JAIN DEEMED-TO-BE UNIVERSITY

SCHOOL OF
COMPUTER
SCIENCE AND IT

# IT GOVERNANCE, RISK, & INFORMATION SECURITY MANAGEMENT

16BCSS41

Credits: 4

(CTIS) – 5th SEM

## Module-4

LECTURE : 4

PRACTICAL: 0

TUTORIAL : 0

Ajay Shriram Kushwaha

SKILL ENHANCEMENT COURSE (SKC) - 3

# Agenda

## Risk Management Program

- Introduction
- Importance of Risk management
- Phases of Risk Management
- Risk Management Process
- Risk Analysis methods.
- Risk-IT Framework of ISACA

# Agenda

Introduction to Risk Management Program

# Introduction

- The term risk refers to the concept that an action or choice can result in a losing situation.
- Risk management is the total process used to identify, control, and minimize the impact of uncertain events.
- Risks can come from various sources including uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root causes.
- The objective of the risk management program is to reduce the risk of performing some activity or function to an acceptable level.

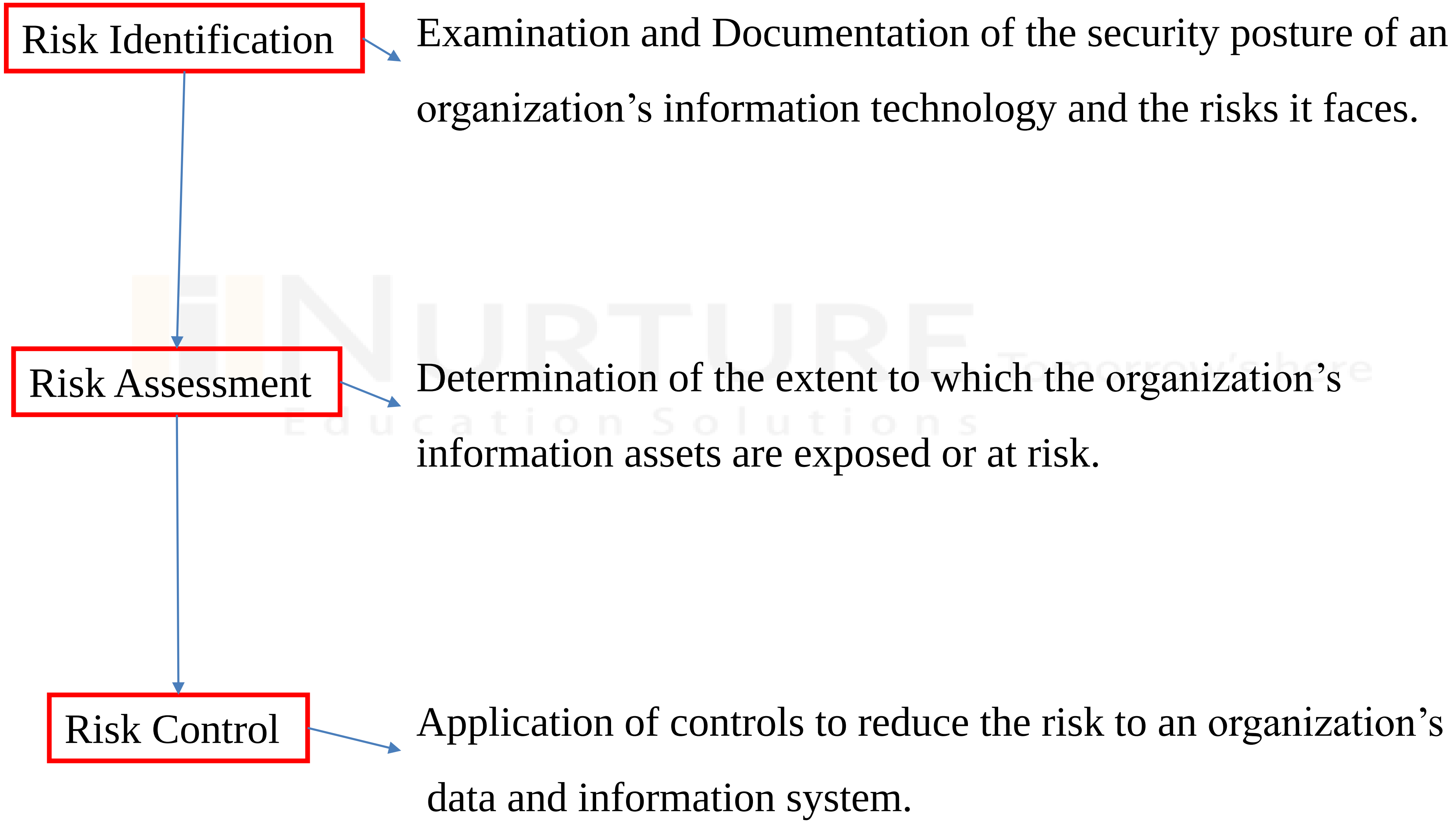
# What is **Risk Management?**

- The formal process of identifying and controlling the risks facing an organization is called risk management. It is the probability of an undesired event causing damage to an asset.

(Or)

The process of identifying Vulnerability in an organization information system & taking carefully respond to CIA.

# Components of Risk Management



Risk Identification

Examination and Documentation of the security posture of an organization’s information technology and the risks it faces.

Risk Assessment

Determination of the extent to which the organization’s information assets are exposed or at risk.

Risk Control

Application of controls to reduce the risk to an organization’s data and information system.

# Agenda

Risk Management  & Software Development Life Cycle

# RM & SDLC

- Effective risk management must be totally integrated into the organization’s system development life cycle.
- The typical SDLC has five phases,

  Analysis

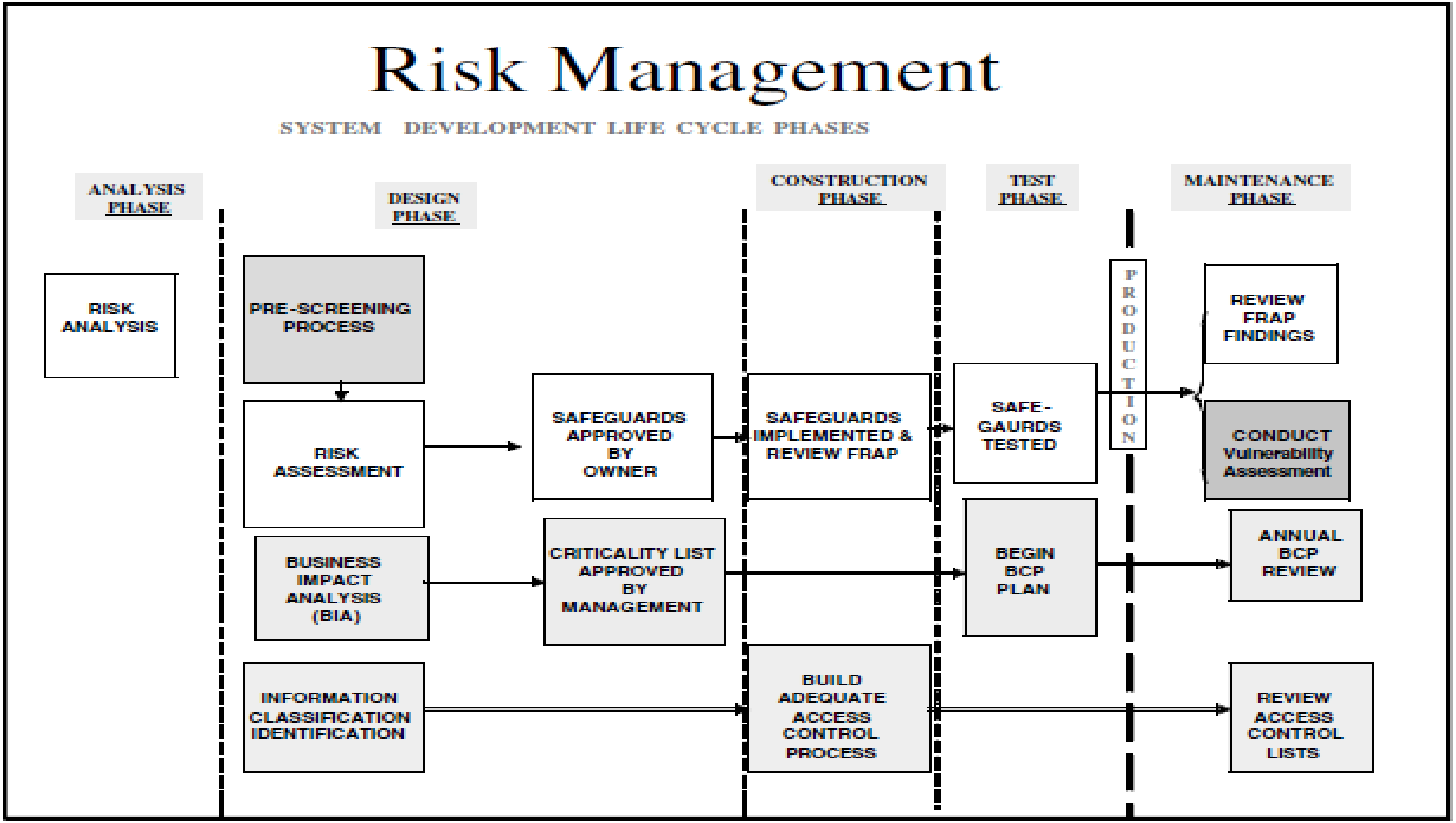
  Design

  Construction

  Test

  Maintenance

# RM & SDLC



Risk Management

SYSTEM DEVELOPMENT LIFE CYCLE PHASES

ANALYSIS PHASE

RISK ANALYSIS

DESIGN PHASE

PRE-SCREENING PROCESS

RISK ASSESSMENT

BUSINESS IMPACT ANALYSIS (BIA)

INFORMATION CLASSIFICATION IDENTIFICATION

SAFEGUARDS APPROVED BY OWNER

CRITICALITY LIST APPROVED BY MANAGEMENT

CONSTRUCTION PHASE

SAFEGUARDS IMPLEMENTED & REVIEW FRAP

BUILD ADEQUATE ACCESS CONTROL PROCESS

TEST PHASE

SAFE-GAURDS TESTED

BEGIN BCP PLAN

PRODUCTION

MAINTENANCE PHASE

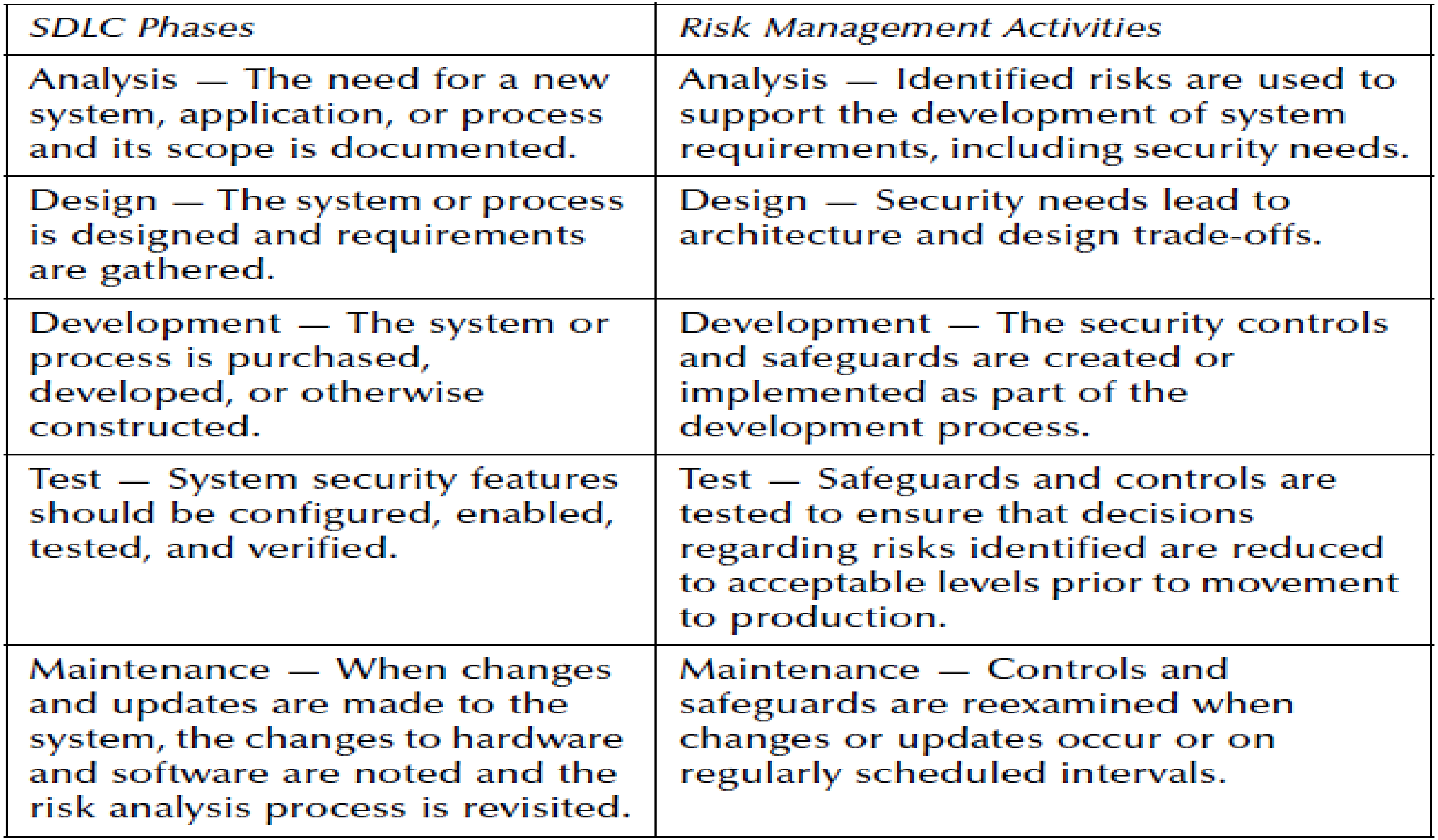
REVIEW FRAP FINDINGS

CONDUCT Vulnerability Assessment

ANNUAL BCP REVIEW

REVIEW ACCESS CONTROL LISTS

# RM & SDLC



| *SDLC Phases* | *Risk Management Activities* |
|---|---|
| Analysis — The need for a new system, application, or process and its scope is documented. | Analysis — Identified risks are used to support the development of system requirements, including security needs. |
| Design — The system or process is designed and requirements are gathered. | Design — Security needs lead to architecture and design trade-offs. |
| Development — The system or process is purchased, developed, or otherwise constructed. | Development — The security controls and safeguards are created or implemented as part of the development process. |
| Test — System security features should be configured, enabled, tested, and verified. | Test — Safeguards and controls are tested to ensure that decisions regarding risks identified are reduced to acceptable levels prior to movement to production. |
| Maintenance — When changes and updates are made to the system, the changes to hardware and software are noted and the risk analysis process is revisited. | Maintenance — Controls and safeguards are reexamined when changes or updates occur or on regularly scheduled intervals. |

# General Sun Tzu Wu Said

If you know your **enemy** and know **yourself**, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know nothing the enemy nor yourself, you will suffer in every battle.

# Context

Know Yourself -:

- Identify, Examine & Understand the information systems.
- To protect assets, you must understand what they are?
- The policies, Education and training programs, and technologies.

Know Enemy -:

- Identifying, Examining & Understanding the threats facing the organization.

# Roles played by the different communities of interest in organization:

**Information Security Specialist** :

- Best understand threats & attacks that introduce risk into the org.

- Take an leadership role in addressing risk.

**Management & Users** : Management ensure resources are allocated to IS & IT.

**Information Technology Specialist**: Must build secure system & operate them safely.

# Risk Management Process

- Inventory Review - Assets
- Identification - Vulnerability
- Controls – Strategies Reviewed
- Cost effective – Measuring the Strategies
- Monitoring – Managing on going process

# Risk Identification Process

**Step 1**: IT professionals or employees they should know about their org. information assets through identifying, classifying and prioritize them

**Step 2**: Once Assets are identified , Then threat identification process is undertaken

**Step 3**: Each assets are examined to identify vulnerabilities

**Step 4**: If found, Controls are identified and assessed to limit possible losses

# Risk Identification

Identify & inventory assets

Classify & prioritize assets

Identify & prioritize threats

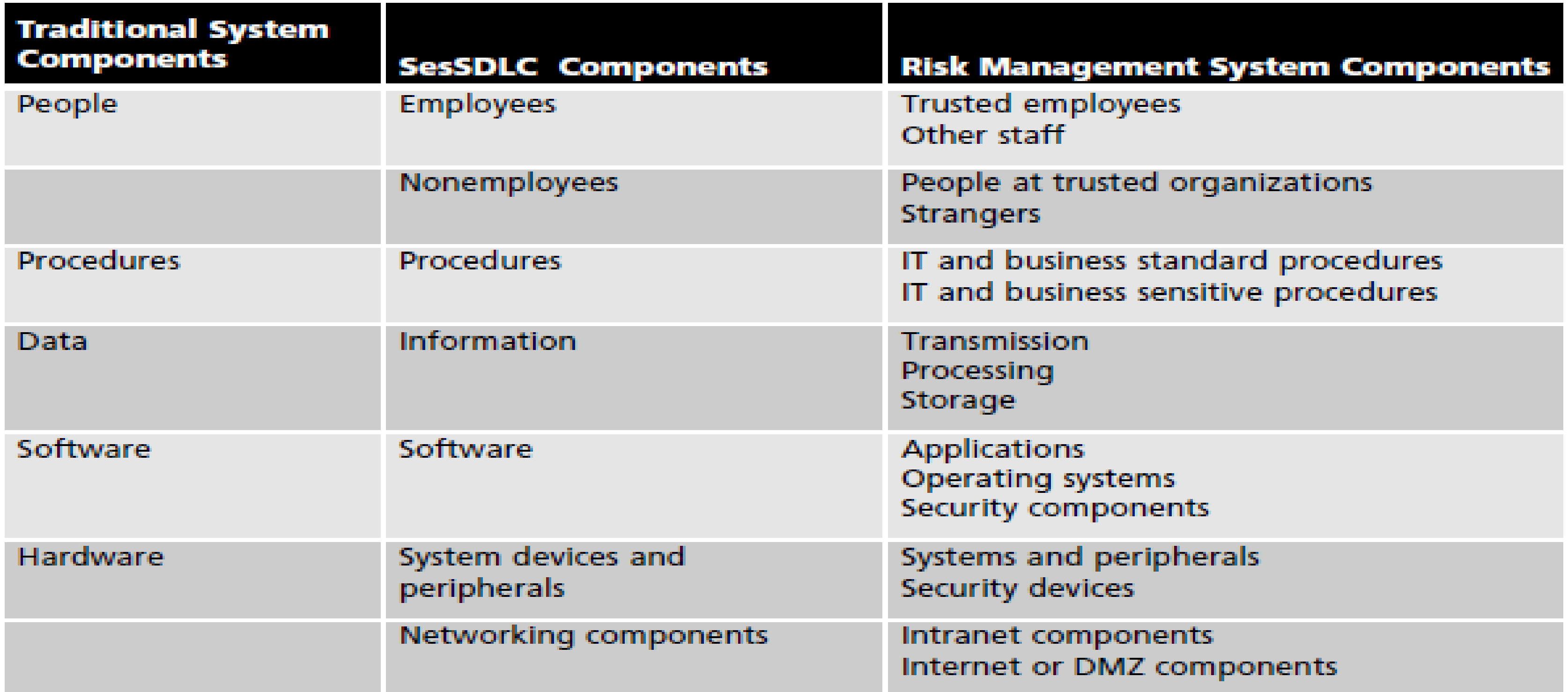
# Asset identification and inventory

# Asset identification

- People
- Procedure
- Data
- Software
- Hardware

# Asset identification

- Identify the organizations’ information assets—that is, identify, classify, and prioritize them.
- Risk identification is an iterative process and begins with the enumeration of assets, including all of the elements of an organization’s system, such as people, procedures, data and information, software, hardware and networking elements



| Traditional System Components | SesSDLC Components | Risk Management System Components |
|---|---|---|
| People | Employees | Trusted employees<br>Other staff |
| | Nonemployees | People at trusted organizations<br>Strangers |
| Procedures | Procedures | IT and business standard procedures<br>IT and business sensitive procedures |
| Data | Information | Transmission<br>Processing<br>Storage |
| Software | Software | Applications<br>Operating systems<br>Security components |
| Hardware | System devices and peripherals | Systems and peripherals<br>Security devices |
| | Networking components | Intranet components<br>Internet or DMZ components |

# Asset Classifications

- Identifying human resources, documentation, and data assets is more difficult than identifying hardware and software assets.
- People with knowledge, experience, and judgment should be assigned the task.

Consider the following asset attributes:

**People:** Position name/number/ID (avoid names and stick to identifying positions, roles, or functions); supervisor; security clearance level; special skills

**Procedures:** Description; intended purpose; relationship to software, hardware, and networking elements; storage location for reference; storage location for update

**Data**: Classification; owner, creator, and manager; size of data structure; data structure used (sequential or relational); online or offline; location; backup procedures employed

# Asset Classification

**H/w, S/w & Network** :

**Name**: Use the most common device or program name. Organizations may have several names for the same product.

**IP address**: This can be a useful identifier for network devices and servers, but does not usually apply to software.

**Media access control (MAC) address:** MAC addresses are sometimes called electronic serial numbers or hardware addresses.

Serial number, Manufacturer name, Software version, update revision, Physical location, Logical location, Controlling entity etc.,

# Data Classification

- **Public**: Information for general public dissemination, such as an advertisement or public release.
- **For Official Use Only**: Information that is not particularly sensitive, but not for public release, such as internal communications.
- **Sensitive**: Information important to the business that could embarrass the company or cause loss of market share if revealed.
- A data classification scheme generally requires a corresponding personnel **security clearance** structure, which determines the level of information individuals are authorized to view, based on what they need to know.
- Fundamental Principle is NEED TO KNOW basis

# Info asset valuation – Prioritize Assets

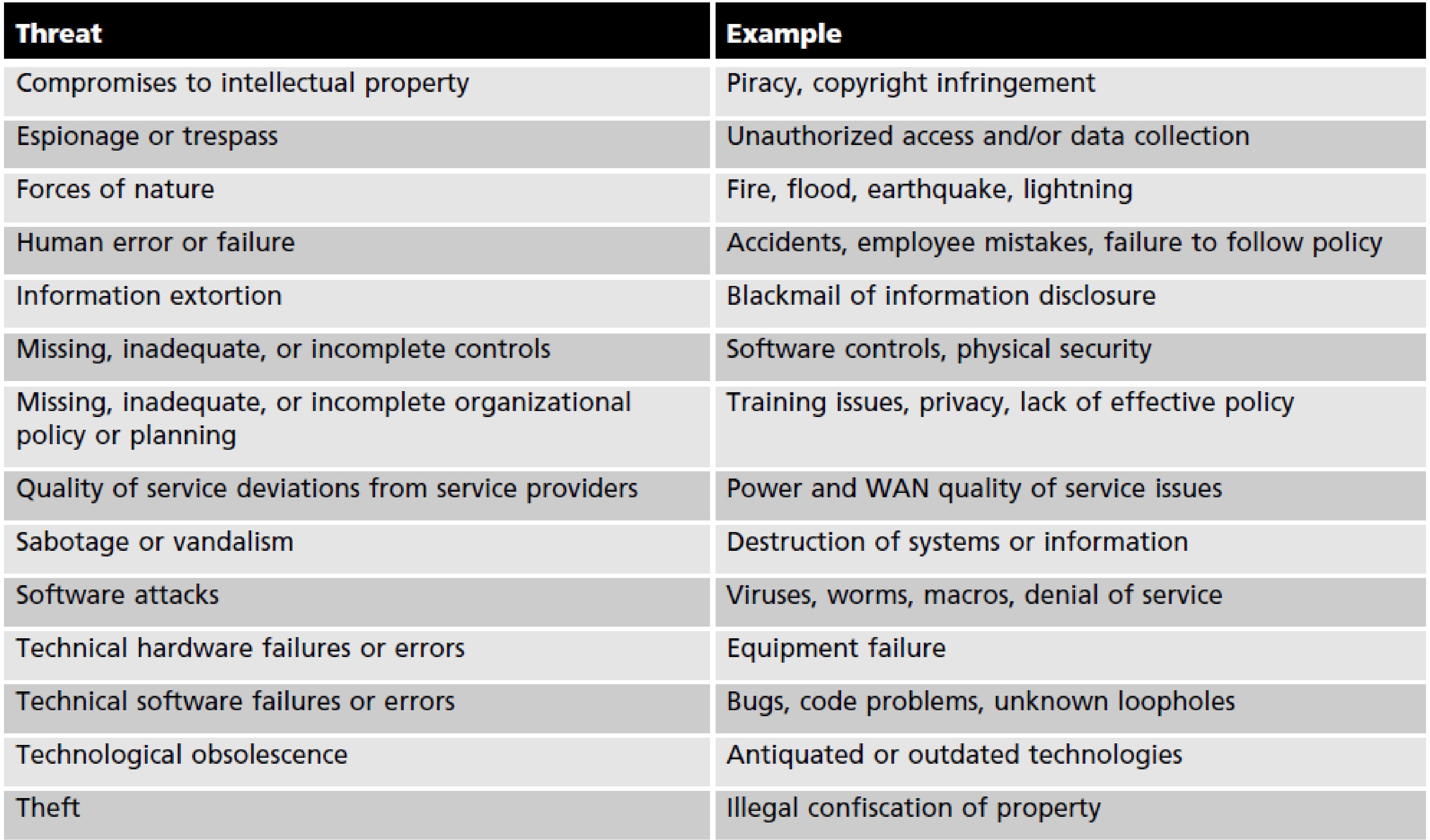
Based on Questionnaire assists in developing the weighting criteria :

- Which information asset is the most critical to the success of the organization?
- Which information asset generates the most revenue?
- Which information asset would be the most expensive to replace?
- Which information asset would be the most expensive to protect?
- Which information asset would most expose the company to liability or embarrassment if revealed?

# Threat Identification

- A threat source is defined as any circumstance or event with the potential to cause harm to the asset under review.
- Typically, there are three major categories of threat sources:
- **Natural threats** — Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events
- **Human threats** —Events that are either enabled by or caused by human beings, such as unintentional acts (errors and omissions) or deliberate acts (fraud, malicious software, unauthorized access). Statistically, the threat that causes the largest loss to information resources remains human errors and omissions
- **Environmental threats** — Long-term power outages, pollution, chemical spills, liquid leakage.

# Categories of Threats to info securit



| Threat | Example |
|---|---|
| Compromises to intellectual property | Piracy, copyright infringement |
| Espionage or trespass | Unauthorized access and/or data collection |
| Forces of nature | Fire, flood, earthquake, lightning |
| Human error or failure | Accidents, employee mistakes, failure to follow policy |
| Information extortion | Blackmail of information disclosure |
| Missing, inadequate, or incomplete controls | Software controls, physical security |
| Missing, inadequate, or incomplete organizational policy or planning | Training issues, privacy, lack of effective policy |
| Quality of service deviations from service providers | Power and WAN quality of service issues |
| Sabotage or vandalism | Destruction of systems or information |
| Software attacks | Viruses, worms, macros, denial of service |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopholes |
| Technological obsolescence | Antiquated or outdated technologies |
| Theft | Illegal confiscation of property |

# Identify and Prioritize threats

Address each threat with a few basic questions, as follows:

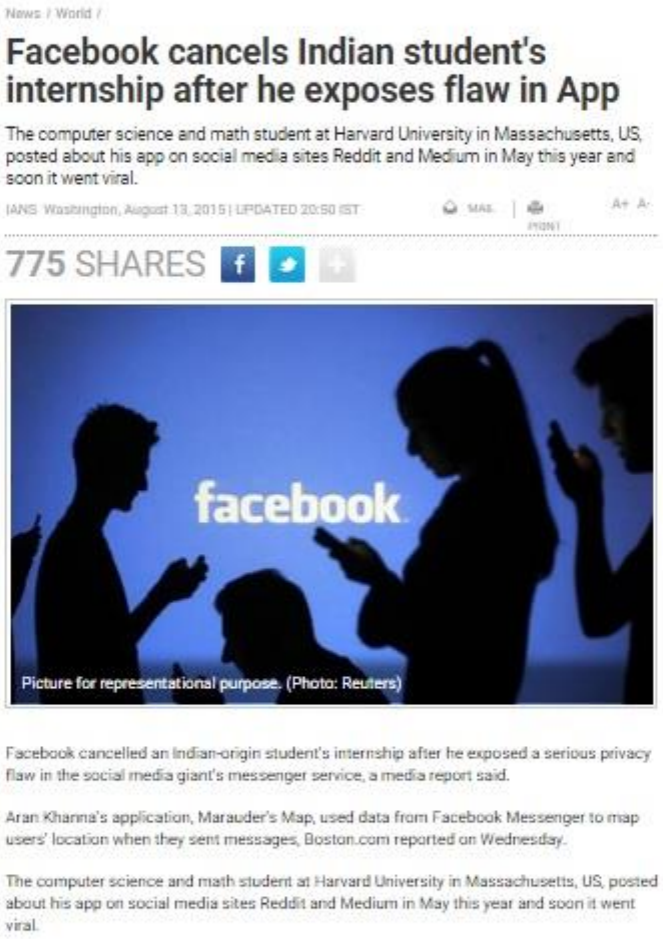
- Which threats present a danger to an organization's assets in the given environment?
- Which threat represent most danger to the organizations information?
- How much would it cost to recover from a successful attack?
- Which of the threats would require the greatest expenditure to prevent?

# Process of Vulnerability identification

- Create a list of Vulnerabilities for each information asset.
- Groups of people work iteratively in a series of sessions give best result.
- At the end of Identification process, you have a list of assets and their vulnerabilities.

| | **Threat** | **Possible Vulnerabilities** |
|---|---|---|
| 1. | Deliberate S/W attacks | IP is vulnerable to DOS. |
| 2. | Acts of Human error or failure | Employee may cause outage |
| 3. | Technical S/W failures or Errors | Vendor supplied routing software could fail |

# Tech News



News / World /

## Facebook cancels Indian student's internship after he exposes flaw in App

The computer science and math student at Harvard University in Massachusetts, US, posted about his app on social media sites Reddit and Medium in May this year and soon it went viral.

IANS Washington, August 13, 2015 | UPDATED 20:50 IST MAIL | PRINT A+ A-

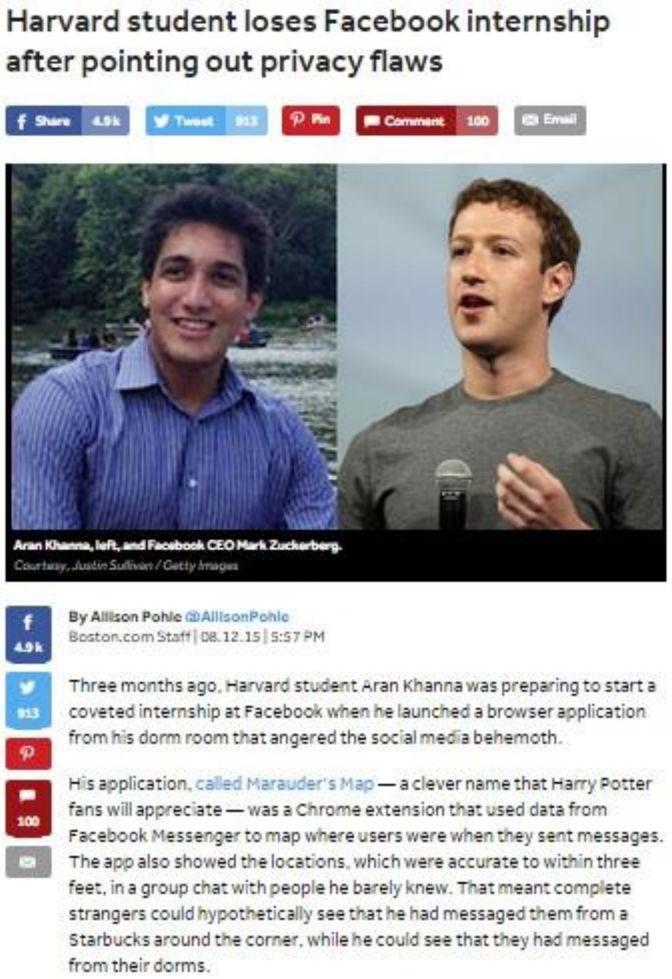
775 SHARES

Picture for representational purpose. (Photo: Reuters)

Facebook cancelled an Indian-origin student's internship after he exposed a serious privacy flaw in the social media giant's messenger service, a media report said.

Aran Khanna's application, Marauder's Map, used data from Facebook Messenger to map users' location when they sent messages, Boston.com reported on Wednesday.

The computer science and math student at Harvard University in Massachusetts, US, posted about his app on social media sites Reddit and Medium in May this year and soon it went viral.



## Harvard student loses Facebook internship after pointing out privacy flaws

Share 4.9k | Tweet 913 | Pin | Comment 100 | Email

Aran Khanna, left, and Facebook CEO Mark Zuckerberg.
Courtesy, Justin Sullivan / Getty Images

By Allison Pohle @AllisonPohle
Boston.com Staff | 08.12.15 | 5:57 PM

Three months ago, Harvard student Aran Khanna was preparing to start a coveted internship at Facebook when he launched a browser application from his dorm room that angered the social media behemoth.

His application, called Marauder's Map — a clever name that Harry Potter fans will appreciate — was a Chrome extension that used data from Facebook Messenger to map where users were when they sent messages. The app also showed the locations, which were accurate to within three feet, in a group chat with people he barely knew. That meant complete strangers could hypothetically see that he had messaged them from a Starbucks around the corner, while he could see that they had messaged from their dorms.

# Risk Assessment

Identify vulnerabilities between assets & threat

Identify & quantify asset exposure

# Process of Risk Assessment

- After identifying all the threats related to information assets.
- Ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process
  - Assessment
  - Controlling risk

Valuation of information Asset:

- Information asset classification worksheet
- Weighted criteria analysis worksheet
- Ranked vulnerability risk worksheet

# Risk Identification Estimate Factors – NIST Standard

- Likelihood
- Value of information assets
- Percentage of risk mitigated
- Uncertainty

# Factors- National Institute of Standards & Technology (NIST) gives some standards

- Likelihood : Probability of specific vulnerability within an organization will be successfully attacked
- 0.1 = Low
- 1.0 = High
- E.g. : No. of network attacks can be forecast based on how many network address the organization has assigned.

# Risk Determination

- Risk = **[ ( Likelihood of vulnerability occurrence ) X (Value of information Asset )] --** ( % of risk mitigated by current controls) + uncertainty of current knowledge of the Vulnerability.

For the purpose of relative risk assessment, risk equals:

- Likelihood of vulnerability occurrence TIMES value (or impact)
- MINUS percentage risk already controlled
- PLUS an element of uncertainty

# Risk Determination – Example 1

Information Asset **A** has a value score of 50 & has one vulnerability:

Vulnerability 1 has a likelihood of 1.0 with no current controls, estimate that assumptions and data are 90% accurate.

**Solution** :

Risk = [(1.0) * 50] – 0 % + 10 %

= (50 * 1.0) –(( 50 * 1.0)* 0.0) + ( 50 *1.0) * 0.1)

= 50 – 0 + 5

= 55

# Risk Determination – Example 2

Information Asset **B** has a value score of 100 & has one vulnerability:

Vulnerability 2 has a likelihood of 0.5 with current controls 50 % , estimate that assumptions and data are 80% accurate.

**Solution** :

Risk = [(0.5) * 100] – 50 % + 20 %

= (100 * 0.5) –(( 100 * 0.5)* 0.5) + ( 100 *0.5) * 0.2)

= 50 – 25 + 10

= 35

# Identify Possible controls

- **Residual Risk** : Residual risk is the risk that remains to the information asset even after the existing control has been applied.

**Categories of Control** :

Policies – General Security Policy, Program Security policies, Issue & System Specific Policies

Programs – Education, Training & Awareness

Technologies – Technical Implementation policies

**Access Control** : Specially addresses admission of a user into a trusted area of the organization.

**Eg**: Computer rooms, Power Rooms.

# Types of Access Control

- Discretionary
- Mandatory
- Nondiscretionary
- Lattice Based

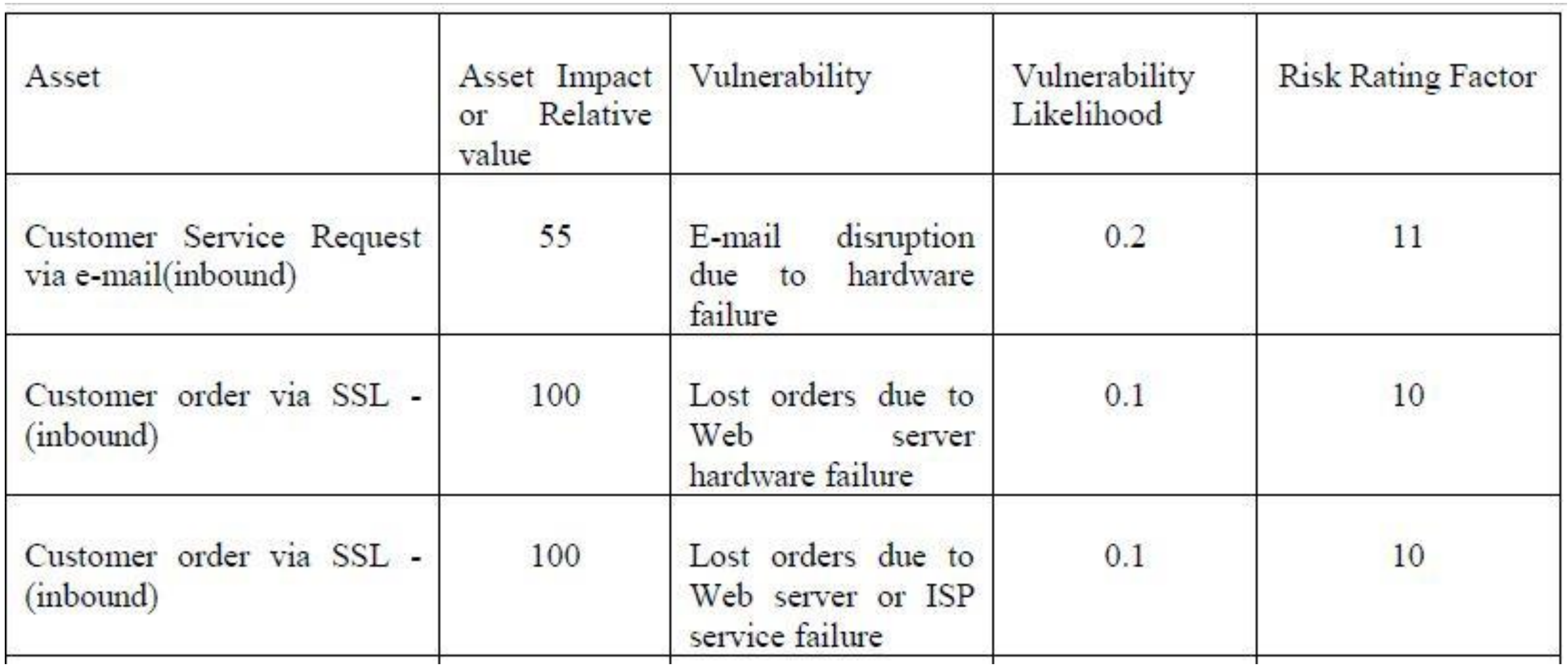
# Types of Access Control

- **Discretionary -** Implemented at discretion or option of the data user
- **Mandatory -** Give users and data owners limited control over access to information resources
- **Nondiscretionary -** Managed by a central authority in the organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)
- **Lattice Based** – Variation of MAC – Users are assigned matrix of authorization for particular area of access.

# Documenting the result of risk assessment

- By the end of the Risk Assessment process, you probably have a collection of long lists of information assets with data about each of them.
- The goal of this process is to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection.
- You should also have collected some information about the controls that are already in place.

# Worksheet Level 2



| Asset | Asset Impact or Relative value | Vulnerability | Vulnerability Likelihood | Risk Rating Factor |
|---|---|---|---|---|
| Customer Service Request via e-mail(inbound) | 55 | E-mail disruption due to hardware failure | 0.2 | 11 |
| Customer order via SSL - (inbound) | 100 | Lost orders due to Web server hardware failure | 0.1 | 10 |
| Customer order via SSL - (inbound) | 100 | Lost orders due to Web server or ISP service failure | 0.1 | 10 |

# Risk control strategy

- Avoidance
- Mitigation
- Transference
- Acceptance

# Avoidance control strategy

- Defend control strategy attempts to prevent the exploitation of vulnerability.
- This is the preferred approach and is accomplished by means of countering threats , vulnerabilities from assets , limiting access to asset and adding protecting

**Common methods of Defend**

1. Application of policy
2. Education and training
3. Application of technology

# Mitigate control strategy

- Mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
- Mitigation begins with the early detection that an attack is in progress and the ability of the organization to respond quickly, efficiently and effectively.

There are three types of plan

1. Incident Response plan – Actions to take while incident is in progress
2. Disaster Recovery plan  - Most common mitigation procedure
3. Business Continuity plan – Continuation of business activities

# Incidence Response plan

- It will be taken while the incident in progress.

This IRP Plan provides answers to questions such as

1. What do I do now?
2. What should the administrator do first?
3. Whom should they contact?
4. What should they document?

- Ex. For example, a system’s administrator may notice that someone is copying information from the server without authorization, signaling violation of policy by a potential hacker or an unauthorized employee

# Disaster Recovery Plan

- It includes entire spectrum of activities used to recover from the incident.

Includes :

  - All preparations for the recovery process
  - Strategies to limit losses during the disaster
  - Detailed steps to follow when the smoke clears
  - The dust settles, or the
  - Floodwater recede.

- DRP focuses more on preparations completed before and actions taken after the incident, whereas the IRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

# Business Continuity Plan

- BCP is the most strategic and long term of the three plans.
- It encompasses the continuation of business activities if a catastrophic event occurs, such as the loss of an entire database, building or operations center.

BCP Includes:

- Planning the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations.
- Many companies offer this service as a contingency against disastrous events such as fires. Floods, earthquakes, and most natural disasters.

# Transfer control strategy

- It is an control approach that attempts to Shift the risk to other assets, other process , or other organizations
- It may be accomplished through
  - Rethinking how services are offered
  - Revising deployment model
  - Purchasing Insurance
  - Outsourcing to other organization
  - Implementing Service contract

**Information Security mistake made by individuals :**

E.g. Password on post it notes, Leaving unattended computers on, Poor password, Plug & Play

**Soln**: Should hire an Quality Security Management and with admin experience.

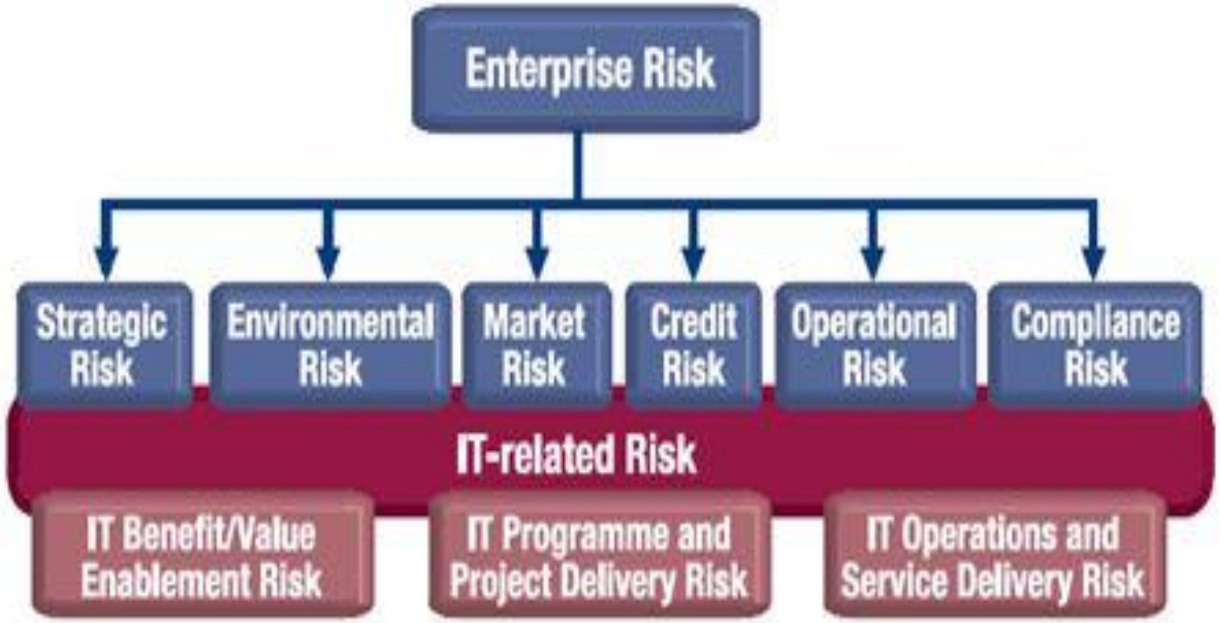
# Accept control strategy

- Is the choice to do nothing to protect a vulnerability and to accept the outcome of its explanation.

**Acceptance is valid only when :**

- Determined the level of risk
- Assessed the probability of attack
- Estimated the potential damage that could occur from attacks
- Performed a thorough cost benefit analysis
- Decided that the particular function, service, information, or asset did not justify the cost of protection

# Risk in an organization



s here

# IT Risk

- 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 risk can be categorized in different ways:

1. IT benefit/value enablement risk—Associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or as an enabler for new business initiatives

2. IT programme and project delivery risk—Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes.

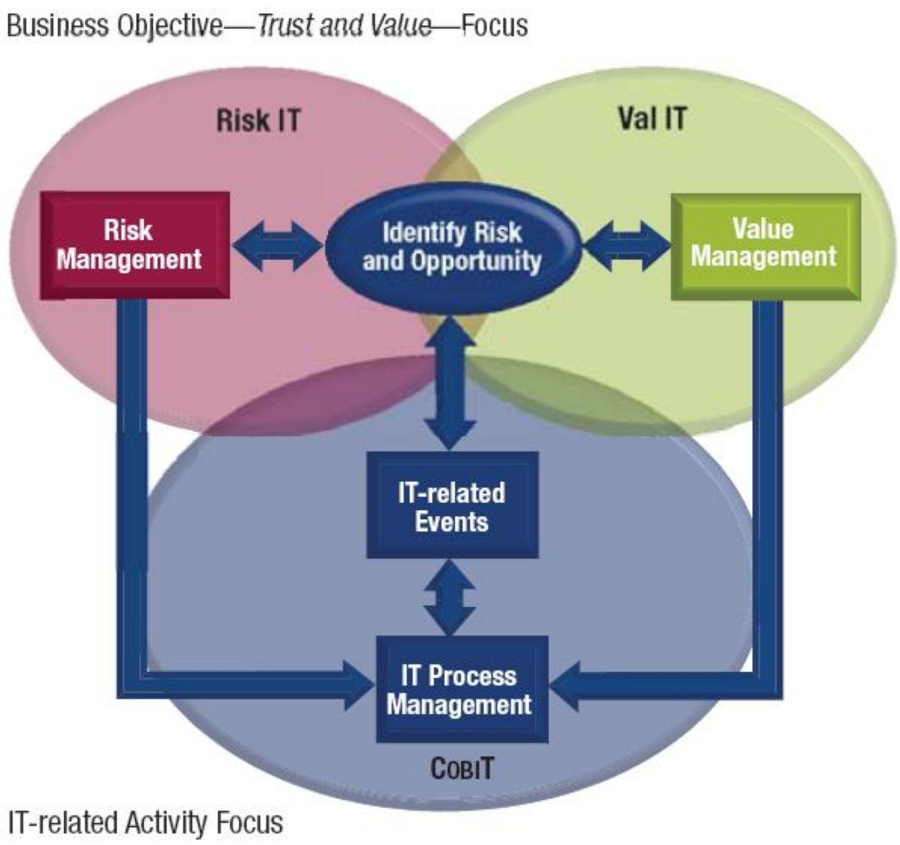
3. IT operations and service delivery risk—Associated with all aspects of the performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

- Many IT risk issues can occur because of third-party problems (service delivery as well as solution development)—both IT third parties and business partners

# Risk-IT Framework

- Risk IT is the first global IT-related risk guidance to provide a comprehensive view of *business* risks related to IT initiatives.
- Risk IT helps enterprises manage risk to achieve goals, seize opportunities and seek greater return.
- Although it is based on, and extends COBIT, Risk IT provides excellent stand-alone guidance.
- Risk IT helps integrate other generic and domain-specific risk management standards and practices.

# Extends COBIT and Val IT


Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
COBIT
IT-related Activity Focus

Risk IT complements and extends COBIT and Val IT to make a more *complete* IT governance guidance resource.

# IT-Related Risk Management

Risk IT is not limited to information security. It covers *all* IT-related risks, including:

- Late project delivery
- Not achieving enough value from IT
- Compliance
- Misalignment
- Obsolete or inflexible IT architecture
- IT service delivery problems

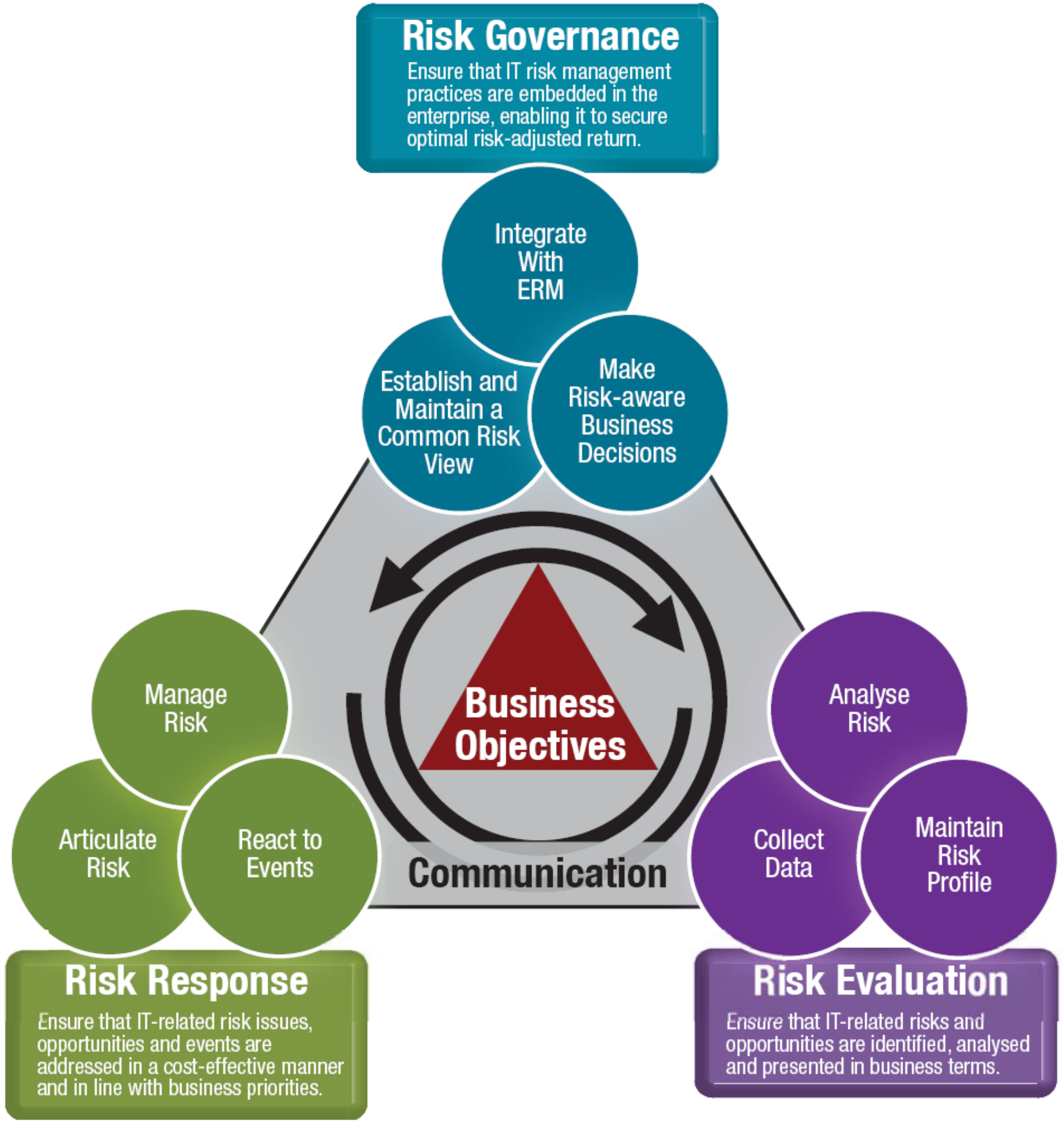
# What it Offers

- Provides guidance to help executives and management ask the key questions, make better, more informed risk-adjusted decisions and guide their enterprises so risk is managed effectively
- Helps save time, cost and effort with tools to address business risks
- Integrates the management of IT-related business risks into overall enterprise risk management
- Helps leadership understand the enterprise’s risk appetite and risk tolerance
- Provides practical guidance driven by the needs of enterprise leadership around the world

# Guiding Principles of Risk IT

- Always connect to enterprise objectives
- Align the management of IT-related business risk with overall enterprise risk management
- Balance the costs and benefits of managing risk
- Promote fair and open communication of IT risk
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Understand that this is a continuous process and an important part of daily activities

# Three Domains of Risk-IT



**Risk Governance**

Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

**Risk Response**

Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

**Risk Evaluation**

Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

# Risk Governance

- Risk Governance: Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. It is based on the following processes:
- RG1 Establish and Maintain a Common Risk View
  - RG1.1 Perform enterprise IT risk assessment
  - RG1.2 Propose IT risk tolerance thresholds
  - RG1.3 Approve IT risk tolerance
  - RG1.4 Align IT risk policy
  - RG1.5 Promote IT risk aware culture
  - RG1.6 Encourage effective communication of IT risk
- RG2 Integrate With ERM
  - RG2.1 Establish and maintain accountability for IT risk management
  - RG2.2 Coordinate IT risk strategy and business risk strategy
  - RG2.3 Adapt IT risk practices to enterprise risk practices
  - RG2.4 Provide adequate resources for IT risk management
  - RG2.5 Provide independent assurance over IT risk management
- RG3 Make Risk-aware Business Decisions
  - RG3.1 Gain management buy in for the IT risk analysis approach
  - RG3.2 Approve IT risk analysis
  - RG3.3 Embed IT risk consideration in strategic business decision making
  - RG3.4 Accept IT risk
  - RG3.5 Prioritize IT risk response activities

# Risk Evaluation

- Ensure that IT-related risks and opportunities are identified, analyzed and presented in business terms. It is based on the following processes:
- RE1 Collect Data
  - RE1.1 Establish and maintain a model for data collection
  - RE1.2 Collect data on the operating environment
  - RE1.3 Collect data on risk events
  - RE1.4 Identify risk factors
- RE2 Analyze Risk
  - RE2.1 Define IT risk analysis scope
  - RE2.2 Estimate IT risk
  - RE2.3 Identify risk response options
  - RE2.4 Perform a peer review of IT risk analysis
- RE3 Maintain Risk Profile
  - RE3.1 Map IT resources to business processes
  - RE3.2 Determines business criticality of IT resources
  - RE3.3 Understand IT capabilities
  - RE3.4 Update risk scenario components
  - RE3.5 Maintain the IT risk register and iT risk map
  - RE3.6 Develop IT risk indicators

# Risk Response

- **Risk Response**: Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities. It is based on the following processes:
- RR1 Articulate Risk
  - RR1.1 Communicate IT risk analysis results
  - RR1.2 Report IT risk management activities and state of compliance
  - RR1.3 Interpret independent IT assessment findings
  - RR1.4 Identify IT related opportunities
- RR2 Manage Risk
  - RR2.1 Inventory controls
  - RR2.2 Monitor operational alignment with risk tolerance thresholds
  - RR2.3 Respond to discovered risk exposure and opportunity
  - RR2.4 Implement controls
  - RR2.5 Report IT risk action plan progress
- RR3 React to Events
  - RR3.1 Maintain incident response plans
  - RR3.2 Monitor IT risk
  - RR3.3 Initiate incident response
  - RR3.4 Communicate lessons learned from risk events

Feel Free to ask for Any query

Ajay Shriram Kushwaha