

Information Security Management System

An ISACA Framework

Solomon B. Anastacio
President, ISACA-Manila
Manager, IT Audit, Meralco

Information Security Management System – an ISACA Framework

The Fundamental Question

Are we maximising the value of our Information Security - enabled business investments such that:

- We are getting **optimal benefits**
- At an **affordable cost**
- With an **acceptable level of risk?**

Over the full economic life cycle of the investment

A New Perspective

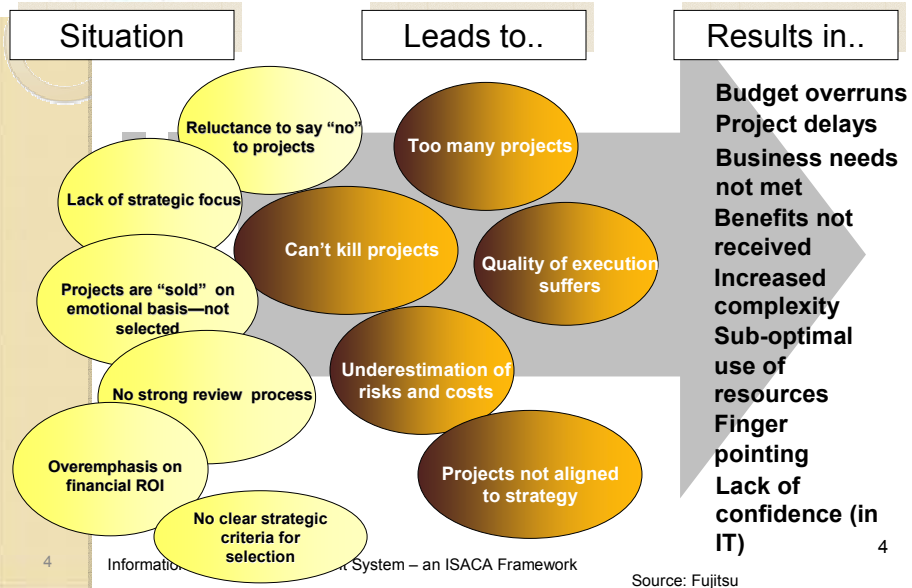


➔ **Investments in**
InfoSec-enabled Change ←

3

Information Security Management System – an ISACA Framework Source: *The Information*

Without Effective Governance



4

Information Security Management System – an ISACA Framework

Source: Fujitsu

4

Information Security Management Domains

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management and Response

from **Certified Information Security Manager (CISM)**

Information Security Management System – an ISACA Framework

Information Security Management Domains

- Information Security Governance
 - Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent

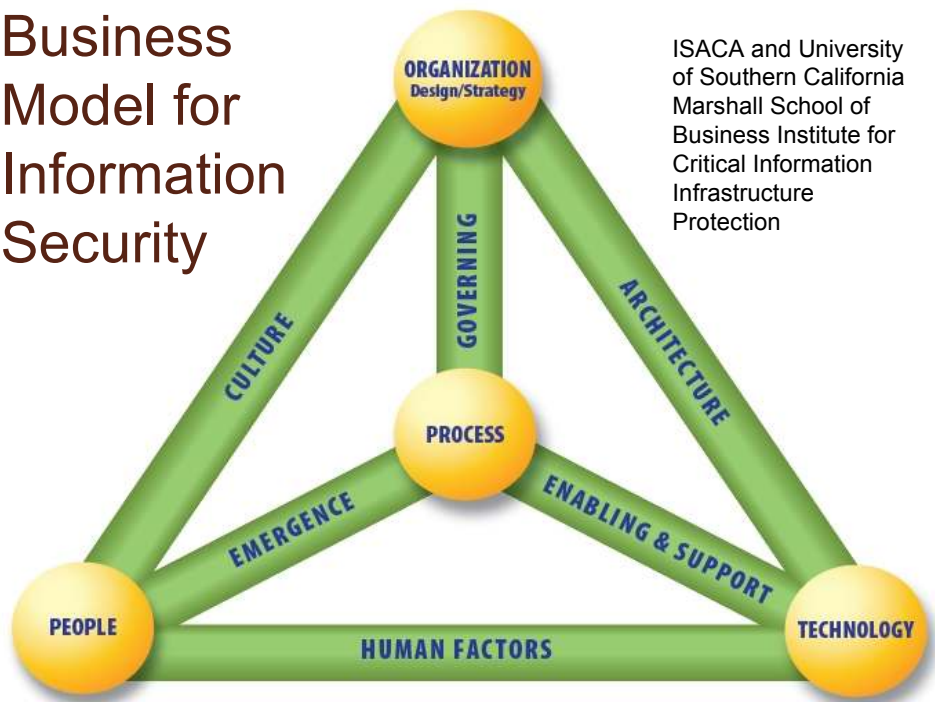
Information Security Management System – an ISACA Framework

Information Security Governance

- A comprehensive security strategy linked to business objectives
- Security policies that address each aspect of strategy, controls and regulation
- A complete set of standards for each policy
- An organizational structure void of conflicts of interest with sufficient authority and resources
- Metrics and monitoring processes to ensure compliance and provide feedback

Information Security Management System – an ISACA Framework

Business Model for Information Security



Information Security Management Domains

- Information Security Governance
- Information Risk Management
 - Identify and manage information security risks to achieve business objectives

Information Risk Management

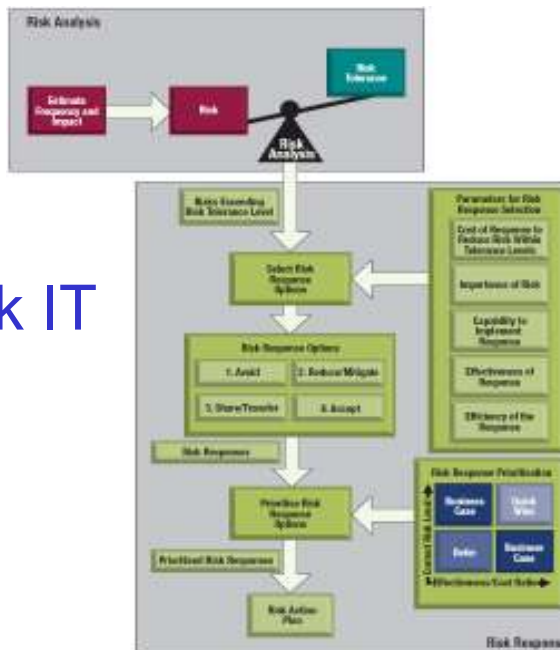
- Understanding of the organization's threat, vulnerability and risk profile
- Understanding of risk exposure and potential consequences of compromise
- Awareness of risk management priorities based on potential consequences
- Organizational risk mitigation strategy sufficient to achieve acceptable consequences from residual risk
- Organizational acceptance/deference based on an understanding of potential consequences of residual risk.

Risk Management Program

- Basic steps in developing a risk management program:
 - Establishing the context and purpose
 - Identifying and valuing assets
 - Classifying assets
 - Identifying threats and vulnerabilities
 - Determining risks
 - Assessing impacts
 - Mitigating risks
 - Educating users
 - Monitoring and reviewing
 - Communicating and consulting

Information Security Management System – an ISACA Framework

from Risk IT



Information Security Management System – an ISACA Framework

Information Security Management Domain

- Information Security Governance
- Information Risk Management
- Information Security Program Development
 - Create and maintain a program to implement the information security strategy

Information Security Program Development

- Plans or Programs to implement the information security strategy including Projects and Activities.
- Information security architectures
- Information security policies, standards, procedures and other documentations that support the security strategy.
- Information security awareness, training and education.
- Information security requirements into the organization's processes and life cycle activities.
- Process to integrate information security controls into contracts.
- Metrics to evaluate the effectiveness of the information security program.

Information Security Management Domain

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
 - Oversee and direct information security activities to execute the information security program

Information Security Program Management

- Management of Internal and External Resource
- Performance of Information Security processes and procedures
- Performance of contractually agreed information security controls.
- Ensuring that information security is an integral part of the other business processes
- Information security advice and guidance
- Performance of Information security awareness, training and education programs
- Monitoring of information security controls and compliance with information security policies.

Information Security Management Domain

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management and Response
 - Plan, develop and manage a capability to detect, respond to and recover from information security incidents

Incident Management and Response

- Processes for detecting, identifying, analyzing and responding to information security incidents.
- Escalation and communication processes and lines of authority.
- Plans and capability to respond to, investigate and document information security incidents.
- Process to communicate with internal parties and external organizations
- Integration of information security incident response plans with the organization's disaster recovery (DR) and business continuity plan.
- Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.

Information Security Management Domains

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management and Response

from **Certified Information Security Manager (CISM)**

Information Security Management System – an ISACA Framework

ISACA Publications



www.isaca.org

Information Security Management System – an ISACA Framework

For more information

- Business Model for Information Security
 - www.isaca.org/bmis
- Certified Information Security Manager (CISM)
 - www.isaca.org/cism



Information Security Management System – an ISACA Framework

A Take Away.....

Kubernán (Gr): To steer a ship; the process of *continually orienting and adjusting*

“Managing an uncertain journey to an uncertain destination”



Information Security Management System – an ISACA Framework