Protecting Information Assets
- Week 2 -

Understanding an Organization's Risk Environment

MIS5206 Week 2

- In the News
- Readings
  - Vacca Chapter 1
  - HDFC BANK: SECURING ONLINE BANKING
  - ISACA RiskIT Framework pp. 1 - 42
- Week 1 Review
- Understanding an Organization's Risk Environment
- Test Taking Tip
- Quiz

In the News

SSH Keys: Managing the Risks - NIST Urges Key Management, Monitoring, Termination

Organizations must carefully manage their SSH keys; otherwise, they'll pose a security risk. That warning comes from the National Institute of Standards and Technology, which has published a draft of new guidelines for the cryptographic network protocol known as secure shell, or SSH, which is widely used to create a secure channel for linking two systems over an otherwise insecure network.

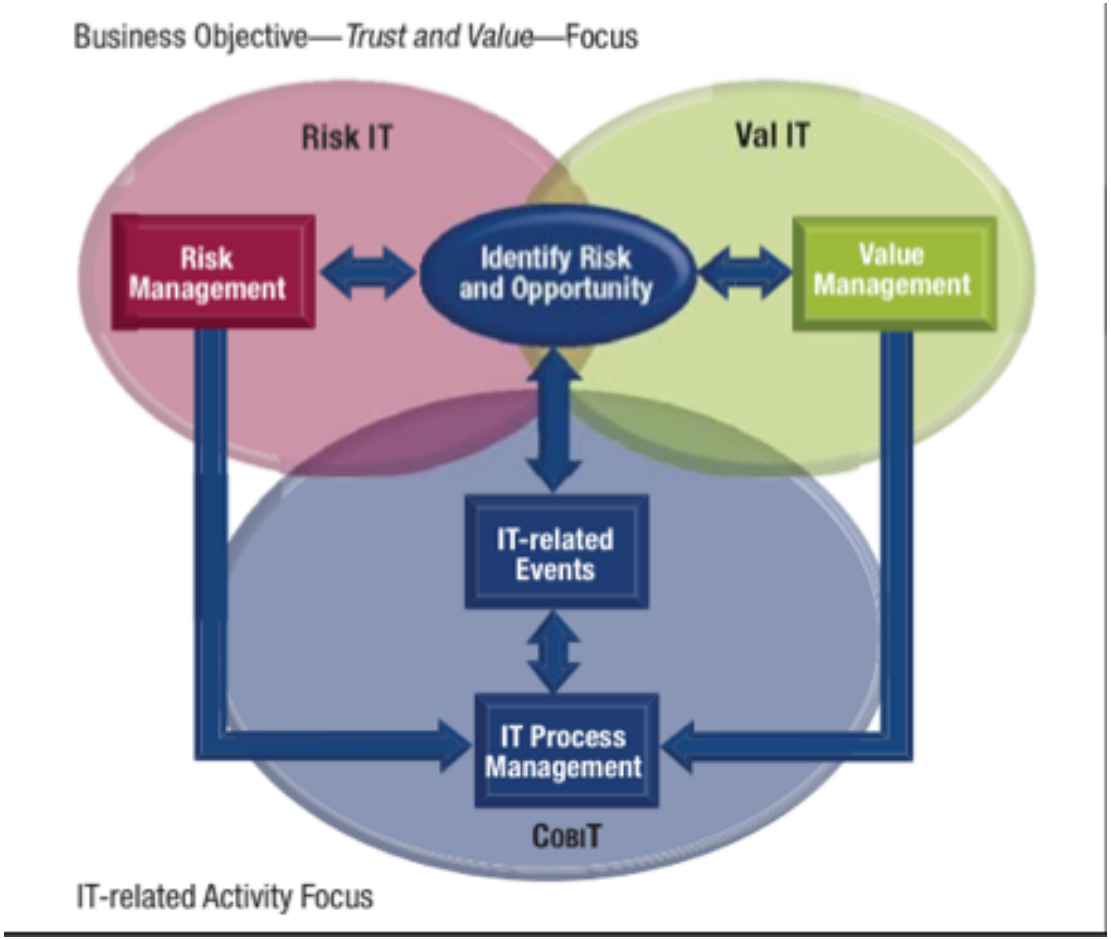
http://www.bankinfosecurity.com/ssh-keys-managing-risks-a-7248

Reading

- Vacca Chapter 1
- HDFC BANK: SECURING ONLINE BANKING
- ISACA RiskIT Framework pp. 1 - 42

Week 1: 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

Understanding an Organization's Risk Environment

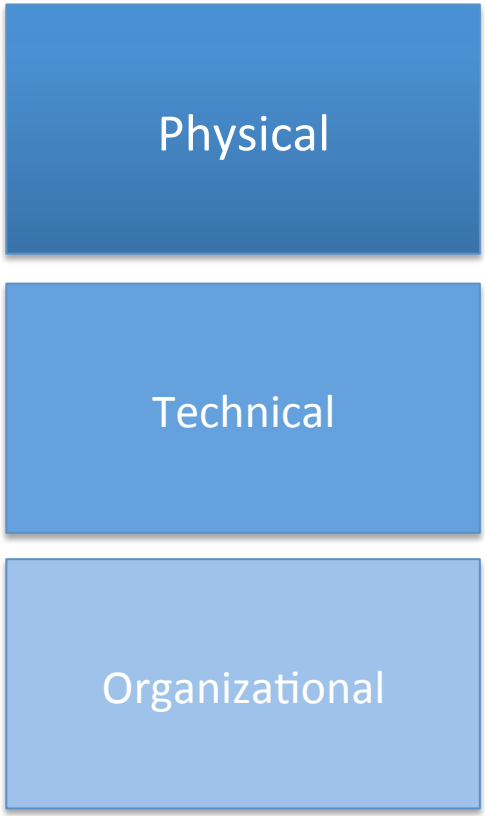
Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification and destruction

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

Human Malicious Threat Examples

- Accessing public material (80 percent unclassified and open to public)
- Black-hat hackers (lightweights to heavyweights)
- Bombing
- Career criminals
- Computer viruses (stealth, polymorphic, macro; over 6,500 different viruses identified)
- Corporate espionage (spies)
- Crackers/scriptkiddies (amateurs, novices; considerably less skilled than hackers)
- Cybercrime/fraud
- Data diddling
- Denial-of-service attacks
- Dumpster diving
- Employees, management (greed, vices, financial pressure, extravagant lifestyle, real or imagined grievances, workplace pressure/stress)
- High-energy radio frequency attacks (laser-like device aimed at buildings housing computers; high-frequency radio waves melt computer chips)
- Impersonation/spoofing (e-mail spoofs, anonymous eMailers, use of someone's login and password)
- Intelligence agencies
- Looping Internet Protocol ISP address (always-on Internet connections vulnerable)
- Password crackers (such as Cracker and LoPht Crack software)
- Physical attacks
- Remote access control software (examples include PCAnywhere, Timbuktu, NetBus, BackOrifice)
- Sabotage
- Social engineering (attacks against persons; using fake badges, blackmail, threat, harassment, bribery and impersonation)
- Surveillance (shoulder surfing, high-powered photography)
- Terrorists
- Trojan horses
- Unshredder software
- Van Eck receptors
- Vendors/suppliers/customers
- Vulnerability scanning software (such as SATAN, CyberCop software)
- War dialing
- Web crawlers

Human Non-Malicious Threat Examples

- Computer operator errors
- Data entry (input) errors
- Fire
- Inadequate access controls
- Inadequate training
- Inadequate human resource policies
- Inadequate program testing/controls incorporated into computer programs
- Inadequate risk analysis undertaken
- Inadequate supervision
- Lack of ethics
- Mislaid disk files
- Physical damage to disk
- Poor management philosophy/attitude
- Unlocked trash containers
- Update of wrong file
- Weak internal controls

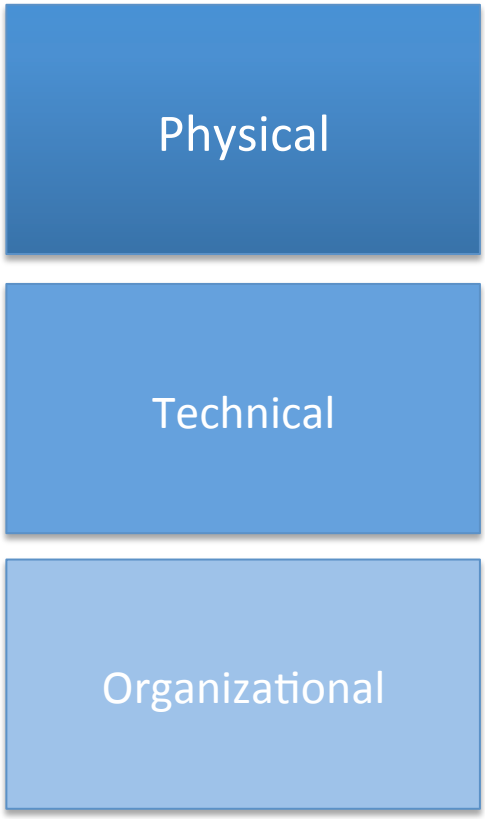
Human Non-Malicious Threat Examples

- Computer operator errors
- Data entry (input) errors
- Fire
- Inadequate access controls
- Inadequate training
- Inadequate human resource policies
- Inadequate program testing/controls incorporated into computer programs
- Inadequate risk analysis undertaken
- Inadequate supervision
- Lack of ethics
- Mislaid disk files
- Physical damage to disk
- Poor management philosophy/attitude
- Unlocked trash containers
- Update of wrong file
- Weak internal controls

Accidental and Natural Threats

- Air conditioning failure
- Building collapse
- Destruction of data, disks, documents, reports
- Destruction of water mains, sewer lines
- Failure of hardware
- Failure of fire alarms, smoke detectors
- Failure of computer programs
- Fire
- Freak accidents
- Gas line explosions
- Power outages (brownouts, blackouts, transients, spikes, sags and power surges)
- Product failure
- Software failure (operating system, database software)
- Global warming
- Ice and snow
- Floods
- Hurricanes
- Lightning
- Tornadoes, wind damage
- Tsunamis
- Bankruptcy
- Damage
- Injury
- Financial loss
- Long-term business interruption
- Loss of life

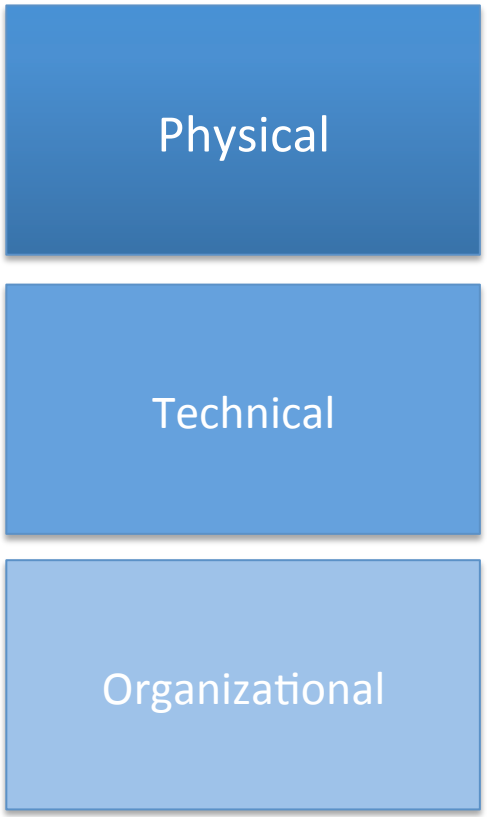
What is a Vulnerability?



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 (SLE) = Asset value X Exposure factor**

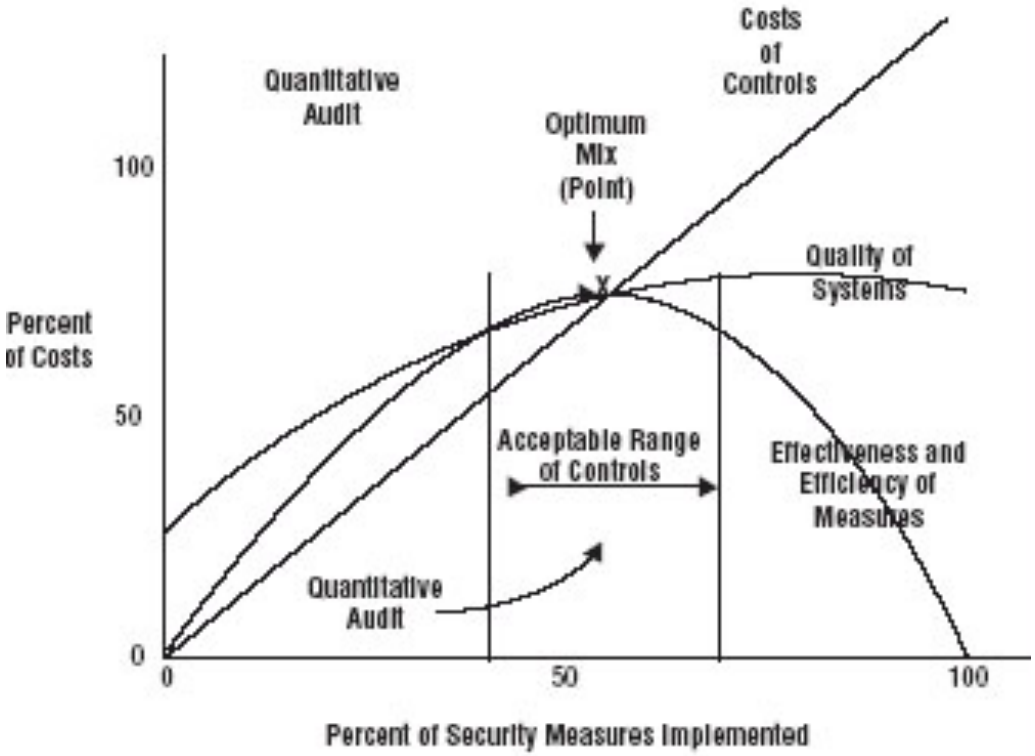
   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

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)

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

Test Taking Tip

- Read the answers first -

This contradicts many people's test taking recommendations.

But, it works. Here's why:

- Quickly alerts you to the type of question to expect
- Focuses your attention in reading the question for meaningful information
- Gives you advanced warning that there may be more than one significant concepts (option to answer in the form "Both A & B")
- Gives you an opportunity to get a sense of the sort of answer the test maker is looking for

Test Taking Tip

Example:

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an EDI environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an EDI environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A

Quiz