Protecting Information Assets
- Week 6 -

Mid-Term Review:
Managing IT Security Risk

MIS5206 Week 6

- In the News
- Readings
  - HBR Review Article
- Mid-Term Review
- Mid-Term Exam

In the News

- Discuss items “in the news”

Reading

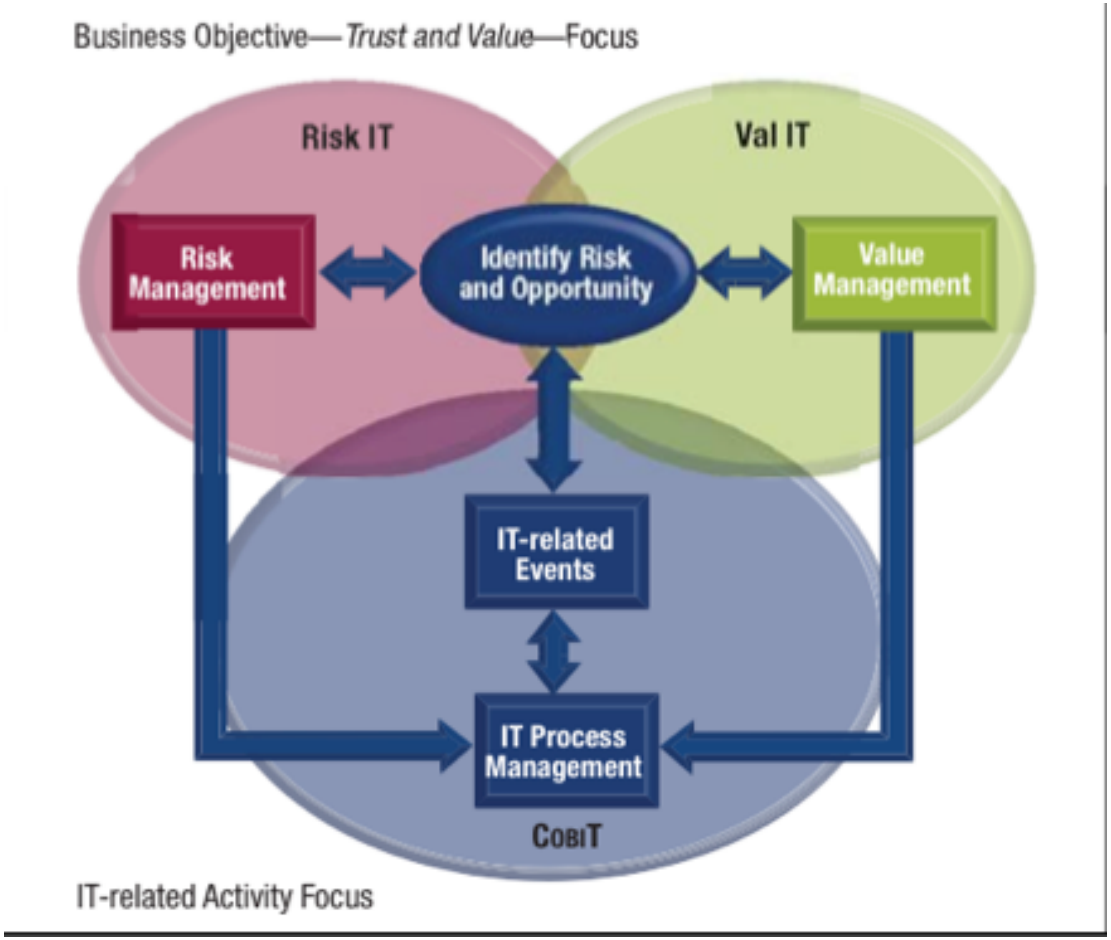
- HBR Article

Mid-Term Review

- Risk IT Framework
- Understanding an Organization's Risk Environment
- Data Classification Process and Models
- Risk Evaluation
- Creating a Security Aware Organization

The RiskIT Framework

The Risk IT framework is to be used to help implement IT governance, and enterprises that have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.



COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

http://www.youtube.com/watch?v=hBH-Osh4Gm8

The RiskIT Framework

IT risk is business risk—specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives.

The RiskIT Framework

The Risk IT framework is about IT risk—in other words, business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk, as shown in the adjacent diagram

The RiskIT Framework

The risk management process model groups key activities into a number of processes. These processes are grouped into three domains. The process model will appear familiar to users of COBIT and Val IT: substantial guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of the process.

Understanding an Organization's Risk Environment

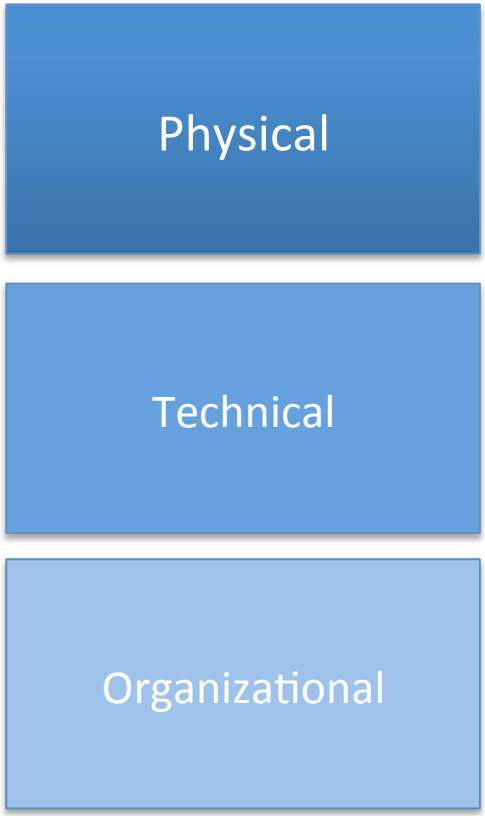
Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification and destruction

Key Concepts

Threat	Potential for the occurrence of a harmful event such as an attack
Vulnerability	Weakness that makes targets susceptible to an attack
Risk	Potential of loss from an attack
Risk Mitigation	Strategy for dealing with risk

What is a Threat?

Any thing that has the potential to lead to unauthorized access, use, disclosure, disruption, modification and destruction of an enterprises' information

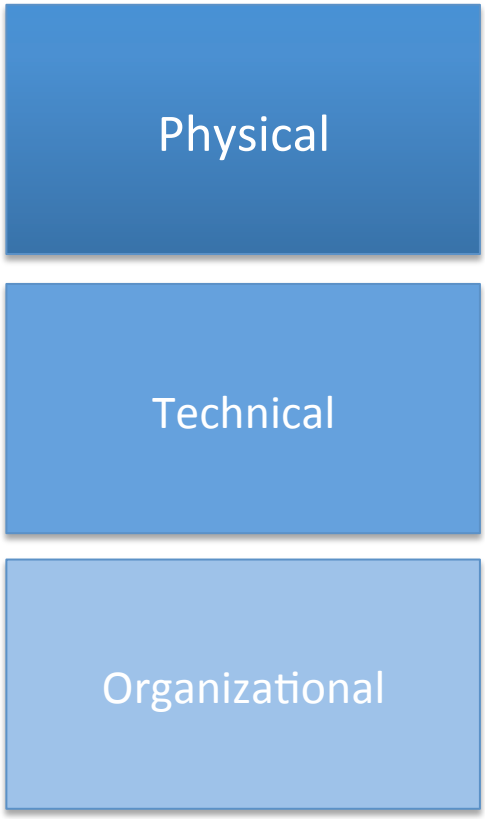


Assessing Threats

Likely threat sources:

- Human malicious
- Human non-malicious
- Accidents
- Natural disasters and other unexpected disruptions

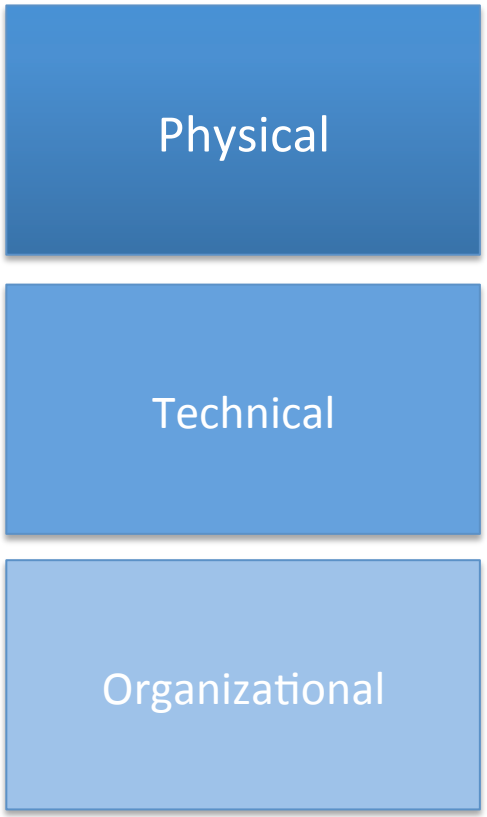
What is a Vulnerability?



Any unaddressed susceptibility to a Physical, Technical or Organizational information security threat

What is a Risk?

The potential loss resulting from unauthorized access, use, disclosure, disruption, modification and destruction of an enterprises' information. Can be expresses in quantitative and qualitative terms.



Information Security Risks

- Alteration of data, data destruction, theft of propriety data
- Backup and recovery costs
- Bankruptcy
- Building collapse
- Business interruption
- Covert takeover of someone's computer
- Crime (non-computer, computer)
- Decreased productivity
- Equipment replacement costs
- Financial loss
- Fraud, theft, larceny, bribery
- Frustration
- Ill will
- Injury
- Inaccurate data
- Eavesdropping, password theft
- Location of modems to exploit
- Loss of competitive edge
- Loss of data
- Loss of life
- Loss of time
- Lost productivity
- Meltdown of computer chips
- Shutdown of networks or web sites Location of holes in networks
- Inability to process critical applications
- Unauthorized access or break-ins to network, other systems
- Replacement costs (software, hardware, other)
- Reprocessing, reconstruction costs

Assessing Risk

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

   – **Single loss expectancy = Asset value x Exposure factor**

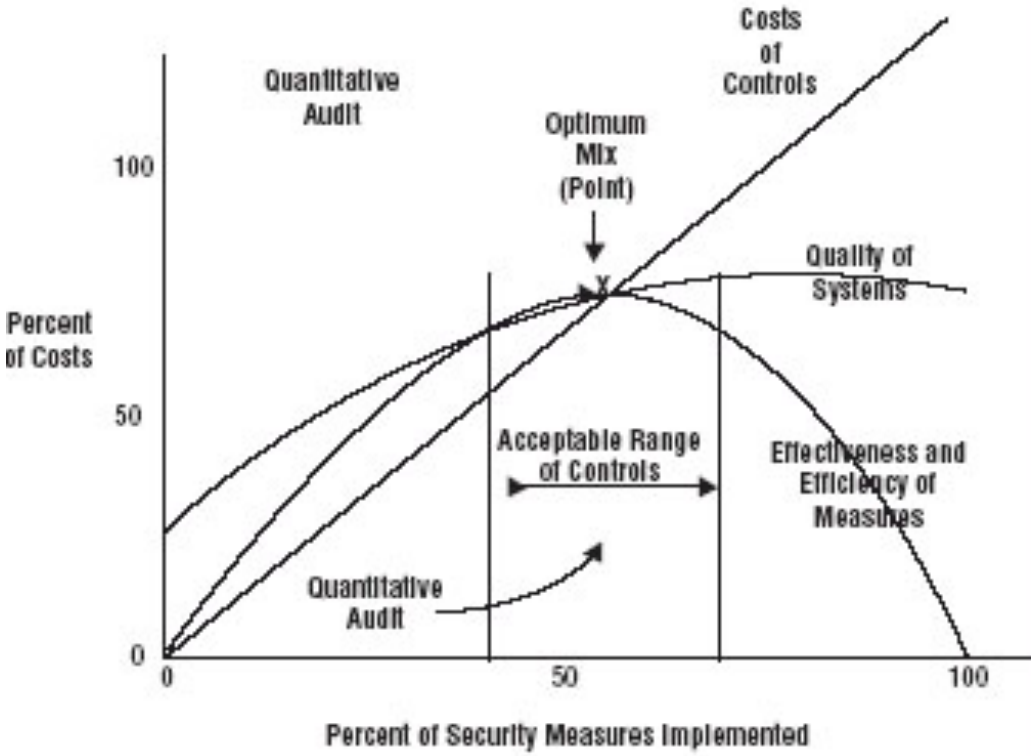
   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the annual rate of occurrence (ARO). Simply stated, how many times is this expected to happen in one year?

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

   – **Annualized loss expectancy (ALE) = Single loss expectancy (SLE) x Annualized rate of occurrence (ARO)**

What is a Risk Mitigation?



An approach for lessening or avoiding the impact of a potential risk in an acceptable and cost-effective manner

Risk Mitigation Approaches

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/ contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private keyinfrastructure
- Fences
- Corporate code of conduct
- Forensic (fraud) audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- Penetration testing
- Placement of authentication/authorization/ database/accounting servers in secure location
- Receptionists
- Residue controls (disintegrator / shredders)
- Secure file wipes
- Secure passwords
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Data Classification Process and Models

In an environment of heightened risk, data classification becomes the fundamental step in trying to protect one of an organization's most important assets — its information.

Information Security Classification

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by Company production activities as specified by the client
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non disclosure agreements with clients\vendors • Company business plans

Other Classification Schemes

- The business or function of an organization may create unique classification requirements
- There are other classification schemes in use besides the international standard

ISO Standard	Common
Unclassified/Public	Public
Proprietary	Sensitive
Client Confidential	Private
Company Confidential	Secret

Risk Evaluation

Risk evaluation is the process of identifying risk Risk Scenarios *and describing their potential* Business impact

The RiskIT Framework

The risk management process model groups key activities into a number of processes. These processes are grouped into three domains. The process model will appear familiar to users of COBIT and Val IT: substantial guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of the process.

Risk Evaluation - Key Components

Collect Data	Identify relevant data to enable effective IT-related risk identification, analysis and reporting
Analyze Risk	Develop useful information to support risk decisions that take into account the business impact of risk factors
Maintain Risk Profile	Maintain and up-to-date and complete inventory of known risks and attributes as understood in the context of IT controls and business processes

Collect Data

Goals and Metrics—RE1

Activity Goals	Process Goal	RE Goal
• Establish and maintain a model for data collection. • Collect data on the operating environment. • Collect data on risk events. • Identify risk factors.	• Identify relevant data to enable effective IT-related risk identification, analysis and reporting.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metric**
• Existence of a defined and documented risk-related data collection model • Number of sources used for data collection • Completeness of risk event data against established standards (e.g., affected assets, impact data, threat community, actions). This includes both discrete event data (e.g., control 'yes' or 'no') and continuous data (e.g., ongoing stream data on server response time). • Number of data items for which the contributing factors have been identified • Completeness of historical data across the top categories and domains of IT risk	• Number of loss events with key characteristics not captured in some form of repository • Degree to which collected data support reporting of trends and scenario analysis • The degree of visibility and recognition into the control state provided by data collection • The degree of visibility and recognition into the threat landscape provided by data collection	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Analyze Risk

Goals and Metrics

Activity Goals	Process Goal	Domain Goal
• Define IT risk analysis scope. • Estimate IT risk. • Identify risk response options. • Perform a peer review of IT risk analysis.	• Develop useful information to support risk decisions that take into account the business relevance of risk factors.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**Domain Metrics**
• Percentage of time analyses are substantiated by later experience or testing (accuracy) • Percentage of time that peer review finds no significant logical, calculation or incompleteness errors (defensibility) • Percentage of time that parallel assessments on the same scenarios performed by different analysts get the same results (consistency) • Percentage of time that analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency) • A 'satisfaction index' derived over risk analysis reporting (e.g., the percentage of favourable satisfaction survey responses from business executives regarding the readability, usefulness and accuracy of risk analysis reports)	• Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope • Percentage of critical assets, targets and resources reviewed for the effect of known operational controls • Percentage of risk analysis undergoing peer review before being sent to management • Ratio of cumulative actual losses to expected loss magnitude	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Maintain Risk Profile

Goals and Metrics

Activity Goals	Process Goal	RE Goal
• Map IT resources to business processes. • Determine business criticality of IT resources. • Understand IT capabilities. • Update IT risk scenario components. • Maintain the IT risk register and IT risk map. • Develop IT risk indicators.	• Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metric**
• Percentage of key business activities with a dependency linkage to supporting IT resources and IT infrastructure resources • Percentage of critical elements of the IT portfolio covered by risk triggers and thresholds • Frequency of updates to the IT risk scenario components • Number of significant internal or external change events not reviewed for impact on IT risk scenario components • Number of significant internal or external change events not reviewed for impact on the IT risk map • Number of realised events with business impact not detected by a trigger mechanism	• Number of approved risk analysis results not yet incorporated into the risk profile • Percentage of critical business services not covered by risk analysis • Completeness of attributes and values across IT risk scenario components • Completeness of key risk data attributes across the IT risk register	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Maintain Risk Profile

RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
	Roles										
RE3.1 Map IT resources to business processes.			I	R			C	A/R	C		I
RE3.2 Determine business criticality of IT resouces.		C		R		C	A	R			I
RE3.3 Understand IT capabilities.			C	A/R				C	C		I
RE3.4 Update IT risk scenario componenets.			C	R	I	C	C	A	R		C
RE3.5 Maintain the IT risk register and IT risk map.		I	A	R	I	I	I	R/C	C		I
RE3.6 Develop IT risk indicators.			A	C			C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Creating a Security Aware Organization

Because of the importance of defending against social engineering and other information security threats, an ongoing awareness program is vital.

Why is Security Awareness Essential?

- We have a culture of trust that can be taken advantage of with dubious intent
- Most people feel security is not part of their job
- People underestimate the value of information
- Security Technologies give people a false sense of protection from attack

Basic Security Policies

- Every employee should be instructed in how to devise a difficult-to-guess password
- Every employee should know their responsibility to comply with the policies and the consequences for non-compliance

Security Policy Types

- Security policies related to computer and voice mail passwords
- The procedure for disclosing sensitive information or materials
- Email usage policy, including the safeguards to prevent malicious code attacks including viruses, worms, and Trojan Horses
- Physical security requirements such as wearing a badge

Security Policy Types (continued)

- The responsibility to challenge people on the premises who aren't wearing a badge
- Best security practices of voice mail usage
- How to determine the classification of information and the proper safeguards for protecting sensitive information
- Proper disposal of sensitive documents and computer media that contain, or have at any time in the past contained, confidential materials

Mid-Term Exam