# 3. INFORMATION SECURITY GOVERNANCE

***Great changes may not happen right away, but with effort even the difficult may become easy !***
***~ Bill Blackman***

Information security involves a wide range of activities including risk identification, protecting citizens' data, disaster recovery, training and education. In order to achieve the information security objectives of government organizations, regardless of size of the organization, there is a need to have clearly defined information security governance framework.

**OBJECTIVE**

To define roles and responsibilities that are essential to the implementation of information security.

Governance specifies the accountability framework and provides oversight to ensure that information security is properly managed within the organization to ensure that adequate protection is available to information assets. Roles and responsibilities of the staff should be clearly defined, and Head of the Organization is ultimately responsible for managing and governing information security activities in their respective organizations. However, designated representatives including Information Security Officers, Chief Innovative Officers, and all other staff have distinct roles to play as specified in this Chapter to accomplish the information security objectives.

## 3.1. Roles and Responsibilities

### 3.1.1. Head of the Organization - HOO

> ***Policy Statement 1:***
>
> ***Head of the Organization Should Provide the Leadership to Information Security Activities.***
> *Applicable to all organizations*

3.1.1.1. Head of the Organization (HOO) must provide the leadership for all information security related activities within the organization.

3.1.1.2. HOO shall be accountable for the security of the information assets, systems, and other digital infrastructure within the organization.

3.1.1.3. HOO shall be overall responsible in implementing the Information Security Policy in the organization.

3.1.1.4. HOO shall give the leadership to create and maintain a Security Culture within in the organization. Failure to develop and maintain a security culture where users are complying with guidelines for the systems and resources they are using can increase the risk of a system user unwittingly assisting with an attack against the system.

3.1.1.5. HOO should provide the leadership to create an information security culture within the organization, where users comply with information security policies and guidelines, and work proactively towards protection of information and systems they use.

3.1.1.6. HOO must nominate a suitable Information Security Officer (ISO) and an Assistant Information Security Officer (AISO) for the organization. Refer Section XYZ.

3.1.1.7. HOO must establish an Information Security Committee (ISC) and Risk Management Committee (RMC) for the organization as specified in the Section XYZ.

3.1.1.8. HOO shall ensure that everyone in the organization from the top to down receive appropriate cyber security education and awareness training.


3.1.1.9. HOO shall allocate resources (Budget, Human Resource and other facilities) to ensure information security in the organization and to build the capacity of ISO, CIO, AISO, and other relevant staff in relation to cyber security.

### 3.1.2. Information Security Organizational Structure

3.1.2.1. HOO shall establish an Information Security Organizational Substructure for the organization. Such substructure is essential to execute, direct and manage information security activities of the organization, and to protect organization against information security breaches, intrusions and interruptions.

***Policy Statement 2:***

***Organization Should Establish an Information Security Organizational Structure.***
*Applicable to all organizations.*

3.1.2.2. Effective information security organizational substructure should include key roles such as (1) Information Security Officer-ISO, (2) Chief Innovation Officer-CIO, (3) Chief Internal Auditor-CIA, and (4) Associate Information Security Officer - AISO. Figure 1 presents an overview of the secure organizational structure. Roles and Responsibilities of each position is presented in the Section XYZ.

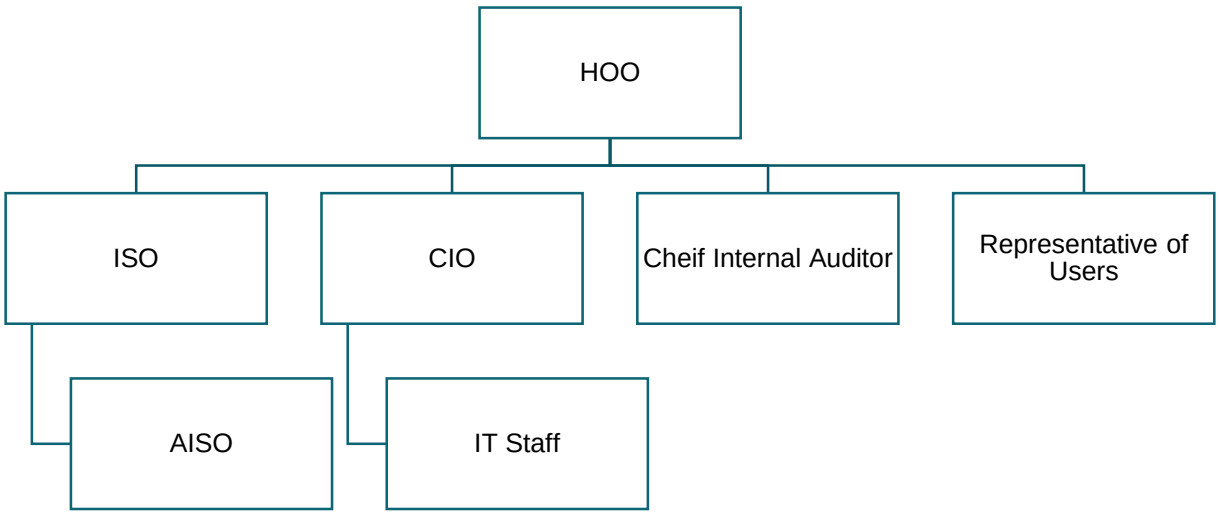


Figure 1. Secure organizational substructure

3.1.2.3. Head of the Organization should appoint (1) an Information Security Committee (ISC), and (2) a Risk Management Committee (RMC) to provide strategic directions information security policy implementations. Information Security Officer and Chief Internal Auditor should directly report to the Head of the Organization with regards to the activities in relation to information security. Roles and Responsibilities of the are presented in the Section XYZ.

### 3.1.3. Information Security Officer - ISO

3.1.3.1. As per the Circular MDIIT/SEC/2019/CS001 (date: 23-05-2019) of the Ministry of Digital Infrastructure and Information Technology, the HOO shall appoint an ISO to the government organization. Criteria for the selection of ISO is stipulated in the Annex XYZ.

***Policy Statement 2.1***

***Organization Should Appoint an Information Security Officer for the Organization.***

*Applicable to all organizations*

3.1.3.2. In the case of where there is no suitable officer to be appointed as the ISO, the CIO (or the person in charge of the subject of IT) should be assigned with information security responsibilities and accountabilities.

**Information Security Officer** is a senior-level executive responsible for establishing and maintaining the organizations objectives, strategy, and action plans to ensure information assets are adequately protected.

*Box 3B*

3.1.3.3. ISO shall be the Secretary to the ISC (Information Security Committee) and shall directly report to HOO. ISO shall serve as the principal advisor to the HOO and the organization on all matters relating to the security of the organization.

3.1.3.4. ISO should be assigned with information security responsibilities and accountabilities.

3.1.3.5. ISO shall develop information security objectives for the organization, and shall develop a strategic information security program and actions plans for the organization with the aim of protecting information assets, computer systems and infrastructure. The information security program must comply with the Information Security Policy of Government Organizations.

3.1.3.6. The ISO is responsible for communications between general staff, ICT staff and business personnel to ensure alignment of organizational objectives and security objectives within the organization.

**Information Security Officer's** role generally needs to be separated from the IT department. ISO should directly report to the HOO, and shall not report to CIO.

*Box 3C*

3.1.3.7. The ISO shall be fully aware of information security incidents occurring within the organization and take appropriate measures to handle information security incidents as per the guidelines issued by the Sri Lanka CERT.

3.1.3.8. The ISO shall closely work with CIO, to ensure that information security considerations are integrated with IT system planning, development and acquisition life cycle.

3.1.3.9. The ISO shall work closely with the Sri Lanka CERT in all information and cyber security related matters.

3.1.3.10. The ISO shall be the officer for handling information security incidents for the organization (refer chapter XYZ for Incidents Response Planning).

3.1.3.11. ISO shall be a member of the RMC, shall be the responsible person for incidents Handling.

### 3.1.4. Assistant Information Security Officer - AISO

3.1.4.1. As per the Circular MDIIT/SEC/2019/CS001 (date: 23-05-2019) of the Ministry of Digital Infrastructure and Information Technology, the HOO shall appoint an Associate Information Security Officer (AISO) to the government organization. Criteria for the selection of AISO is stipulated in the Annex XYZ.

3.1.4.2. AISO is an executive, who is responsible handling technical matters in relation to cyber security, and executing strategic initiatives formulated by the ISO.

3.1.4.3. The main responsibility of an AISO is to implement and monitor security controls for the protection of information assets, computer systems, networks and other digital infrastructure of the organization. AISO should also facilitate IT staff to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.

### 3.1.5. Chief Innovation Officer – CIO

> ***Policy Statement 2.2***
>
> ***Organization Should Empower Chief Innovation Officer with Information Security.***
> *Applicable to all organizations*

3.1.5.1. The Chief Innovation Officer (Director IT or the officer responsible for the subject of IT) should be trained and empowered to implement information security controls to protect the organization's information, systems and other digital assets.

3.1.5.2. Chief Innovation Officer must ensure that information security risk is assessed and appropriate controls are implemented to mitigate risks, and disaster recovery procedures are developed, tested and adequately implemented.

3.1.5.3. In the case of organization does not have a suitable candidate to be appointed as Information Security Officer, the Chief Information Officer should be empowered to play the role of Information Security Officer.

### 3.1.6. Chief Internal Auditor – CIA

3.1.6.1. In addition to the generic functions performed by the Chief Internal Auditor (CIA), HOO shall assign additional responsibilities to CIA audit the implementation of information security initiatives in order to protect information assets (and other digital infrastructure).

> ***Policy Statement 2.3***
>
> ***Organizations Should Empower Chief Internal Auditor with Information Security.***
> *Applicable to CII*

3.1.6.2. Chief International Auditor should be assigned with the responsibilities for initiating and overseeing Information Security Audits of the organization, assessing the progress of adopting Information Security Policy and Baseline Security Standards, and reporting information security related findings to the Audit and Management Committee (AMC) for further actions.

3.1.6.3. Organization shall develop the capacity of the Chief Internal Auditors.

### 3.1.7. Information Asset Owners and Custodians

3.1.7.1. Organization should identify Asset Owners and Custodians. Asset Owner is senior executive level officer who has the responsibility for controlling the whole lifecycle of an asset.

> ***Policy Statement 7.3:***
>
> ***Organization should Identify Asset Owners and Custodians.***
>
> *Applicable to all organizations*

3.1.7.2. The Custodian of the information asset will be responsible for the protection of the asset and for implementing the controls (as identified and approved by the owner of the information asset) related to the protection of the asset.

3.1.7.3. Owner and Custodian is responsible for managing the entire lifecycle of the asset – from creation, modification to destruction.

3.1.7.4. The IAO is responsible for facilitating the Asset Classification process as specified in the Assets Classification Chapter to ensure that assets are appropriately classified and protected.

3.1.7.5. IAO is responsible for reviewing the access requests to information assets and shall authorized user access to information assets. Level of privileges allocated to users shall be authorized by the IAO.

3.1.7.6. IAO shall periodically review access controls placed on the information asset and update the controls whenever necessary. Special attention shall be paid when the sensitive assets are disposed (Refer Chapter Assets Protection for secure asset disposal).

### 3.1.8. Information Systems Users

3.1.8.1. System users comply with information security policies and procedures within their organization. Chapter 4 presents the user responsibilities in general.

## 3.2. Committees

### 3.2.1. Information Security Committee - ISC

3.2.1.1. To implement the Information Security Substructure for the organization, the HOO shall appoint an Information Security Committee (ICS) for the organization. The HOO shall chair the Committee and rest of the members of the committee shall include Information Security Office (ISO), Associate Information Security Officer (AISO), Chief Innovation Officer (CIO), and Chief Internal Auditor (CIA). ISO shall be the Secretary to the Committee.

***Policy Statement 2.4***

***Organization Should Establish an Information Security Committee.***
*Applicable to all organizations.*

**Information Security Committee** is responsible in leading and managing all Information Security related activities within the organization, including information security planning, funding, implementation and monitoring the implementation of information security measures.

*Box 3E*

3.2.1.2. ISC shall provide guidance and advice to ISO to perform his duties in relation to information security efficient and effective manner.

3.2.1.3. ISC shall bear the ultimate responsibility for all activities in relation to the information security.

3.2.1.4. ISC shall develop information security action plans for the government organizations, and ensure that adequate resources are allocated to implement the action plans.

3.2.1.5. The ISC must ensure that the organization has well-documented information security policies, incident response plans, disaster recovery plan, asset classification, information asset classification and data sharing policy, and or any other policies necessary for ensuring the information and cyber security of the government organization. ISC shall ensure that the government organization implements such initiatives adequately.

3.2.1.6. ISC shall ensure that government organization implements adequate controls to ensure the security, confidentiality, availability, and integrity of the information and security of IT systems and devices.

3.2.1.7. ISC shall act as the Steering Committee for Information Security activities.

### 3.2.2. Risk Management Committee - RMC

3.2.2.1. HOO shall appoint a Risk Management Committee (RMC) for the organization. Risk Management Committee is an independent committee which directly reports to the HOO. Risk Management Committee shall include ISO, Process Owners (sectional heads), and Information Asset Owners. Deputy Head of the Organization or senior executive officer shall be the chairperson of the Risk Management Committee.

> ***Policy Statement 2.5***
>
> ***Organization Should Establish a Risk Management Committee.***
> *Applicable to CII*

3.2.2.2. RMC is responsible for implementing the Risk Management Process for the organization as described in Chapter XYZ.

3.2.2.3. RMC shall develop the organization's risk profile and key areas of risk, in particular, in the area of information technology.

3.2.2.4. RMC shall identify key risk areas of the organization and identify specific risks to computers, information systems and digital infrastructure, and inform Information Security Committee (ISC) to implement necessary controls.

3.2.2.5. RMC shall develop and maintain Risk Register for the organization.

3.2.2.6. RMC shall develop a risk management plan for the organization and take the leadership in implementing the risk management plan.

## 3.3. Security in Job Definitions

3.3.1. Staff who were involved in information assets classified as Confidential and Sensitive must be assigned with specific documented responsibilities. ISC shall develop specific responsibilities of the staff and get the approval HOO.

3.3.2. Staff who are given information security roles must aware on the specific job roles and responsibilities. All the staff (including new staff) must have received any necessary briefings on security aspects before being granted access to information assets or systems.

3.3.3. For the staff who are dealing with information assets classified as Secret or Confidential must go through security clearance before they are appointed for a position or transferred to a position, and periodic security clearance checks.

> Staff who are dealing with information assets classified as Secret or Confidential must go through security clearance.
>
> *Box 3G*

3.3.4. Security clearance shall be applied on all types of employees including temporary personnel, contract personnel and third party service providers.

3.3.5. All supervisory roles (CIO, ISO, CIA) are responsible for the performance and conduct of the staff personnel reporting to them. With the support of ISO,

functional heads are required to assess the impact on the security of information resources to which the staff has access.

## 3.4. Capacity Building of Accountable Individuals

It is widely understood that 95% of the cyberattacks are due to human errors. Therefore, increasing information and cyber security skills across all types of employees of the organization is essential.

> ***Policy Statement 3***
>
> ***Organization Should Build the Capacity of the Accountable Individuals.***
> *Applicable to all organizations*

3.4.1. Information Security Officer (ISO) should ensure that security awareness and training are critical components of the information security action plan of a government organization.

3.4.2. Information Security Committee (ISC) should take appropriate actions to develop the information security capacity of staff accountable individuals (Assets Owners, Custodians, Head of the Organization, Information Security Officer, Associate Information Security Officers, Chief Innovation Officers, Chief Internal Officer) and the users at different levels through awareness and trainings. Awareness activities shall be carried to promote security and informs the staff of security activities. Training activities are essentials to produce relevant and needed security knowledge and skills within the government staff.

3.4.3. Information security capacity building shall be an ongoing activity of the government and it should be included in the annual training plan of the organization.

3.4.4. ISC must provide ongoing information security awareness and training for personnel on topics such as user responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures, incident reporting and handling, and potential security risks and counter-measures.


Awareness and knowledge degrades over time without ongoing refresher training and updates. Providing ongoing awareness and training will assist in keeping personnel aware of issues and their responsibilities

3.4.5. The government organization allocates sufficient time for new employees to review the guidelines, security policies, standards, and procedures.

3.4.6. With the support of Sri Lanka CERT, the organization shall assess the information security skills of employee frequently.

## 3.5. Strategic Alignment

3.5.1. Aligning information security activities with the organization's operational needs is essential to protect

***Policy Statement 4***

***Organization Should Align Information Security Objectives with Organizational Objectives.***
*Applicable to all organizations*

organization against information security breaches and intrusions.

3.5.2. ISO, in consultation with ISC and Functional Heads should therefore, analyze the organizational objectives to identify dependencies on information security, and then link information security objectives to overall organizational activities.

3.5.3. All information security strategies, programs, projects and activities of the government organization should be designed in a such a way that those initiatives are linked with organizations objectives.

## 3.6. Information Security Action Plans

3.6.1. Information Security Committee (ISC) should develop and implement Information Security Action Plans (long term, medium and short term plans) which spells out the way in which security is to be guaranteed in realizing the objectives of the organization.

***Policy Statement 5***

***Organization Should Develop an Information Security Action Plan***

*Applicable to all organizations*

3.6.2. Based on the information security priorities determined by a risk assessment, the organization should also allocate budget for information security activities in the action plans.

## 3.7. Comply with Information Security Policy

3.7.1. All the organizations should comply with the Information Security Policy for the Government Organizations. Sri Lanka CERT shall conduct annual information security readiness assessments to determine level of compliance, and the organization should facilitate Sri Lanka CERT to conduct the survey.

***Policy Statement 6***

***Organization Should Comply with Information Security Policy***

*Applicable to all organizations*

3.7.2. Head of the Organization is accountable for implementing the information security policy at organization.

## Notes