certifications after attending appropriate training sessions.

Requirements:

1. The Organisation should identify a suitable government agency or a government empanelled agency or another agency directly authorized/empanelled by the certification agency for the certification
2. The Organisation should undertake process of certification of its security measures for IT/OT assets
3. The Organisation should undertake certification of its employees, vendors and contractors who are operating critical assets of the Organisation
4. The Organisation should maintain all observations made by certifying agency and share them with the competent government authority as and when needed

E) Security Control – Personnel and Training

MR 26 - Security Awareness Training

This MR defines a formal procedure for educating the appropriate personnel in the Organisation about cyber security. A security awareness programme is made with the aim of educating the personnel about the strategy, policies and procedures defined by the Organisation. The skills and knowledge thus acquired will be vital forces for growth of the Organisation.

Requirements:

1. The Organisation should formulate strategies, plans and programs for training the appropriate personnel in cyber security
2. The Organisation should review, assess and modify (if needed) the training strategies, plans and programs at least once a year
3. The Organisation should make sure that all appropriate personnel undertake training as per the strategies, plans and programmes defined by the Organisation
4. The Organisation should set up a training curriculum after identification and evaluation of vulnerabilities and threats in coordination with the Information Security Department (ISD)
5. The identified seminars, conferences and workshops could be conducted by the Organisation itself or by competent external agencies

MR 27 - Personnel Risk Assessment (including Supply Chain)

Personnel risk assessment is an integral cyber security control which deals with the safety and security of the critical information from unauthorised personnel and unauthorised access. It accounts for the risks which the personnel could pose to the Organisation. It also helps the senior officials in the Organisation to identify the risks to which the Organisation is exposed and hence take appropriate measures to mitigate such risks.

Requirements:

1. The Organisation should have a well-documented personnel risk assessment programme for persons having authorised access to the critical cyber assets
2. The Organisation should perform identity verification and a thorough background check for employees deployed on critical roles
3. The Organisation should ensure that all employees sign a Non Disclosure Agreement (NDA) prior to joining the Organisation
4. Each personnel risk assessment should be updated through HR/Vigilance every five years after the initial check which is conducted during the joining of the personnel
5. The Organisation should also include the elements of the supply chain like the contractors, subcontractors etc. and subject them to the same identity verification and thorough background check as for its internal employees

F) Security Control – Physical Security

MR 28 - Physical Security Plan

This security control deals with the specification of a physical security plan that is needed in order to counter the threats and vulnerabilities. It is used to protect the critical cyber assets and critical information from potentially harmful sources. Absence of a physical security control can lead to a reduction in the effectiveness of cyber security controls.

Requirements:

1. The Organisation should devise suitable plans and policies for implementation of physical security control
2. The Organisation should identify and mark various security zones like secure, restricted etc.
3. The Organisation should keep a visitor log of each entry and exit into the secure zone along with the date and time of entry

4. The Organisation should use biometric readers and access control badges for a more stringent control of unauthorised physical access
5. The Organisation should conduct periodic mock drills and audits in order to identify the threats and vulnerabilities of the physical security system
6. The Organisation may deploy hardware such as high-delay-time fencing products, vehicle barriers, retractable bollards, crash-rated gates and sally ports, video surveillance and intrusion detection systems around its entire perimeter. Advanced motion analytics may be deployed along unmanned secure zones
7. The Organisation should change the keys and combinations on a defined frequency for accessing secured zone where access control is not implemented
8. The Organisation should formulate a maintenance and testing program to make sure all physical security and safety systems are functioning properly
9. The Organisation should ensure that only authorised personnel have access to critical devices

G) Security Control – Operations

MR 29 - Monitoring and Review Policy

Monitoring and review of security policies is a vital part of the policy framework as it is required to fill the loopholes. It provides an opportunity to the Organisation to keep updating its security posture through regular checks, thus making the security controls and policies more effective.

Requirements:

1. The Organisation should regularly monitor and review all the security controls viz. the policies, plans, guidelines, standards and procedures atleast once a year
2. The Organisation should keep a comprehensive and detailed record of the 5 most recent audits, reviews, modifications and updates to its security policies, plans, guidelines, standards and procedures
3. After assessing the effectiveness of security controls, the Organisation to modify and/or update the controls
4. The Organisation should document all such changes (if any) and take sign off from the CISO and the Senior Management

MR 30 – Change and Configuration Management

During the hardware or software product lifecycle, changes are made to fix errors, apply patches or to enhance the product functionality. Changes are inevitable, and therefore the Change and Configuration Management control helps in seamless transformation during a change in the Organisation's plans, policies, procedures, configurations, etc.

The purpose of Configuration management is to establish and maintain the integrity of the software products throughout its life cycle. Configuration management involves identifying configuration items for the software project, controlling these configuration items and changes to them, and recording and reporting status and change activity for these configuration items. Configuration management enables the management of artefacts from the initial concept through design, implementation, testing, baselining, building, release, and maintenance.

Requirements:

1. The Organisation should develop a baseline configuration, individually or by group, which shall include the following items:

- i. Operating system(s) (including version) or firmware including virtualized environment
 - ii. Any commercially available or open source application software (including version) intentionally installed
 - iii. Any custom software installed
 - iv. Any logical network accessible ports
 - v. Any security patches applied
2. The Organisation should authorize and document changes that deviate from the baseline configuration
3. For a change that deviates from the baseline configuration, the Organisation should update the baseline configuration as necessary within 30 calendar days of completing the change
4. For a change that deviates from the baseline configuration:
 - i. Prior to the change, the Organisation should determine required cyber security controls that could be impacted by the change
 - ii. Following the change, the Organisation should verify that required cyber security controls determined in (i) are not adversely affected
 - iii. The Organisation should document the results of the verification
5. Where technically feasible, for each change that deviates from the existing baseline configuration:
 - i. Prior to implementing any change in the production environment, the Organisation should test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls are not adversely affected
 - ii. The Organisation should document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments

MR 31 - Contingency Plans

This MR addresses the requirement of a documented management process for contingency plans in order to ensure that effect of a security breach or incident is minimal and does not affect the business processes of the Organisation. It encompasses crisis management, business continuity and disaster recovery. Last but not the least, it also includes the learnings and remedial actions in terms of mitigating the vulnerabilities that were exploited, in order to prevent similar incidents in future.

Requirements:

1. Wherever considered critical to the business continuity, the Organisation's system shall have an enhanced redundancy built in the architecture. Eg Firewalls are configured in "deny all" mode. If the connectivity of SCADA to the Organisation's enterprise network controls is protected by such firewalls, and SCADA data is needed in the Organisation's enterprise network all the time, then the firewalls shall be redundant and configured in fail over mode.

Similarly, critical data shall be backed up through redundant path or redundant devices.
2. The Organisation to implement the following:
 - a) The system/device shall have a back-up strategy and architecture in place

- b) The back-up strategy shall list the data to be backed up. This shall include (but not limited to) operating system files, middleware/SCADA system software, configuration data/ database files, network settings, controller settings/program, and real time archival data (if not already covered in the system historization scheme)
 - c) The back-up strategy shall take into account the vendor-recommended procedure for system restore. It shall also include a checklist of all files necessary to restore the system in the case of an incident
 - d) The back-up strategy shall include a procedure for verification of successful system/device back up
 - e) The back-up process shall not hamper in any way the normal operation of the system/device
 - f) The back-up architecture shall also be described which can be either based on distributed architecture or centralized architecture. Reason for choosing either architecture shall be documented
 - g) The back-up architecture using USB devices shall be prohibited. Removable media back-up shall be using DVDs and all other requirements for security shall be followed during the process
 - h) Frequency for the restoration testing should be defined and adhered to.
3. The system shall have a clear documented procedure and architecture for supporting disaster recovery. Disaster Recovery (DR) site shall be as far as possible in a different seismic zone. If the same is not possible, DR site is to be created at a different physical location of the same organization and reasons for the same shall be clearly documented. There shall be fail proof replication of data between Data Center (DC) and DR sites. The communication bandwidth for data transaction between DC and DR shall be adequate. There shall be agreed RTO and RPO. The organisation has to perform DC – DR drill once in every six months as per the pre-approved Drill Document and note the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameters for all the applications. The Organization shall also perform mock drills for failover of Master Control Centre to Backup Control Centre once in 6 months. All operations during this mock period to be done from the Back-up Control Centre.

MR 32 – Incident Response Management System

Incident response management systems are employed to deal with critical events when a security breach has already taken place or in emergency situations. These incidents can lead to serious damage to the critical data which the Organisation houses and consequently to the security of the Organisation. An incident can be a network or computer attack, an environmental one or a physical security attack.

Requirements:

1. The following should be enforced by the Organisation for incident response:
 - a) The Organisation should have a well documented incident response process for each type of incident
 - b) The process should include Standard Operating Procedures (SOP) identifying the roles and responsibilities of each person and the agencies where the incident should be reported along with the escalation matrix
 - c) The incidents to be covered shall include (but not be limited to) virus attack, denial of service attack, unauthorized copying/ disclosure of information, tampering,

- unauthorized modification of information, malicious alteration of operating systems, wire tapping, theft of any hardware or software resource (excluding end user devices), attempts to gather information, hacking attempt, network outages, denial of service attack
- d) Natural disasters (Flood, Earthquake, Cyclone) shall also be included in the incidents however their analysis shall be treated differently
 - e) Electrical outages and fire (not caused by any cyber vulnerability) shall also be included in the list of incidents
 - f) The process should also include the response period for restoration of the affected business process. Eg. in case of SCADA, if the functions are partially affected due to a security incident, this shall be the time taken to restore the full functionality of the SCADA
2. The Organisation should implement the following for reviewing the incident response process:
- a) Incident response shall be subjected to review and updates, if necessary, on every reported incident or every [user defined] period as per the need of the business process. The maximum period of such review shall be one year
 - b) In case of every reported incident, a thorough analysis shall be performed by the ISD regarding the vulnerabilities that were exploited in the security incident and the changes, if any, that are required in the incident response. Eg. this lead to creating additional redundancy in the system architecture or additional back-up mechanisms to quickly restore the business process that was hampered as a result of the incident.
 - c) If any deviations from the incident response surface during an actual incident, the same shall be analysed and if required, the incident response shall be updated along with clearly documented reasons thereof.
3. The Organisation to implement the following for spreading awareness about the incident response process:
- a) Creating awareness among employees for reporting of all types of cyber security incidents. The list of persons with their residential phone numbers and mobile numbers to be contacted during emergency should be displayed at each relevant location
 - b) The updation of the incident response process as a result of periodic review or as a result of incident analysis shall also be distributed to all the intended recipients. Requirements of clause (a) above shall also apply to the updation of the incident response plan
 - c) Incident response process for business continuity to be implemented through mock drills at regular intervals

MR 33 - Security of Redundant Systems

Redundant systems are required in most electrical systems in order to ensure the reliability and availability. Since power systems are one of the most critical infrastructure, it is important to ensure the highest levels of performance at all times. Ensuring the security of these redundant systems thus becomes paramount.

Requirements:

1. The Organisation should apply security controls on redundant systems in a similar manner as for mainstream systems
2. The Organisation should identify if any redundant systems do not require security controls
3. The Organisation should take sign-off from the CISO and senior management if some security controls are not applied to redundant systems
4. There should be a provision of taking periodic image-based back-up of critical servers for OS and applications for faster restoration of services by deploying the image on a bare metal server

MR 34 - Technology Obsolescence

Useful life of IT and OT assets is the period of time for which the asset will be economically feasible for use in a business. In other words, it is the period of time for which the IT/OT asset will be in service and used to earn revenues. Life of asset is defined under following categories:

- Legal Life: The life of a leased asset would be limited to the period of the lease
- Physical Life: The asset may physically wear out and be reduced to scrap
- Technical Life: A technically superior asset may supersede the old asset resulting in the cost saving, which would translate into a competitive advantage for the user
- Commercial Life: The present value of the operating and maintenance expenditures may exceed the cost of replacement

The commercial life of any IT/OT asset is the shortest of the above mentioned categories. There are many factors that contribute to the useful life of IT/OT assets - deterioration of electronic components due to thermal stress, wear and tear of mechanical parts, which increases the downtime of IT/OT systems. Technology in computer hardware/software systems changes very fast and becomes out-dated/obsolete within a period of three to six years. Un-availability of spare parts or discontinuation of support for the devices by OEM is one of the contributing factors to decide useful life of IT/OT assets. Vendors stop supporting the obsolete technology and it becomes difficult to get spare parts/upgrades of the old assets. Old assets are not suitable to work on updated versions of operating system and applications. Technically superior assets also supersede old assets.

Requirements:

Organisations to bifurcate the IT and OT assets into following groups and their useful life may be decided based on the latest Company's Act:

1. **Backend devices** such as servers, storage, tape library, core switches, distribution switches, internet switches, security systems like firewalls, intrusion prevention, intrusion detection system, web content filters, etc. with associated software with useful life of 6 years
2. **End user devices** such as laptops, desktops, printers, scanners, readers, plotters, small UPS upto 2.2 kVA, IP Phones, etc. with associated software with useful life of 3 years
3. **Office equipment** such as Projectors, Video Conferencing equipment, CCTVs, cameras, etc. with useful life of 5 years
4. **Communication equipment**
 - a. Media like Radio, high frequency carrier system, Optical Fiber Cable, Optical Ground Wire, etc. with useful life of 15 years
 - b. Terminating electronic equipment like Multiplexer, PTN equipment, etc. with useful life of 7 years

- c. RF mesh for smart metering with useful life of 10 years
- 5. **Telephone lines and telephones**
 - a. PSTN phones with useful life of 18 years
 - b. IP enabled phones, headsets, microphones etc. with useful life of 3 years

6. References

The following references have been used for the preparation of this Manual:

1. NERC CIP Standards Version 5
2. 'Top 10 Findings and Recommendations of Cyber Security Preparedness Survey' published by ISGF and NCIIPC in 2015
3. NIST IR 7628 Revision 1 (Volume 1) Guidelines for Smart Grid Cyber Security published in 2014
4. '21 Steps to Improve Cyber Security of SCADA Networks' published by US DoE
5. Guidelines for Protection for Critical Information Infrastructure (Version 2) published by NCIIPC on January 16, 2015
6. NIST Special Publication 800-82 Revision 2 published in 2015