ISO 27001 Implementer's Forum

Guideline for Roles & Responsibilities in Information Asset Management

Document ID	ISMS/GL/	003	Classification	Internal Use Only
Version Number	Initial		Owner	
Issue Date	07-08-2009		Approved By	

SOME RIGHTS RESERVED

This work is copyright © 2009, **Mohan Kamat** **and** **ISO27k implementers' forum**, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.).

Title	Roles in Information Asset Management
Document ID	ISMS/GL/003
Date	07-08-2009
Status	**Initial**

Prepared By:	Mohan Kamat	07-08-2009
Reviewed By:		
Reviewed By:		
Approved By:		
Approved By:		

Distribution List	
Apex Committee	To approve and authorize
ISMS Forum	To review and update
All Department / Function Heads	To understand and comply

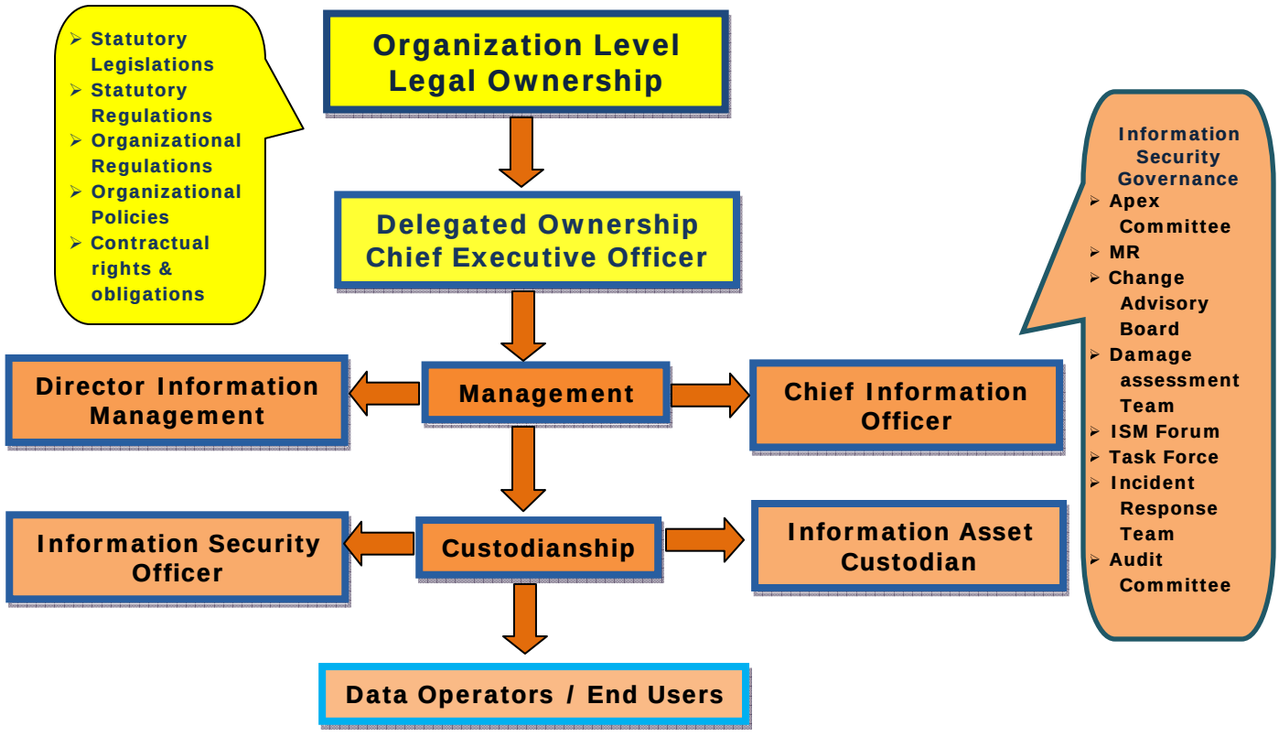
Amendment History

Version No	Page No	Details of Amendment	Amendment Date	Approved By

1. Overview

All information assets shall be managed at organization level. The ownership of the information assets shall reside with the organization and individuals shall be assigned and made responsible and accountable for the information assets. Specific Individuals shall be assigned with the ownership / custodianship / operational usage and support rights of the information assets.

2. Information Asset Management Roles



3. Information Asset Management Responsibilities

1. Legal Owner

The top management shall be legal owner of information asset. No individual can claim IP rights of an Information asset, unless and otherwise specifically agreed and approved by the management in contractual agreement.

2. Delegated Ownership

The CEO shall have authority to represent the organization for the protection and security of the information asset as ownership of Information assets is delegated to this organizational role. CEO shall approve the Information Management / Security Policy.

The CEO may delegate full / partial ownership along with the defined responsibilities to any officer / contractor / third party with operational rights and responsibility.

The responsibilities of the Asset owner are as follows:

- ✓ Updating of information asset inventory register;
- ✓ Identifying the classification level of information asset;
- ✓ Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;
- ✓ Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;
- ✓ Authorizing access to those who have a business need for the information, and
- ✓ Ensuring access is removed from those who no longer have a business need for the information.

3. Director Information Management

The Director, Information Management ensures that the information resources of organization are managed as a corporate asset and assists in establishing the strategic direction of information management for the organization. They provide support and leadership to officers and other directors responsible for managing information resources on a day-to-day basis.

The Director, Information Management shall

- ✓ provide specialist advice relating to information management practices
- ✓ contribute to the strategic direction of information management within the organization
- ✓ co-ordinate the development and implementation of information management practices including policies, standards, guidelines and procedures
- ✓ assist business units to define and understand their responsibilities in relation to information management
- ✓ assist business units to identify their information needs and requirements
- ✓ Work with the Chief Information Officer to plan and implement systems to effectively manage the agency's information assets.

4. Chief Information Officer

The CIO ensures that strategic planning processes are undertaken so that information requirements and supporting systems and infrastructure are aligned to legislative requirements and strategic goals. The CIO ensures that information security policies and governance practices are established to ensure the quality and integrity of the agency's information resources and supporting IT systems. They oversee the development of tools, systems and information technology infrastructure to maximise the access and use of an agency's information resources.

The Chief Information Officer is responsible for:

- ✓ interpreting the business and information needs and wants of the organization and translating them into ICT initiatives
- ✓ setting the strategic direction for information and communications technology and information management
- ✓ ensuring that ICT and information management investment is aligned to the strategic goals of the organization
- ✓ ensuring that projects and initiatives are aligned and coordinated to deliver the best value
- ✓ ensuring ICT planning is integrated into business planning
- ✓ identifying opportunities for information sharing and cross collaboration on projects and initiatives.

5. Information Security Officer

The information security officer is responsible for developing and implementing information security policy designed to protect information and any supporting

information systems from any unauthorised access, use, disclosure, corruption or destruction.

The information security officer shall:

- ✓ Develop policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with organizational *Information security* policy
- ✓ Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- ✓ Work with information custodians to ensure that information assets have been assigned appropriate security classifications.
- ✓ Maintenance and upkeep of the asset as defined by the asset owner
- ✓ System Restart and recovery
- ✓ Implementing any changes as per the change management procedure
- ✓ Backup of the information
- ✓ Updating of information asset inventory register;
- ✓ Identifying the classification level of information asset;
- ✓ Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;
- ✓ Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;
- ✓ Authorizing access to those who have a business need for the information, and
- ✓ Ensuring access is removed from those who no longer have a business need for the information.

6. Data Operators / End Users

Employees, Third Parties, Contractors authorized by the Owner / custodian to access information and use the safeguards established by the Owner / custodian. Being granted access to information does not imply or confer authority to grant other users access to that information.

The users are bound by the acceptable usage policy of the organization.