Version 1

NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

BLOCK III, OLD JNU CAMPUS, NEW DELHI-110067 (INDIA)

Table of Contents

1. Introduction

1.1. Since the creation of the National Critical Information Infrastructure Protection Centre (NCIIPC) in January 2014, we have had frequent interactions with various organisations spread across all critical information infrastructure sectors. During these interactions, one of the most common concerns we faced was the lack of an accurate assessment of the present status of the cyber security controls implemented by organisations. We realised that even within an organisation, personnel across various verticals viewed this differently, based on their own specialisations and the vertical they represented.

1.2. This is a worrying aspect. We noticed that in some organisations the Information Technology (IT) and Operational Technology (OT) personnel had distinctly divergent views. Resultantly, the organisational cyber security posture was considerably weaker than it should have been.

1.3. A large number of technical documents indicating measures required to implement strong cyber security architecture are available. However, there is little guidance available for organisations wishing to determine the efficacy of cyber security controls implemented, as well as that of the actual implementation process. It is with a view to close this gap that NCIIPC has created this document.

1.4. In addition, the present method of assessing the efficacy of implemented controls is largely by means of cyber security audits. While there is no denial on the role and importance of these audits, it is also important to stress that a cyber security audit is essentially a snapshot of controls as they existed at the time of the audit. What is crucial for any organisation however; is the steady state, ongoing status of their cyber security mechanisms. This document outlines the basic aspects requiring consideration. The emphasis here is also on the fact that any analysis is worthless unless shortcomings are remediated. In order to ease the remediation process, it is important for a clear and actionable plan involving the concurrence and support of the senior most management of the organisation.

1.5. It is expected that a systematic analysis of the processes outlined in this document would enable organisations to determine with a large degree of accuracy, their present status, the major gaps (if any), and the way ahead

towards strengthening and maintaining the strength and resilience of their cyber security posture.

1.6. In order to address the requirements of the largest cross section of our constituency, we have made a deliberate attempt to be technology and process agnostic. In addition, the resultant outcome of this exercise, when undertaken by any organisation would enable their senior most management to understand the present status, along with steps required to enhance their cyber security posture. A deliberate effort has been made to keep the entire process as jargon free as possible. In addition, wherever possible, an attempt has been made to ensure that the process itself indicates expectations from CISOs and their cyber security teams.

1.7. Diagram given in Figure-1 depicts the work flow for establishing the above, as part of the NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure:

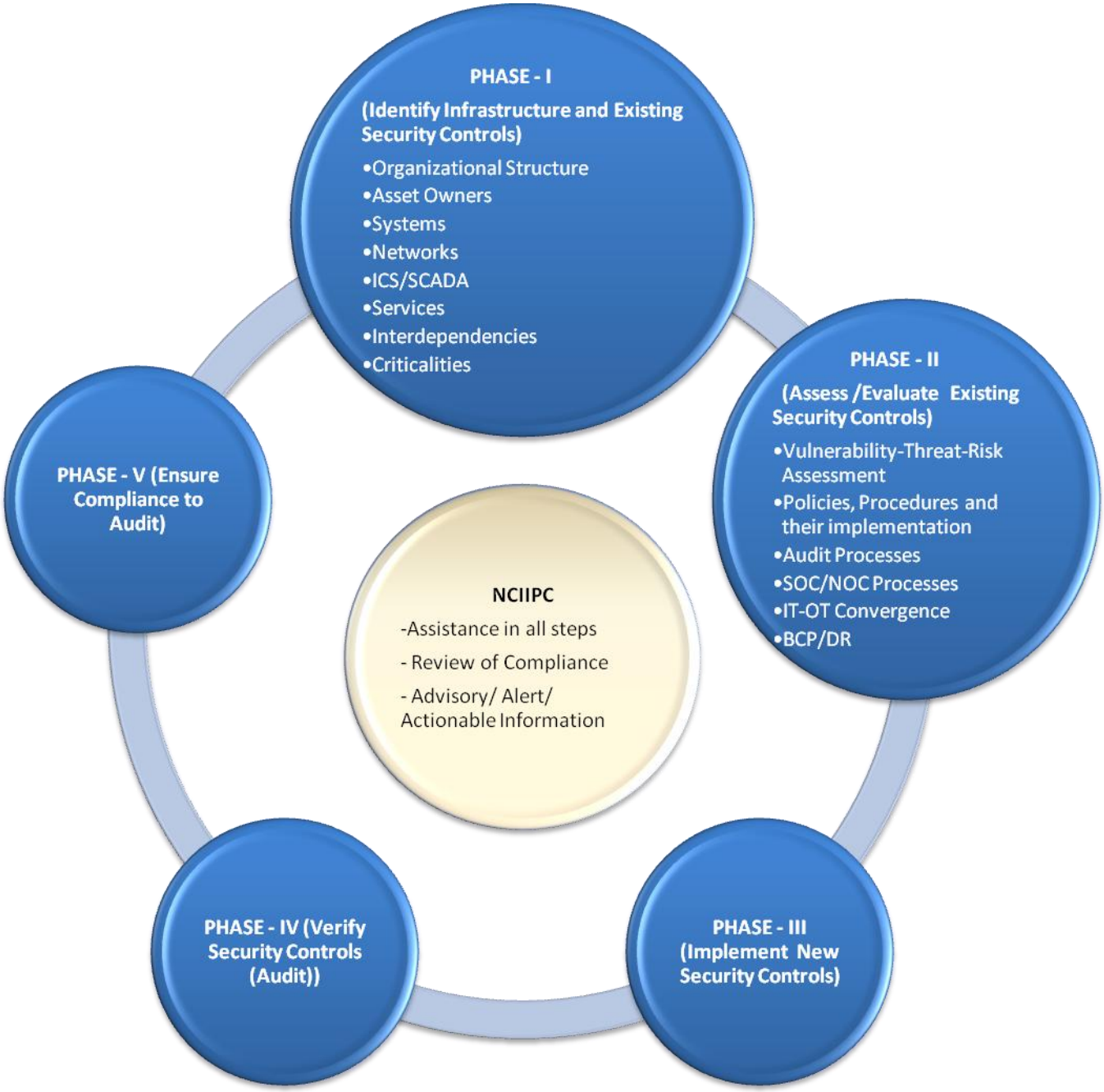

Figure-1: NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure

Steps/phases for conducting the evaluation of cyber security are explained in detail in subsequent paragraphs.

2. PHASE-I: Identify Infrastructure

In this step/phase, Organisation needs to identify organisational critical business processes, Cyber Assets and incoming & outgoing dependencies, along with **existing Cyber Security Controls**:

a) Organisational cyber security structure

b) Systems

c) Industrial Control Systems (ICS)

d) Network

e) Services

f) Criticalities

g) Interconnectivity/interdependency

h) Continuity

Details are given in subsequent paragraphs along with sample questions.

2.1. Organisational cyber security structure:

Organisation needs to constitute / appoint / identify the following:

2.1.1 Information Security Steering Committee (ISSC).

2.1.2 Chief Information Security Officer (CISO).

2.1.3 Who does the CISO report to?

2.1.4 Sectoral CISO Details

2.1.5 Management commitment to information security

2.1.6 Information security coordination

2.1.7 Allocation of information security responsibilities

2.1.8 Contacts with Government authorities/agencies/associations

2.1.9 Frequency, level and quality of Cyber Security Training/awareness

2.1.10 Addressing security in third party agreements

2.1.11 Addressing security when dealing with customers

2.1.12 Information Security Workforce

2.1.13 Certification and accreditation

2.1.14 Cyber Security Incident Response Team

2.1.15 Roles and Responsibilities of owners of cyber security processes

2.1.16 Senior Management Accountability

Sample Questions:

Does the CISO report directly to the Board of Directors?

Are all components (IT/OT/ERP etc) reporting to the CISO?

Is IT (Information Technology) and OT (Operation Technology) a board agenda?

2.2. **Systems**

Organisation needs to identify its systems, related processes and existing security controls:

2.2.1 System Procurement Standards or Services Acquisition

2.2.1.1 System acquisition contracts

Organisation may identify system acquisition processes/automated-systems and corresponding security controls to protect them.

Sample Question:

Are security functional requirements and specifications included in system acquisition contracts based on an assessment of risk?

2.2.1.2 Vendors/contractors

Organisation needs to identify processes and security controls for dealing/managing vendors/contractors and services provided by them.

Sample Question:

Do acquisition documents require that vendors/contractors provide information describing the functional properties of the security controls employed within the system?

Are OEMs providing Security Support/pre-public release for yet to be patched vulnerabilities?

2.2.2 Software development

Organisation needs to identify security controls applied to software development life cycle. This also includes outsourcing and integrator security testing.

Sample Question:

Is a baseline configuration for the development and test environments maintained and managed separately from the operational baseline?

Does your organisation encourage the vendor to follow software development standards for trustworthy software throughout the development life cycle?

SDLC: Software Development Life Cycle: Is Organisation involved during the cycle?

2.2.2.1 Outsourcing

Sample Question:

Does Security Policy/Procedure exist for outsourcing? Does SLA comply with the security policy?

2.2.2.2 Developer/Integrator Security Testing

Sample Question:

Are system developers/integrators required to implement and document a configuration management process that tracks security flaws?

Does the system developer/integrator perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations?

2.2.3 System Integrity

To ensure system integrity, Organisation needs to identify processes and applied security controls with respect to the following categories:

2.2.3.1 Flaw Remediation and Functional Verification

Organisation needs to identify processes for verifying functionalities provided by the systems/applications and detecting, reporting & correcting system flaws.

Sample Question:

Are system flaws identified, reported, and corrected?

Does the system notify the system administrator when anomalies are discovered?

2.2.3.2 Security Alerts

Organisation needs to identify process for generation of cyber security alerts and advisories.

Sample Question:

Are internal security alerts, advisories, and directives generated?

2.2.3.3 Software Information Integrity

Sample Question:

Does the system monitor and detect unauthorized changes to software and information?

2.2.4 System Protection

2.2.4.1 OS Hardening & Least Functionality & Unnecessary Software/service removal

Organisation needs to identify existing OS hardening controls. This also includes:

2.2.4.1.1 Default configuration change

2.2.4.1.2 White-listing of services, ports and protocols

Sample Question:

Are automated mechanisms used to prevent program execution in accordance with defined lists? (e.g., white-listing)

Is the system periodically reviewed to identify and eliminate unnecessary functions, ports, protocols, and/or services?

2.2.4.2 Malicious code protection

Organisation needs to identify malware protection mechanisms applied to their various systems.

Sample Question:

Does the information system implement non-signature-based malicious activity detection?

2.2.4.3 Information Input Validation

Input validation is first line of defence when creating a secure application. Organisation needs to identify processes/controls for limiting the input data to be processed by the applications.

Example: SQL Injection, Cross-site-scripting etc. ("OWASP checklist")

2.2.4.4 Cryptographic Considerations

Organisation needs to identify Cryptographic Security controls applied to systems such as usage of encryptions, hashing, digital signature and processes such as key management.

Sample Question:

Are other cryptographic solutions such as cryptographic hashes considered in place of storing encrypted user passwords and authentication tokens?

2.2.4.5 Secure system failure state

Organisation needs to identify the secure System Failure States defined for various systems.

Sample Question:

Does the system fail to a known state for defined failures?

Does the system fail to a closed state for unknown/undefined failures?

2.2.4.6 Application Partitioning

Applications partitioning is to be done at different levels. For example, between a user and the application, and between two applications.

Sample Question:

Is user functionality separated from system management functionality? For example: usage of non-administrative privilege based Standard user accounts.

2.2.5 Log and Monitoring

The Organisation needs to identify process for monitoring logs of various systems for security events/incidents. The monitoring process should be systematic and well documented.

Sample Question:

Are logs reviewed on a defined frequency?

Does the system prohibit inclusion of sensitive information in error logs or associated administrative messages?

2.2.6 Access Control

Organisation need to identify access controls mechanisms and security controls applied. This includes user account management, usage of multifactor authentication.

Sample Question:

Are guest/anonymous and shared accounts disabled?

Is role-based access control (RBAC) used to restrict user privileges to only those required to perform the task?

2.2.7 Patches and Updates

Organisation need to identify patch management process and security controls applied for the same.

Sample Question:

Do you apply all critical control system supplier approved operating system updates in accordance with company policy?

Are received cyber security updates tested on a non-production system/device for validation before installing on production systems?

2.2.8 Media handling

Organisation needs to identify applied security controls for ensuring security of data.

2.2.8.1 Management of removable media

2.2.8.2 Disposal of media

2.2.8.3 Information handling procedures

2.3. Industrial Control System (ICS/SCADA)

Organisation needs to identify security controls for Supervisory Control and Data Acquisition (SCADA) and control systems. This includes the security controls applied under above “Systems” category.

Sample Question:

Are conditions and mechanisms established for authorized individuals to access the ICS systems from an external system?

Has cyber security risk assessment been undertaken for ICS/SCADA system as part of the overall information security risk assessment? This includes critical asset identification, asset security management etc.

Have adequate security management protocols and procedures been implemented for systems with known, identified vulnerabilities which cannot be stopped/shut down until the next maintenance cycle?

2.4. Networks

Organisation needs to identify its networks; and security controls applied for protection of all data that leaves or enters the local computer or local server from a network. This includes:

2.4.1 Access Control Or Network Access

Organisation needs to identify security controls applied for Access Control over the networks. Such as:

2.4.1.1 Identification (User ID) and Authentication

2.4.1.2 Passwords

2.4.1.3 Least privilege

2.4.1.4 Account Management

Sample Question:

Is network access to defined privileged commands authorized only for compelling operational needs and is the rationale documented?

2.4.1.5 Logon Notification

2.4.1.6 Remote Access Control

Organisation needs to identify processes and controls for remote access. This includes monitoring remote logins to the networks, analysis of logs

Sample Question:

Does the system terminate a network connection at the end of a session or after a defined time period of inactivity?

2.4.2 Log and Monitoring

The Organisation needs to identify process for monitoring logs of various networking devices for security events/incidents. The monitoring process should be systematic and well documented.

Sample Question:

Are logs reviewed on a defined frequency?

Does the system prohibit inclusion of sensitive information in error logs or associated administrative messages?

2.4.3 Audit and Accountability

Organisation needs to identify security controls applied for generating audit records and network monitoring information to identify inappropriate or unusual activity. This includes:

2.4.3.1 Audit (Events) Generation

2.4.3.2 Audit (Events) Alerts and Monitoring

2.4.3.3 Logging inclusive of , but is not limited to, critical host file changes, unauthorized and authorized client connection activity, and ad-hoc network creation.

2.4.4 Communication Protection OR Boundary Protection

Organisation needs to identify end-points, zones, communication protocols, and security controls applied to secure the perimeter. This includes:

2.4.4.1 Boundary Protection

This includes cyber security controls for different zones/perimeter/endpoints.

Sample Question:

Are public facing servers placed in a DMZ i.e. behind a firewall with an additional firewall between that and any systems on the internal network?

Are security servers placed directly in the DMZ (e.g., patch management, anti-virus, IDS, etc.)?

Is a DMZ with paired firewalls (from different vendors) deployed between the corporate and control system networks?

2.4.4.2 Network Protocols

Organisation needs to identify communication protocols used in the network such as NTP/SNMP/Telnet/ARP.

Sample Question:

Are only known authorised protocols permitted to execute?

Are appropriate protocol based filters applied at all boundaries/zones?

Web Protocols

Do HTTP proxies block all inbound scripts and Java applications?

2.4.4.3 Fault Management

Organisation needs to identify established procedures for addressing fault management processes; and processes for fault resolution.

Sample Question:

Is adequate redundancy ensured for critical networks? Where necessary, does this redundancy also extend to the ISP/TSP including their backhaul systems/networks?

Have appropriate security SLAs been incorporated for any outsourced fault management services?

2.4.4.4 Intrusion Detection/Prevention Systems (IDS/IPS)

Organisation needs to identify Intrusion Detection/Prevention devices/processes deployed within their network, along with security assurance of these devices themselves.

Sample Question:

Are adequate network-based IDS/IPS deployed, including between the control network and corporate networks?

2.4.4.5 Traffic & Services

Organisation needs to identify traffic and service management controls deployed within their networks.

Sample Question:

Is control system traffic given priority over any non-control system traffic?

Are control signals reporting mechanisms incorporated in the organisational SIEM?

2.4.4.6 Data Flow Control

Sample Question:

Is the DCOM protocol used only between the control network and the DMZ networks and is the protocol between the DMZ and the corporate network explicitly blocked?

2.4.4.7 Virtual Local Area Networks (VLANs)

Organisation needs to identify security controls applied for securing VLANs.

Sample Question:

Are VLANs effectively deployed, having each automation cell assigned to a single VLAN to limit un-necessary traffic and allow network devices on the same VLAN to span multiple switches?

2.4.4.8 Modems

Organisation needs to identify modems and security controls applied for securing modems.

Sample Question:

Are modems disconnected when not in use, and is there a timeout after a fixed period of inactivity?

2.4.4.9 Virtual Private Networks (VPNs)

Organisation needs to implement adequate security controls for VPNs.

2.4.4.10 Firewall

Organisation needs to identify firewalls and security controls applied for securing these firewalls. This includes:

2.4.4.10.1 General Firewall

2.4.4.10.2 Web Application Firewall (WAF)

2.4.4.10.3 Firewall Rules/Policies

2.4.5 Encryption

Organisation needs to identify appropriate usage of encryption to protect confidentiality of data during transitions and processes such as key management.

2.4.6 Configuration Management

Organisation needs to identify appropriate configuration management processes.

Sample Question:

Are initial configuration settings documented and held by a third party within the organisation?

Are change management procedures/policies well established and documented?

Is there a cohesive set of network/system architecture diagrams and other documentations including nodes, interfaces, and information flows?

2.4.7 Wireless Networks

Organisation needs to identify Wireless Networks and security controls applied for securing these Wireless Networks.

Sample Question:

Is the system scanned for unauthorized wireless access points at a specified frequency, and is appropriate action taken if such access points are discovered?

2.4.8 Network Management Systems (NMS)

Organisation needs to identify their network management systems and security controls associated with NMS.

Sample Question:

Are adequate security protocols implemented on NMS protocols (eg. Security implementation on SNMPv3)?

Are maintenance software tools used with care on system networks to ensure that system operations will not be degraded by their use?

2.4.9 Control System and Enterprise Network Security Coordination Process

Organisation needs to identify network security coordination processes for controls systems.

Sample Question:

Does the network security coordination process include a delineation of roles and responsibilities associated with coordination, communication, and accountability of information security on and between the control systems and enterprise networks?

2.4.10 Security Operation Centre (SOC)

Organisation needs to identify people, processes, and technologies associated with SOC.

Sample Question:

Are the SOC protocols perimeters and responsibilities adequately defined?

Is SOC management and reporting suitably insulated from the NOC?

Is there dedicated manpower assigned to SOC, including working on 24x7x365 basis?

2.5. **Services**

Organisation needs to identify the services: services being used and the services being provided, along with existing cyber security controls.

2.5.1 System and Services Acquisition

Security controls applied under “Systems” category (“System Procurement Standards or Services Acquisition”) may be referred here.

2.5.2 Service Hardening/ Least Functionality

Organisation needs to identify existing service hardening controls.

Sample Question:

Are unused administrative utilities, diagnostics, network management tools, and system management functions disabled?

2.5.3 Continuity

Organisation needs to identify all service continuity processes, such as disaster recovery, backup, and restoration.

Sample Question:

Do alternate telecommunications services avoid sharing a single point of failure with primary telecommunications services (e.g., radio and lease lines)?

2.5.4 Cross-Organization

Identify service sharing/linkages/dependencies on other organisations.

Sample Question:

Does the organization share services with other organizations and coordinate audit information transmitted across organizational boundaries?

2.5.5 Personnel

Organisation needs to identify personnel risk assessment/mitigation processes applied for security of its services.

Sample Question:

Are the results of personnel risk assessments documented, and are personnel risk assessments of contractor and service vendor personnel conducted pursuant to Standard?

2.6. **Criticalities**

Organisation needs to identify criticalities of their CII. This includes the following:

2.6.1 Details of CII identified by the Organisation

2.6.2 Vulnerability/Threat/Risk (VTR) analysis on the CII

2.6.3 Details of Security Control applied to mitigate VTR

2.6.4 Details of Residual Risk acceptable in terms of CII

2.6.5 Details of identified Incoming and Outgoing dependencies of CII

2.6.6 Details of CII reported to NCIIPC after approval from regulatory body/ministry for initiating process of notification of CII

2.6.7 Details of mechanism applied of sharing the vulnerabilities identified with NCIIPC for cross sectoral reporting

2.7. **Interdependencies**

Organisation needs to identify its dependencies on other organisations, risk associated and security controls considered:

2.7.1 Cross-Organization

Identify service dependencies on other organisations.

Sample Question:

Does the organization share services with other organizations and coordinate audit information transmitted across organizational boundaries?

2.7.2 Continuity

Organisation needs to identify its business dependencies on other organisations.

Sample Question:

Do alternate telecommunications services avoid sharing a single point of failure with primary telecommunications services (e.g., radio and lease lines)?

2.7.3 Outsourcing

Sample Question:

Does Security Policy/Procedure exist for outsourcing?

Has SLA compliance with the security policy been ensured?

2.7.4 Supply Chain Protection

Organisation needs to identify the complete supply chain of its cyber resources and the existing security controls applied to prevent any supply-chain contamination.

Sample Question:

Are supply chain vulnerabilities protected from threats initiated against organizations, people, information, and resources that provide products or services to the organization?

2.7.5 Service acquisition contracts/SLA

Sample Question:

Are formal contractual and confidentiality agreements established for hiring service from the external parties?

2.7.6 Vendors/contractors/ Personnel

Sample Question:

Are the results of personnel risk assessments documented, and are personnel risk assessments of contractor and service vendor personnel conducted pursuant to Standard?

2.8. **Asset Owners**

Organisation should identify asset owners, associated processes, risks and security considered. This includes:

2.8.1 Personnel

Sample Question:

Are documents and data files in the terminated employee's possession transferred to new authorized owners?

2.8.2 Roles & Responsibilities

Sample Question:

Does the cyber-security team establish and document a framework in accordance with company policy that defines the security organization and the roles, responsibilities, and accountabilities of the system owners and users?

2.8.3 Asset Location

Sample Question:

Are the risks associated with physical and environmental hazards considered while planning new system facilities or reviewing existing facilities?

Have necessary risk mitigation processes employed for such physical and environmental hazards?

2.8.4 Configuration Management

2.8.4.1 Asset Inventory

Sample Question:

Has an inventory of the components of the system been developed, documented and maintained that accurately reflects the current system?

Has an inventory of the components of the system been developed, documented, and maintained?

Does the asset inventory include information deemed necessary to achieve effective property accountability?

3. PHASE-II: Assess/Evaluate Vulnerabilities/Threats/Risks

This phase/step involves assessment/evaluation of the Security Controls (technological and/or procedural) identified in above phase/step.

3.1. Evaluate Vulnerability-Threat-Risk Assessment

Organisation needs to evaluate their Vulnerability-Threat-Risk assessments reports on basis of which the existing security controls have been implemented for protecting the infrastructure. The reports need to be checked for correctness, consistency and completeness considering the topics/categories and subcategories as mentioned for Phase-I.

3.2. Evaluate Network Architecture (with Security Devices in place)

This step is to be considered in conjunction with the above step. The existing Network Architecture (with security devices in place) needs to be evaluated for correctness, consistency and completeness considering the topics/categories and subcategories as mentioned for Phase-I.

3.3. Evaluate International Standards applied

Organisation needs to evaluate correctness, consistency and completeness of security controls identified in Phase-I with respect to security controls mentioned in the International Standards adopted. For example, organisations might have considered an ISO 27001 standards or North American Electric Reliability Corporation (NERC) or National Institute of Standards and Technology (NIST).

3.4. Evaluate Organisational Policies

Organisation needs to evaluate correctness, consistency and completeness of their Security Policies with respect to standards such as ISO 27001, North American Electric Reliability Corporation (NERC), National Institute of

Standards and Technology (NIST) etc. Organisations may evaluate whether their set of security policy covers following:

3.4.1 Security Policy

3.4.2 Information Security Policy

3.4.3 System Security Policy

3.4.4 Planning Policy

3.4.5 Personnel Security Policy

3.4.6 Physical and Environmental Policy

3.4.7 System and Services Acquisition Policy

3.4.8 Configuration Management Policy

3.4.9 System and Communication Protection Policy

3.4.10 Information and Document Management Policy

3.4.11 Maintenance Policy

3.4.12 Email Security Policy

3.4.13 Awareness and Training Policy

3.4.14 Incident Response Policy

3.4.15 Media Protection Policy & Procedures

3.4.16 System Control and Integrity Policy

3.4.17 Access Control Policy

3.4.17.1 Remote Access Policy & Procedures

3.4.17.2 Account Management Policy & Procedures

3.4.17.3 Identification and Authentication Policy & Procedures

3.4.18 Audit and Accountability Policy

3.4.19 Monitoring and Review Policy

3.4.20 Security Assessment Policy

3.4.21 Cryptographic Policy

3.4.22 Risk Assessment Policy

3.4.23 Portable Media Policy

3.4.24 Wireless Network Policy

3.4.25 Mobile Phone Policy

3.4.26 Malicious Code Protection Policy

3.4.27 CDA (Critical Digital Assets) Policy & Procedures

3.4.28 Change Control Policy & Procedures

3.4.29 Contingency Policy & Procedures

3.4.30 BCP(Business Continuity Plan) Policy & Procedures

3.4.31 Crisis Management Plan (CMP)

3.4.32 Cloud Computing Security Policy

3.4.33 SCADA and ICS Specific Policy

3.4.34 IT (Information Technology) and OT (Operation Technology) Sub-policies

3.5. Human Resource Management Policies Specific to Cyber Security Controls

Organisation needs to evaluate correctness, consistency and completeness of their Human Resource Management Policies in terms of cyber security perspective.

Following parameters/clauses may also be checked:

3.5.1 Personnel

Sample Question:

Has risk designations been assigned to all positions and are screening criteria established for individuals filling those positions?

3.5.1.1. Personnel Screening

3.5.1.2. Personnel Termination

3.5.1.3. Personnel Accountability

Sample Question:

Does a formal accountability process exist that clearly documents potential disciplinary actions for failing to comply?

3.5.2. Access Agreements

Sample Question:

Is access to classified information with special protection measures granted only to individuals who have a valid access authorization that is demonstrated by assigned official government duties?

3.5.3. Training & Awareness

3.5.3.1. Training Requirements

3.5.3.2. Security Awareness

3.5.3.3. Security Training

Sample Question:

Does training cover all levels / designations of personnel?

Does the frequency and depth of training reflect the role of the individual?

3.5.3.4. Training Records

3.5.3.5. Security Groups

3.5.3.6. Technical Training

3.5.3.7. Incident Response Training

3.5.3.8. Awareness Training

3.5.3.9. General Training

3.5.3.10. Specialized Training

3.5.3.11. Cross-Functional Team

Sample Question:

Does the CST include a member of the information technology staff, an instrumentation and control system engineer, a control system operator, a subject matter expert in cyber security, and a member of the management staff?

3.5.3.12. Situation Awareness

3.5.3.13. Contingency Training

Sample Question:

Does the organization provide contingency training to system users of their contingency role and responsibility in recovery? Also when contingency plans change and are they done within a predetermined time allowance?

3.6. **Compliance**

Organisation needs to evaluate correctness, consistency and completeness of their cyber security audit process for compliance check. Following parameters/clauses may also be assessed:

3.6.1 Audit and Accountability

3.6.1.1. Auditable Events List

Sample Question:

Is execution of privileged functions (account creations, modifications, and object permission changes) included in the list of events to be audited by the system?

3.6.1.2. Audit Generation

Sample Question:

Are audit records produced that contain sufficient information to establish what events occurred, when the events occurred, where the events occurred, the sources of the events, and the outcomes of the events?

3.6.1.3. Audit Protection General

Sample Question:

Is compliance to the security policy demonstrated through audits in accordance with the audit program?

3.6.1.4. Audit Failure Response

Sample Question:

Does the response to audit failures include using an external system to provide these capabilities?

3.6.1.5. Audit Monitor/Analysis

Sample Question:

Is the auditing capability implemented on NHMIs to ensure that all operator activity is recorded and monitored by authorized and qualified personnel and are historical records maintained?

3.6.1.6. Protection of Audit Information

3.6.1.7. Information Disclosure

Example: Non Disclosure Agreement by Auditors

3.6.1.8. Frequency of Audits

3.7. **Procedures**

Organisation needs to evaluate correctness, consistency and completeness of their security procedures. Following parameters/clauses may also be checked:

3.7.1. Implementation and Management of SOC/NOC

3.7.1.1. Audit and Accountability

Sample Question:

Is analysis of audit records integrated with analysis of performance and network monitoring information to identify inappropriate or unusual activity?

Is extra care taken to ensure that automated scanning tools used on the business networks do not scan the ICS network by mistake?

3.7.1.2. Audit (Events) Generation

3.7.1.3. Audit (Events) Alerts and Monitoring

3.7.1.4. Logging

Sample Question:

Does logging include, but is not limited to, critical host file changes, unauthorized and authorized client connection activity, and ad-hoc network creation?

3.7.2. Monitoring Physical Access

Sample Question:

Does the organization employ automated mechanisms to recognize classes/types of intrusions and initiate response actions?

3.8. Business Continuity Plan/Disaster Recovery

Organisation needs to evaluate correctness, consistency and completeness of their Business Continuity Plan. Following parameters/clauses may also be checked:

3.8.1. Continuity of Operations Plan

Sample Question:

Does the continuity of operations plan address the issue of maintaining or re-establishing production in case of an undesirable interruption for the system?

Do designated officials review and approve the continuity of operations plan?

3.8.2. System Backup

Sample Question:

Are backups of critical system software, applications, and data created and secured?

3.8.3. Contingency Plan

Sample Question:

Is normal operation of the system resumed in accordance with its policies and procedures after a security event?

3.8.4. Alternate Storage Site

Sample Question: Is alternate storage sites identified and are agreements in place to permit the storage of system configuration information?

3.8.5. Alternative Command and Control Methods

Sample Question:

Are alternate command/control methods identified, and are agreements in place to permit the resumption of operations within a defined time period when the primary system capabilities are unavailable?

Are necessary communications for the alternate control centre identified, and are agreements in place to permit the resumption of system operations for critical functions within a defined time period when the primary control centre is unavailable?

3.8.6. Disaster Recovery

Sample Question:

Is there a capability to recover and reconstitute the system to a known secure state after a disruption, compromise, or failure?

3.8.7. Fail-Safe Response

Sample Question:

Is the system able to execute an appropriate fail-safe procedure upon the loss of communications with the system or the loss of the system itself?

3.8.8. Continuity of Operations Plan Update

Sample Question:

Are updates to the recovery plan(s) communicated to personnel responsible for the activation and implementation of the recovery plan(s) within 30 calendar days of the change being completed?

3.8.9. Info System Recovery

Sample Question:

Does the organization protect backup and restoration hardware, firmware, and software?

3.8.10. Denial of Service Protection

Sample Question:

Does the organization employ monitoring tools to detect indicators of denial of service attacks against the information system and monitors system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks?

4. PHASE-III: Implement Security Controls

4.1. It is expected that each Critical Information Infrastructure organisation will undertake this exercise in the spirit of an accurate self assessment of their existing cyber security status. Obviously, the specific questions, areas covered etc are largely organisation and sector specific.

4.2. It is expected that the findings would be recorded for the organisation as a whole, rather than across segments or verticals within an organisation. This is a key part of the entire exercise in order to ensure that the senior most management has a view of the Organisational security posture, rather than a segmented / fractured view as normally seen.

4.3. It is expected that organizations from the Critical sectors would share their findings with the NCIIPC alongwith their plans for ensuring that their cyber security posture is maintained at the appropriate level.

4.4. Based on findings the Organisation needs to device and implement security controls for improving the cyber security posture.

5. PHASE-IV: Verify Implementation of Security Controls

5.1. To check effectiveness of the security controls implemented in the above step, organisations must conduct Cyber Security Audit.

5.2. Audit reports are expected to be shared with NCIIPC, as it would help in ensuring that their cyber security controls have been implemented at the appropriate levels.

6. PHASE-V: Ensure Compliance to Audit

6.1. The compliance of cyber security audit conducted is required to be done diligently.

6.2. Residual Risks must be properly documented and sign off of senior management be obtained.

6.3. Compliance reports are expected to be shared with NCIIPC, as risks accepted by the organisation are to be evaluated considering the CII aspect and dependencies amongst other critical sectors/organisations.

7. Conclusion

7.1. While a large amount of literature outlining processes and procedures required to achieve desirable levels of cyber security exists, there is a need to provide a clear assessment to senior management regarding their present status and effectiveness.

7.2. As brought out in the introduction, this framework is a support mechanism aimed at providing insight into the steady state cyber security deployment and operations within an organisation.

7.3. NCIIPC is available throughout this evaluation exercise for providing any assistance required.