iNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 4.1

Information Security Management System

Aim

To equip students on basics of Information Security Management system (ISMS), its process and the roles and responsibilities of IT security

Instructional Objectives

After completing this chapter, you should be able to:

- Explain information security management system
- Describe performance optimization
- Elaborate on role and responsibility of IT security
- Explain the process of duty segregation in information security management

Introduction to Information Security Management

Importance of Information Security Management

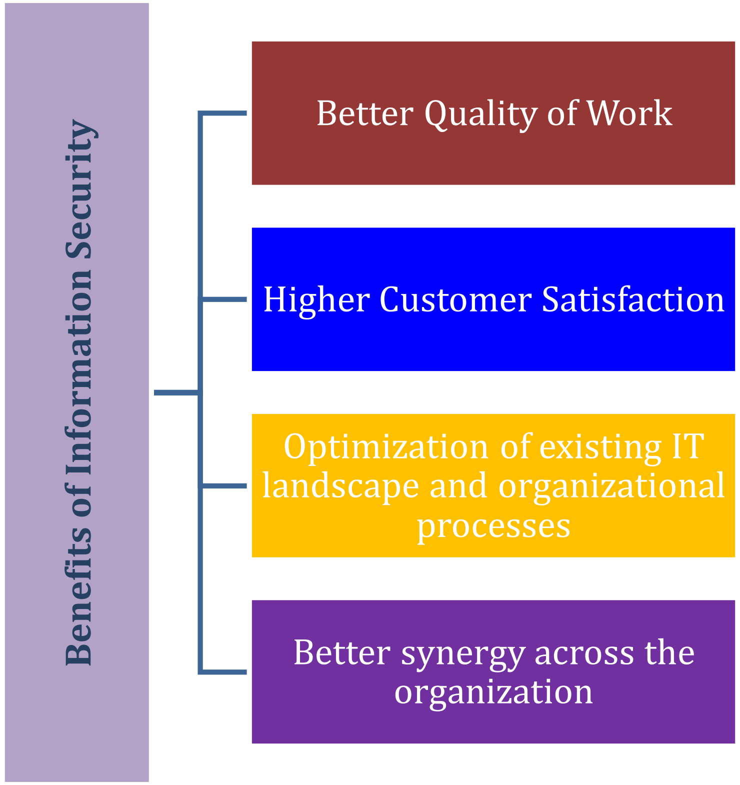
Information is of utmost importance to companies. Having access to the right information at the right time is the key for any business.

- Most of the companies are IT enabled businesses today.
- Data is created, stored, modified and transmitted through IT systems.
- It is very critical to safeguard the IT systems that we use today.
- IT security incidents have very high impact on business costing them billions of dollars.
- Information security is more about optimizing the information security management processes than information security technology.
- Though investments in information security technology will provide medium to long term benefits, maximum returns can be obtained by optimizing the information security processes and procedures that are implemented.

Benefits of Information Security

Long term benefits of Information Security Management include:

- Better Quality of Work
- Higher Customer Satisfaction and hence increased customer confidence
- Optimization of existing IT landscape and organizational processes
- Better synergy across the organization due to better integration of information security management in existing structures.


Benefits of Information Security
Better Quality of Work
Higher Customer Satisfaction
Optimization of existing IT landscape and organizational processes
Better synergy across the organization

Long term benefits of Information security

Information Security versus IT Security

Generally people assume that Information Security and IT Security are synonyms. However they are not. Let us look at this example to understand the difference between them:

Example: Assume that you have the perfect IT security mechanisms and software in place. But one malicious act by an administrator or staff can bring the whole IT system down – and this was not due to a software error but because of a malicious act of a staff member.

The IT system being down can lead to information not being available at the time of need. Hence information security is not just about IT systems but also about humans, paper documents or information stored, held, transferred, transmitted in any form.

Securing your IT systems against breach is just half the work done since information security comprises of physical security, human resources, legal protection, organization and its processes.

Information Security versus IT Security (contd)

From the previous example, we understand that:

- The purpose of information security is to build a structure or system that will take into account all kinds of risks and protects all the information assets (both IT and Non-IT) by implementing appropriate controls.
- ISO 27001:2013 is the latest ISO standard for Information security management. It provides a complete and comprehensive security implementation guideline.
- Guidelines is provided for all assets including hardware, software, suppliers, vendors, customers, data transmission and documentation.
- ISO 27002 lists about 133 controls, out of which just about 46% of them are IT related.

Quiz / Assessment

1. IT Security encompasses the security of ___________.

a) The IT Systems only

b) The IT Systems, human security, paper documents, information transfer, information in any form

c) All IT and Non-IT systems

d) Computer systems against virus attacks only

Quiz / Assessment

2. ________ is more about optimizing the information security management processes than information security technology.

a)Informative system

b)Information security

c)Internet access

d)Initial stages

Quiz / Assessment

3. __________ is a main threat to Information system.

a)Data process

b)Privacy enquiry

c)System approach

d)Computer theft

Performance Optimization

Performance Optimization - The ISMS Process

- ISO 27001 defines how to implement an information security management system for the organization.
- It is a strategic decision taken by the company based on its business and security requirements, its risk profile and appetite, controls and processes that are employed, the number of employees with the organization etc.
- ISO 27001 is a certifiable standard unlike ISO 31000 which was not meant for certification. Hence compliance to ISO 27001 can be assessed and certified.
- ISO 27002 is the list of all available controls for ISMS. These controls are very generic and can be adopted by any organization. ISO 27002 has 33 controls and the controls that are not in scope of the organization have to be declared up start in the statement of applicability.
- Just like any organization wide initiative, even for the implementation of ISMS, management support is vital. Management should provide active support by coming up with the required Information Security policies and procedures.

Performance Optimization -Steps in ISMS Process

1. Scope Definition -The first step in the ISMS process is the scope definition. The scope of the ISMS is defined based on the nature of business, the organization culture, structure, location, information assets and technology.

2. Draw up the Asset Inventory - The next step in the process is to come up with all the important information assets for the organization.

3. Risk Assessment - Once the assets are drawn up, the next step is to identify any risk to the information asset. The risks are identified, analyzed and prioritized against the risk profile.

4. Risk Treatment - The Risk Treatment Plan (RTP) should lie within the purview of the organizations' information security policy. This is the key document during the entire PDCA (Plan, Do, Check and Act) life cycle of ISMS.

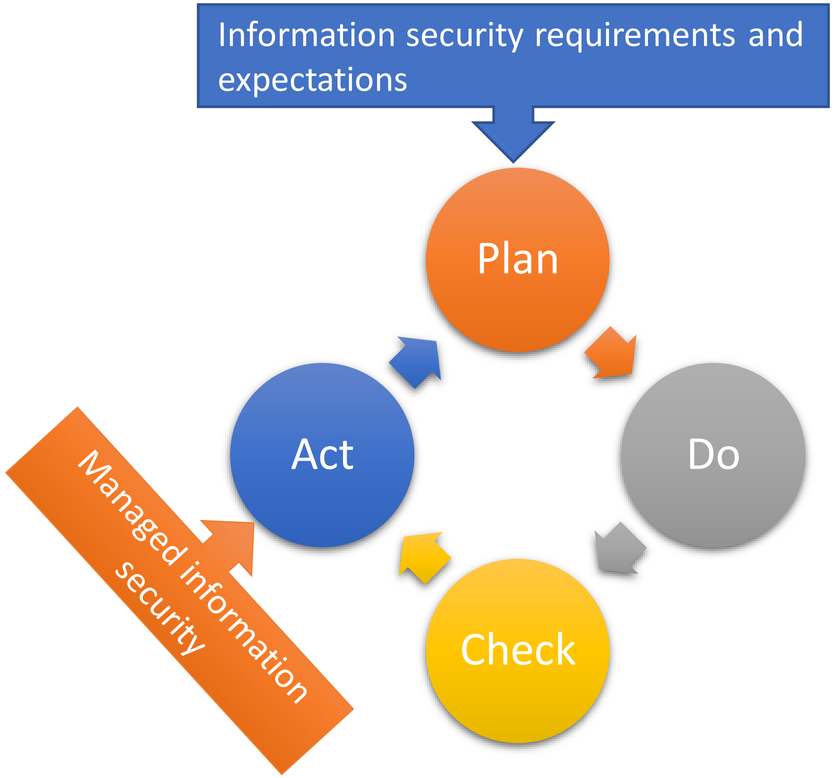
Performance Optimization - Steps in PDCA Cycle Process

1. Plan - In this step the ISMS is established.

2. Do - ISMS Implementation - This process involves implementing the ISMS policies, procedures and controls across the organization.

3. Check – Compliance Review - This process is about monitoring and reviewing of the ISMS implementation

4. Act –Corrective Actions - Based on the results of performance of the processes, corrective and preventive actions are taken so that the ISMS policies and processes take care of these issues.


Information security requirements and expectations
Plan
Do
Check
Act
Managed information security

PDCA Cycle of ISMS Process

Process Optimization or performance optimization of the ISMS

The key to performance optimization is to determine where you stand or what the maturity level of a process is.

The top management has invested a lot on the implementation of ISMS across the organization and would certainly like to know the return on their investment.

Has the security improved over the years after implementing the ISMS etc.?

How is the organization placed against its peers and competitors?

The answer to all these above questions is answered by Security metrics.

What is a security metric?

One of the practical definitions of security metric is given by Brotby. W.K of Taylor and Francis Group LLC, Boca Raton, FL

“Metrics is a term used to denote a measure based on a reference and involves at least two points, the measure and the reference. Security in its most basic meaning is the protection from or absence of danger. Literally, security metrics should tell us about the state or degree of safety relative to a reference point and what to do to avoid danger”

What is a security metrics ?

“Metrics is a term used to denote a measure based on a reference and involves at least two points, the measure and the reference. Security in its most basic meaning is the protection from or absence of danger. Literally, security metrics should tell us about the state or degree of safety relative to a reference point and what to do to avoid danger”.

There are numerous reasons as to why we would need security metrics. Here are the important ones. It helps in:

- Communicating the performance
- Driving performance improvements
- Measuring the effectiveness of the implemented controls
- Diagnose the security problems
- Pinpointing the accountability
- Resource allocation
- Demonstrates the security compliance
- Benchmarking

Steps in the process of security metrics

Quiz / Assessment

4. A Security metric is important because it __________.

a)Helps in communicating performance of the system

b)Helps in driving the performance process

c)Helps in measuring the data

d)Helps in achieving solutions

Quiz / Assessment

5. Characteristics of a good metric is one ___________.

a)That is consistent in measurement

b)That helps in system process

c)That can provide a subjective measure

d)No unit of measure is required.

Quiz / Assessment

6. The _________could be training the resources, implementing new tools for securing the software to implementing new processes or optimizing the existing processes.

a)corrective action

b)Estimate action

c)Positive action

d)System action

Role and Responsibilities of IT Security

IT Security Roles and Responsibilities

Legal Owner

The top management will legally own all the information assets of the organization. IP rights are also held by the top management unless specified so in a contractual agreement.

CEO

The ownership of the information assets will be delegated to the CEO of the organization. He / She shall approve the information management / security policy.

The CEO has full authority to further delegate certain responsibilities to others below him.

IT Security Roles and Responsibilities

Director, Information Management

He/ she Ensures that all the information resources are managed corporate assets and helps in providing a strategic direction for the information system management.

- The responsibilities of the director, information management are:
- Advises on the information security management practices to the organization
- Provides strategic direction for implementation of IS management to the organization
- Helps in the development and implementation of the IS management practices, policies and procedures

Chief Information Officer

The CIO ensures that the IT strategy aligns with the enterprise strategy.

The CIO is responsible for:

- Identifying and recognize the IT needs of the organization and convert them into IT infrastructure and strategic objectives
- Setting the IT Strategy for the organization

IT Security Roles and Responsibilities

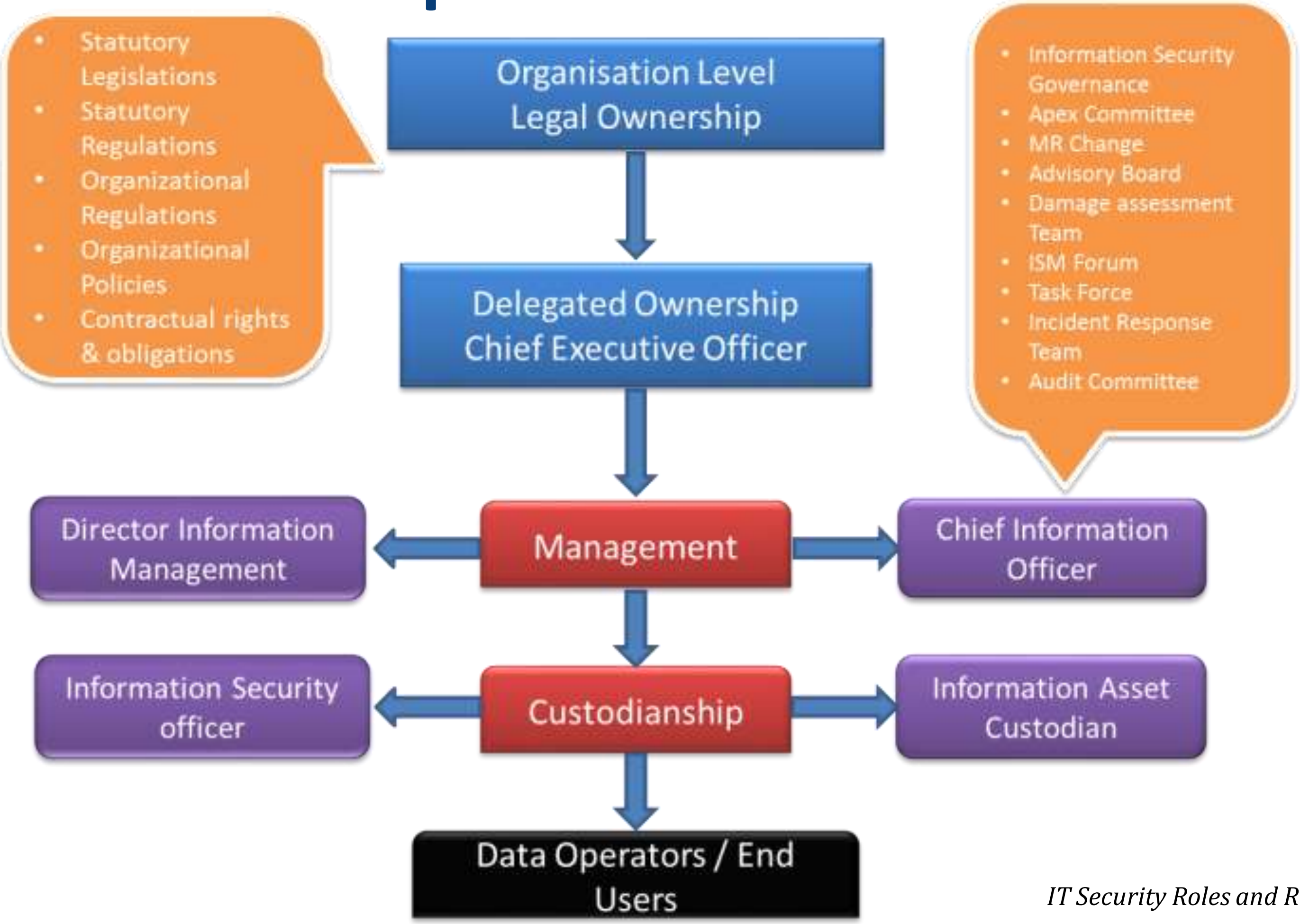
Information Security Officer: The responsibility of the information security officer is to implement processes and procedures as per the information security policy of the organization. It is his responsibility to secure and safeguard all the information assets of the organization.

Data Operators / End Users: Follow the information asset usage guidelines. Access the information asset for the required use as per the business requirements

Risk Assessor: The person assessing the risk can be the project or program owner, the asset owner or information security officer or the risk owner. The responsibilities include:

- Establishing the context for the risk assessment – whether it is for the project, product, process or organization
- Identification of the risks
- Risk Analysis
- Risk Evaluation
- Risk Treatment

IT Security Roles and Responsibilities



Statutory Legislations
Statutory Regulations
Organizational Regulations
Organizational Policies
Contractual rights & obligations
Organisation Level Legal Ownership
Delegated Ownership Chief Executive Officer
Information Security Governance
Apex Committee
MR Change
Advisory Board
Damage assessment Team
ISM Forum
Task Force
Incident Response Team
Audit Committee
Director Information Management
Management
Chief Information Officer
Information Security officer
Custodianship
Information Asset Custodian
Data Operators / End Users

IT Security Roles and Responsibilities

Quiz / Assessment

7. Which of the following are the responsibilities of the CEO?

a) Establishing the context for the risk assessment – whether it is for the project, product, process or organization

b) Information security incident management

c) The ownership of the information assets

d) Process of system management

Quiz / Assessment

8. What are the responsibilities of the Information Security Officer?

a) Creating awareness on duties

b) Disaster process

c) Change Management Implementation for all the information assets

d) Implementation of the Risk Treatment Plan

Quiz / Assessment

9. Responsibility of Integrating the IT Strategic and the organizational Strategic plan lies with

a) CEO

b) CIO

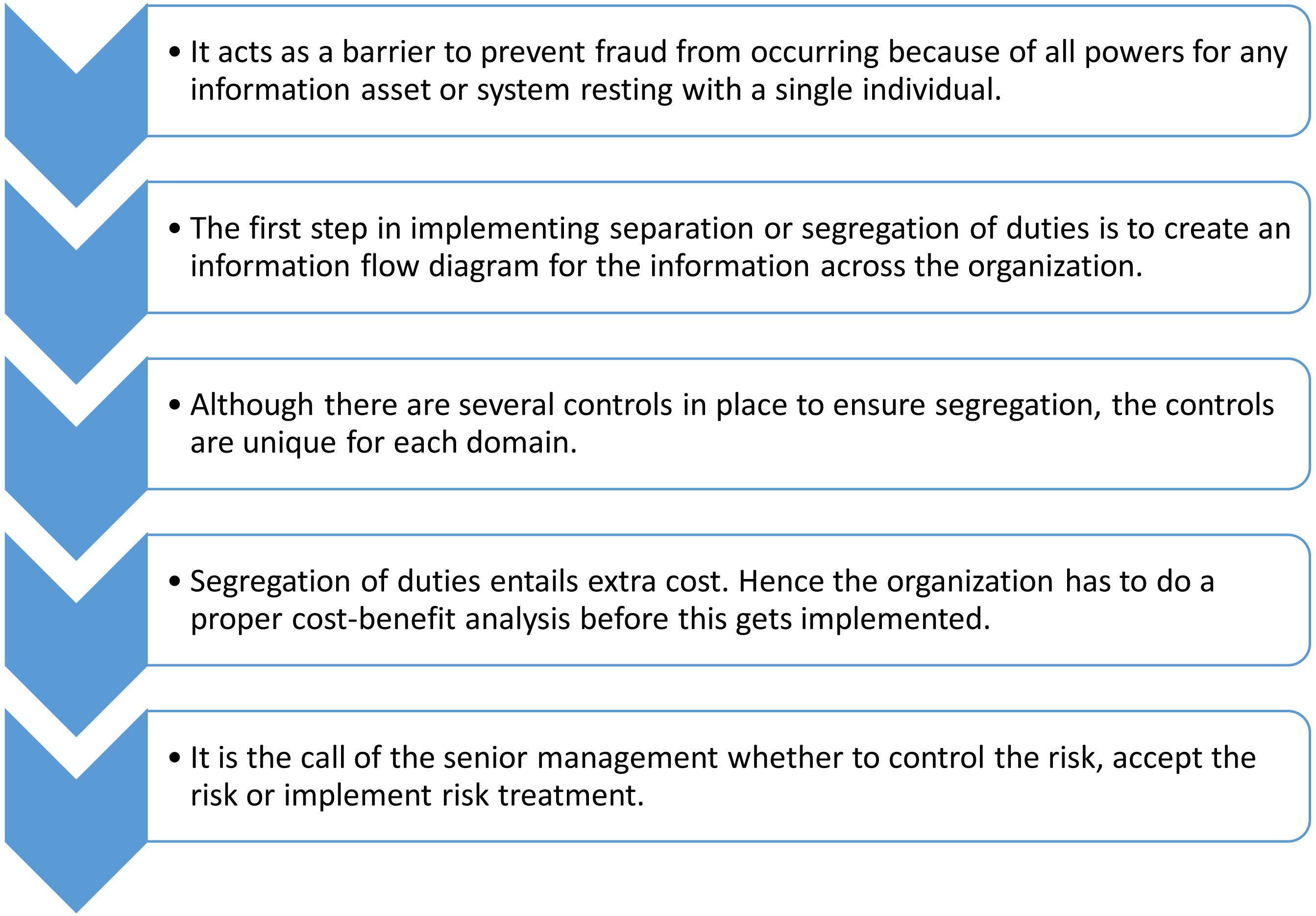
c) Director, Information Technology

d) Project Owner

Segregation of Duties

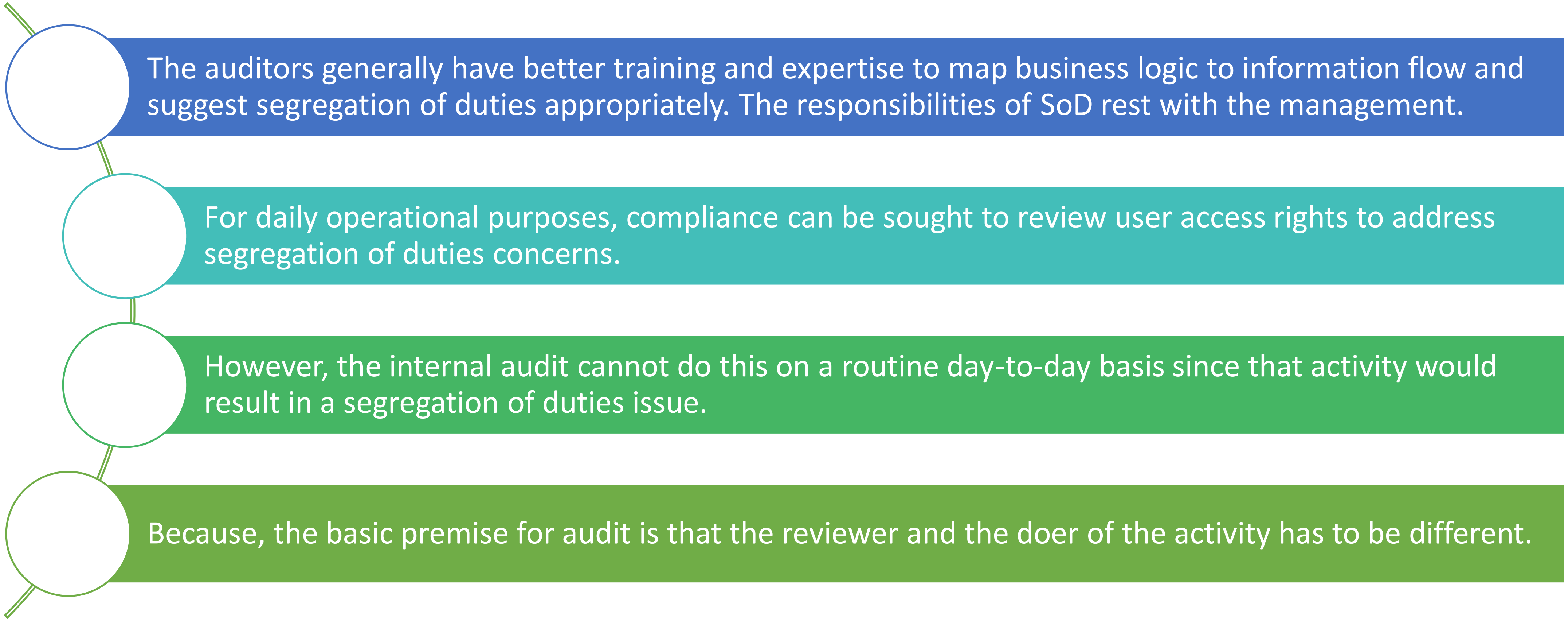
Segregation of Duties

Segregation of duties or Separation of duties (SoD) is a classic security strategy to tackle conflict of interest, the appearance of conflict of interest and fraud.



- It acts as a barrier to prevent fraud from occurring because of all powers for any information asset or system resting with a single individual.
- The first step in implementing separation or segregation of duties is to create an information flow diagram for the information across the organization.
- Although there are several controls in place to ensure segregation, the controls are unique for each domain.
- Segregation of duties entails extra cost. Hence the organization has to do a proper cost-benefit analysis before this gets implemented.
- It is the call of the senior management whether to control the risk, accept the risk or implement risk treatment.

Segregation of Duties in Information Technology



The auditors generally have better training and expertise to map business logic to information flow and suggest segregation of duties appropriately. The responsibilities of SoD rest with the management.

For daily operational purposes, compliance can be sought to review user access rights to address segregation of duties concerns.

However, the internal audit cannot do this on a routine day-to-day basis since that activity would result in a segregation of duties issue.

Because, the basic premise for audit is that the reviewer and the doer of the activity has to be different.

Quiz / Assessment

10. Segregation of Duties is a ____________.

a) IT Strategy to align with the organization
b) Risk Management Policy
c) A security strategy
d) A service management strategy

Quiz / Assessment

11. The first step in implementing separation or segregation of duties is to create an ___________diagram for the information across the organization.

a) Information flow
b) Development
c) Authentic
d) Segment

Quiz / Assessment

12. The first step in implementing segregation of duties is to create an __________diagram for the information across the organization.

a) Flow of content
b) Graph
c) Representation
d) Information flow

Activity

Activity can be either offline or online

Offline Activity
(30 min)

- Divide the class into two to three groups and perform a group discussion on roles and responsibilities of IT security.

Note: Refer Table of Content for the activities

Summary

- ✓ Data is created, stored, modified and transmitted through IT systems. It is very critical to safeguard the IT systems that we use, as IT security incidents have a high impact on business and can prove to be very expensive.
- ✓ Information security is about optimizing the information security management processes.
- ✓ The purpose of information security is to build a structure or system that will take into account all kinds of risks and protects all the information assets (both IT and Non-IT) by implementing appropriate controls.
- ✓ The legal owner of all the information assets of the organization is the top management. IP rights are given to the top management unless specified so in a contractual agreement.
- ✓ Security strategy to tackle conflict of interest, the appearance of conflict of interest and fraud is known as Segregation of duties or Separation of duties (SoD)
- ✓ The auditors have better training and expertise to map business logic to information flow and suggest segregation of duties appropriately. The technology group will not have sufficient expertise to implement the segregation of duties.
- ✓ The CIO responsible for the implementation of IT Security / Governance mechanisms should not have signature authority over security tasks.

e-References

- *Information security Management system.* Retrieved 2008, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile
- *Information security.* Retrieved March 07, 2007, from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
- Roles and Responsibilities for Information asset management. Retrieved July 8th, 2009, from http://www.iso27001security.com/ISO27k_Roles_-_responsibilities_for_information_asset_management.pdf
- *Separation of Duties in Information Technology.* Retrieved from http://www.sans.edu/research/security-laboratory/article/it-separation-duties
- *ISMS implementation and certification process.* Retrieved from http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_overview_v2.pptx.
- *A Guide to Security Metrics.* Retrieved June 19th, 2006, from https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

External Resources

1. Weill, P. & Ross, J. (2004). *IT governance*. Boston: Harvard Business School Press.
2. Harkins, M. (2013). *Managing risk and information security*. [New York]: Apress.
3. Peltier, T. (2010). *Information security risk analysis, third edition*. Boca Raton, Fla.: CRC Press.