Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations

CISO to be appointed in each Ministry/Department/Organisation

- With the rapid digitalisation of functions and processes of Government/Government organizations, the need for adopting secure cyber practices is becoming extremely important.
- A cyber breach can cause severe financial damage, and bring the functioning of Government/Government organisations to standstill.
- It is therefore imperative, that every organisation involved in the use of Information Technology in the discharge of its functions must identify and document its Information Security (IS) requirements that arise from various sources including the following sources:

- An assessment of risks (RA) to the organisation in the context of the organisation's business strategy and objectives; through which threats to an organisation's information assets are identified, vulnerabilities and likelihood of occurrence are evaluated and their potential impact is estimated;
- The legal, statutory, regulatory and contractual requirements that an organisation, its trading partners, contractors and service providers have to fulfil;
- The set of principles, objectives and business requirements for Information handling, processing, storing, communicating and archiving that are developed for Operations Support in an organization.

- Organisations must identify and implement an Information Security Management System (ISMS) that encompasses Cyber Security as well as physical and logical security controls for risk mitigation as appropriate, to protect the organisation from business harm resulting from information security issues or cyber crises.

- To ensure a structured mechanism, in accordance with best information security system practices, the Ministry of Electronics and IT has advised all Ministries/Departments to nominate a Chief Information Security Officer (CISO) for the Ministry/Department and also advise similar action to Chief Executives/Heads of Government organizations including PSUs/Autonomous Bodies/Attached Offices/ Statutory Bodies under their control. It shall be the responsibility of Secretary of the Ministry/Department (CEO/Head in case of organizations) to identify a member of senior management as a 'Chief Information Security Officer (CISO)' to establish a cyber security program, coordinate security policy compliance efforts across the organisation and interact regularly with CERT-In 'Point of Contact'.

- The CISO must be given the mandate and resources to establish an Information Security program, coordinate security policy compliance efforts across the organisation and interact regularly with regulatory agencies such as CERT-In.

- The CISO shall preferably report to the Secretary of the Ministry/Department (CEO/Head in case of organisations). If for some reason, that is not possible, CISO must report directly to next seniormost person in the Ministry/Department (CEO/Head in case of organisations)

Roles and Responsibilities of CISOs

- Maintaining and updating the threat landscape for the organisation on a regular basis including staying up to date about the latest security threat environment and related technology developments.
- Establishing a cyber security program and business continuity programme and for drafting of various security policies e.g., Information security policy, Data governance and classification policy, Access control policy, Acceptable use of assets and asset management, Risk assessment and risk treatment methodology, Statement of Applicability, Risk management framework including third parties, Cryptography, Communications security, Information Security awareness programs for all personnel in the organisation and Incident management.

- Ensuring review of the Information Security Policy by internal and/or external subject matter experts to check for the adequacy and effectiveness of the ISMS programme
- Reviewing and updating the cyber security policy documents.
- Defining rules for secure and acceptable use of communication channels for the business requirements of the department/organization.

- Developing and implementing a security architecture for the organisation by leveraging technology and understanding of threat landscape.
- Establishing and reviewing the Risk Assessment methodology and selection of appropriate controls for risk mitigation by leveraging technology and an understanding of the threat landscape in the organisation.
- Interacting with regulatory bodies and external agencies that could be of help to maintain information security for the organization, e.g. CERT-In

- Ensuring that the following activities are carried out at regular intervals, either directly or through the deployment of subject matter experts

- Log review, analysis and exception reporting
- Vulnerability Assessment & Penetration Testing (VAPT) of all websites, portals and IT systems, on a quarterly basis at a minimum; ensuring that websites are GIGW compliant
- Web Application Security Assessment (WASA) and white-listing of all web applications in use by the organisation, annually at a minimum
- Software Development Lifecycle (SDLC) Audit and periodic Code Reviews to ensure that applications continue to be secure
- Information Security Audit of IT Systems and controls, including site audits as appropriate, where online operations span multiple locations. The audit should ensure the following:

- No unsupported operating systems are in use in the department
- CISO prescribed hardening guidelines, patch management guidelines, anti virus / malware guidelines, no privilege access on endpoints, regular review of access privileges, acceptable configuration guidelines and procedures are properly implemented;
- Ensure defined principles of secure software development process is followed for all software applications and the same is reflected in contracts, if software development is outsourced;
- Citizen / customer data privacy to be ensured in case if citizen / customer data is captured and maintained;

- Periodic assessment / audits of third party service providers to assess risks to you organisation;
- Certify that the time synchronisation of the Network Time Protocol in the organisation has been done with the National Physical Laboratory.
- Issuing and periodic review of device hardening guidelines, patch management guidelines, anti-virus / malware guidelines, User Access Management guidelines, privilege access management guidelines, end point management guidelines, connectivity guidelines for Trading partners and external agencies, controls on mobile devices and wireless technology

- Authorising an Acceptable Use policy for software packages and freeware in consonance with the organisation's risk/threat landscape, business objectives and Security Policy & Procedures
- Adopting a suitable IT Governance framework for implementing supporting processes such as Configuration Management, Change Management, Incident Management and Problem Management etc. CISO should ensure that appropriate instructions are issued for adherence to processes within the organisation and that no authorised changes are carried out to online systems without specific Change Approval.
- Ensuring that the IT infrastructure deployed for online operations is kept up to date as per policy and is always under maintenance and technical support so that security patches and bug fixes are regularly applied to protect the infrastructure from vulnerabilities.
- Ensuring that clauses pertaining to Information Security are incorporated into contracts/agreements/MoUs with service providers.

- Securing senior management approval for emergent/urgent procurements necessary to keep the infrastructure safe from attacks and exploits
- Developing and Implementation of scenario-based Incident Response plans to deal with Cyber crises, contingencies and disasters, attack on IT systems etc. This should include incident containment, assessment, root cause analysis, mitigation/ prevention, continuous monitoring, forensics and reporting as required. This should include the following:

- Ensuring that Incidents, especially repeat incidents are investigated and corrective action taken as identified through a comprehensive Root Cause Analysis (RCA)
- Ensuring that information security incidents are reported to CERT-In

- Coordination with stakeholders in all matters related to internal and external security and covering the following aspects:

- Assessing the adequacy of controls for Confidentiality, Integrity and Availability of all the Information Systems;
- Explaining exceptions, if any, to security policies and procedures along with the risk to business;
- Systematically identifying and managing security risks from an end-to-end perspective on a periodic basis;
- Assessment of the maturity and effectiveness of the security program;
- Steps proposed to remediate gaps identified, if any; and
- Impact of the incidents and breaches on the organisation from a business perspective.

- Establishing a Cyber Crisis Management Group with the head of organisation (or his appointed representative) as its Chairman and to prepare a list of contact persons to be contacted during crisis e.g. internal: financial, personnel etc. and external: law enforcement agencies, CERT-In etc. complete with up-to-date contact details. CCMG should authorise a Cyber Crisis Management Plan (CCMP) outlining roles and responsibilities of organisational stakeholders. Implementing the CCMP, including security best practices and specific action points:

- Planning and executing periodic disaster recovery drills/simulation exercises in order to establish the adequacy of the Business Continuity Plan
- Ensuring that periodic tests are conducted to evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks as well as after any major incident
- Where the geographical spread of IT Systems and online operations spans multiple locations across the country, identifying personnel responsible for implementation of information security at the local level as well as for periodic reporting as required to the CISO.

- Coordinating all matters related to security internally and externally while providing regular reports to the head of the organisation covering the following aspects:

- Assessing the adequacy of controls for confidentiality, integrity and availability of all the information systems;
- Explaining exceptions, if any, to security policies and procedures along with the risk to business;
- Systematically identify and manage security risks from an end to end perspective on a periodic basis;
- Assessment of the maturity and effectiveness of the security program;
- Steps proposed to remediate gaps identified, if any; and
- Impact of the incidents and breaches on the organisation from a business perspective.

- Develop and implement ICT disaster recovery and security incident management processes, which consists of following activities:

- To coordinate response to security incidents;
- To prepare evidence for legal action following an incident; and
- To comply with the security suggestions provided to them in incidents' analysis' reports;
- To analyze incidents in order to prevent their recurrence; and
- To report information about security incidents without delay to CERT-In.

Thank You