SUGGESTED ROLES AND RESPONSIBILITIES OF CISO

To effectively perform his/her duties it is recommended that CISO should possess the following:

(a) Management capabilities ;

(b) Strategic planning abilities

(c) Knowledge of relevant legislative or regulatory requirements such as IT Act and associated Rules and

(d) Some competence/exposure in the field of information security;

(e) Good communication and writing skills.

CISO's roles and responsibilities may include but not limited to the following:

Strategic Planning

Suggested responsibilities under this role are:

1. Seek top management support and direction for implementing information security measures in the organization.
2. Identify information security goals and objectives consistent with organization business need/objectives
3. Define the scope and boundaries of the information security program.
4. Understand legal and regulatory requirement.
5. Define information security implementation strategies.
6. Estimate budget and resources required.
7. Plan and establish organization-wide Information security Management System (ISMS) in accordance with ISO/IEC 27001 Standard, directions and advice of NCIIPC and other relevant security standards.
8. Define risk management framework.
9. Define information security measurement metrics and other key performance indicators.
10. Get approval for information security plan, budget and resources from top management.

Policy Planning

Suggested responsibilities under this role are:

1. Identify information security polices, standards, procedures, guidelines and processes
2. Define formal process for creating, documenting, reviewing, updating, and implementing security policies.
3. Define information security policy.
4. Define policy for classification of information and information as sets.
5. Lead and coordinate development of organization specific information security policies, procedures, guideline and processes in consultation with various stake holders including NCIIPC.
6. Get approval of information security policies, procedures, guidelines and processes.

Information Security Management

Responsibilities under this role are:

1. Assist in developing, maintaining, reviewing and improving strategic organization-wide information security and risk management plan.
2. Disseminate information security policies, procedures and guideline to all concerned.
3. Enforce implementation of approved information security policies, procedures, guideline and ISMS etc.
4. Integrate information security procedures with organization's business processes.
5. Ensure that information security considerations are integrated with IT system planning, development / acquisition life cycle.
6. Periodically evaluate and review effectiveness of information security policies, procedures, standards, guideline and processes, ISMS etc.
7. Issue alerts and advisories with respect to new vulnerabilities / threats to all concerned.
8. Perform risk assessment steps like: (a) identify and make inventory of assets within the scope of information security plan; (b) identify and document threats to those assets; (c) perform vulnerability analysis; (d) perform impact analysis; (e) evaluate level of risk; (f) determine acceptability or treatment of risk based on risk acceptance criteria.
9. Perform risk treatment like: (a) Identify appropriate 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.
10. Implement automated and continuous monitoring of security incidents.
11. Maintain a record of information security incidents and breaches.
12. Take remedial action to reduce / diminish the impact of information security incidents and breaches.
13. Share management approval report on information security and breaches

with NCIIPC

14. Ensure compliance with legal and regulatory requirements for information security.
15. Raise information security awareness among management, employees, contractors and other stake holders.
16. Provide role based training on information security to the workforce.
17. Evaluate effectiveness of training & awareness program and continuously upgrade it.
18. Coordinate and lead in implementation of 'Business Continuity Plan (BCP)'.
19. Periodically conduct mock drill to evaluate effectiveness of business continuity plan.
20. Define and implement change management plan for both the change in information systems and the change in ISMS itself.
21. Ensure compliance of information security by contractors/suppliers etc.

Other responsibilities may include:

1. Ensure that before issuing NOC (No Objection Certificate) to the employee, who has resigned or has been terminated or is leaving organization, all equipments have been taken back and all his accounts either have been deleted or their passwords have been changed.
2. Maintain an information and communication technology (ICT) as set register containing details of asset, its owner and its security classification.
3. Ensure that all storage media, when no longer required, are disposed security and safely as per laid down procedures.
4. Ensure safety and security of portable computing devices/storage media when they are taken outside of the organization.
5. Ensure all information systems with organization are adequately patched and updated.

Information Security Auditing

Suggested responsibilities under this role are:

1. Periodically evaluate and review effectiveness of Information Security Management System.
2. Evaluate compliance with respect to legal and regulatory requirement for information security.
3. Evaluate compliance with respect to organization specific information security policies, procedures, standards, guidelines and directives & advice of NCIIPC.
4. Perform information security audit at least annually or whenever significant changes have been made in IT systems/ Infrastructure.
5. Prepare information security audit report along with recommendations for improving information security.
6. Obtain senior management approval of information security audit report.
7. Send a copy of management approved audit report periodically to NCIIPC.

National Critical Information Infrastructure Protection Centre

Block No. 3 Old JNU Campus, New Delhi 110067
Toll Free No.: 1800-11-4430
Email: helpdesk1@nciipc.gov.in;
helpdesk2@nciipc.gov.in

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

Roles and Responsibilities of Chief Information Security Officers (CISOs) of Critical Sectors in India

2015