RISK MANAGEMENT

ALDRIN P. OBSANGA
Polytechnic University of the Philippines
College of Computer and Information Sciences

Learning Outcomes

At the end of this lecture, the student will be able to:

- Define risk management, risk identification, and risk control
- Describe how risk is identified and assessed
- Assess risk based on probability of occurrence and likely impact
- Explain the fundamental aspects of documenting risk via the process of risk assessment
- Describe the various risk mitigation strategy options
- Identify the categories that can be used to classify controls
- Recognize the existing conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis
- Describe how to maintain and perpetuate risk controls

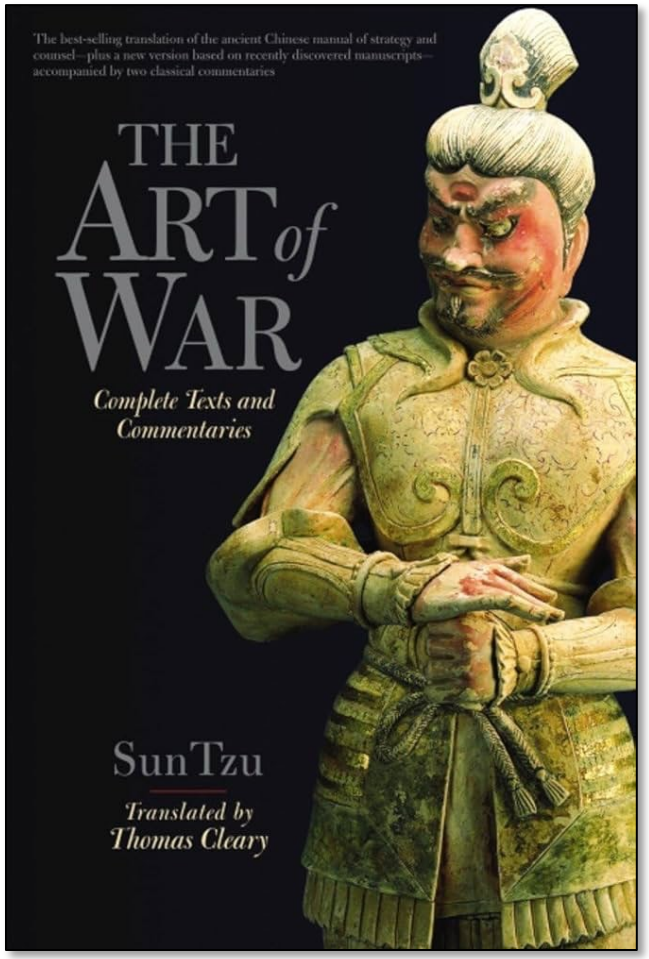
OVERVIEW OF RISK MANAGEMENT

ALDRIN P. OBSANGA
Polytechnic University of the Philippines
College of Computer and Information Sciences

OVERVIEW OF RISK MANAGEMENT
Defining Risk Management

- **Risk Management:** The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.
- A key responsibility for every manager.
- Relies on formal and repeatable processes.
- Essential for protecting information assets and ensuring the organization can achieve its mission.

OVERVIEW OF RISK MANAGEMENT
Sun Tzu and the Art of Risk Management



"If you know the 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 neither the enemy nor yourself, you will succumb in every battle." – Sun Tzu

OVERVIEW OF RISK MANAGEMENT
Sun Tzu and the Art of Risk Management

- **Know Yourself:** Identify, examine, and understand the organization's information and systems.
  - What are the assets?
  - Where are they located?
  - How do they add value?
  - What are their vulnerabilities?
  - What protections are already in place and are they effective?
- **Know the Enemy:** Identify, examine, and understand the threats facing the organization.
  - Which threats most directly affect security?
  - Rank threats based on the importance of the assets they target.

RISK MANAGEMENT FRAMEWORK AND RISK MANAGEMENT PROCESS

ALDRIN P. OBSANGA
Polytechnic University of the Philippines
College of Computer and Information Sciences

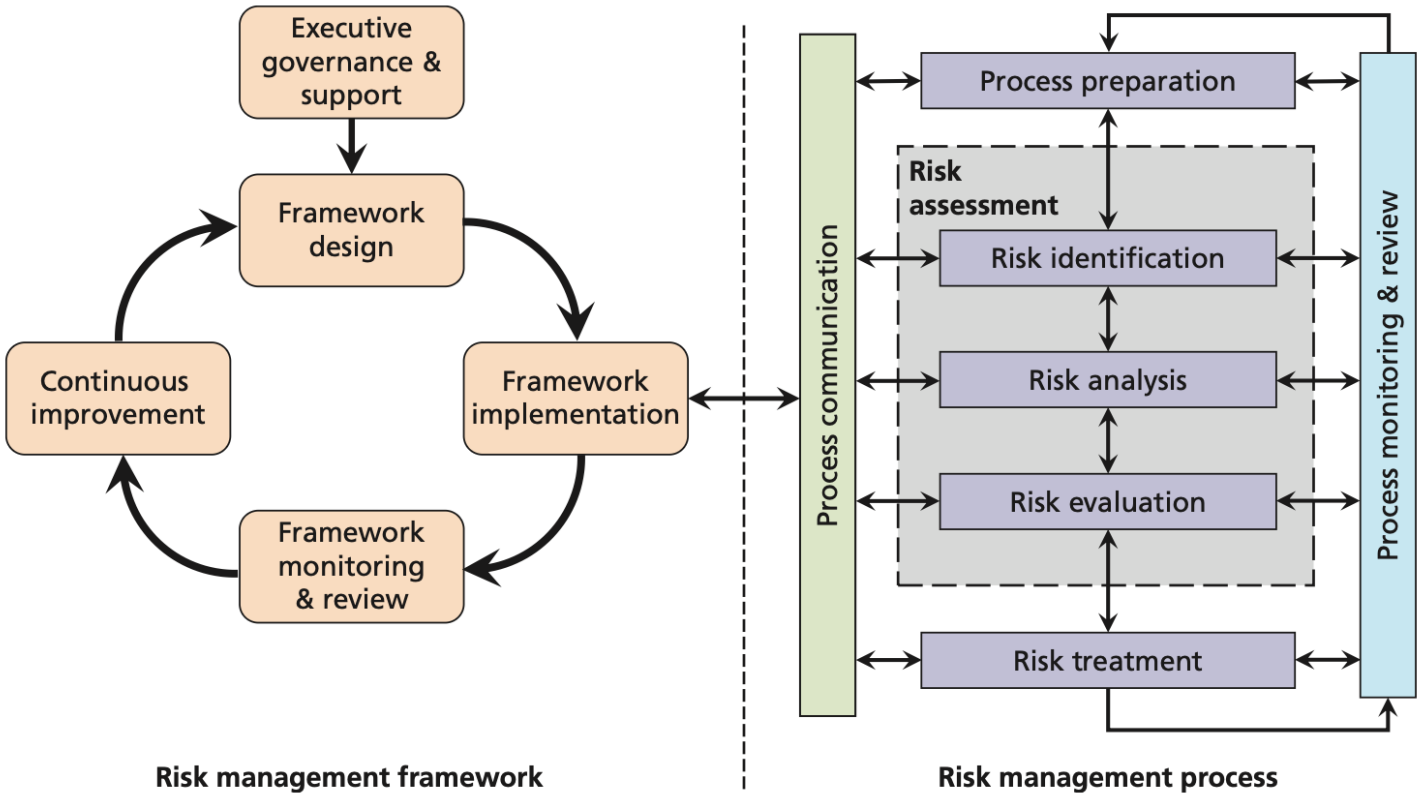
RISK MANAGEMENT FRAMEWORK AND PROCESS
Structuring Risk Management

- Risk management involves discovering and understanding answers to some key questions about the risk associated with an organization's information assets:
  1. Where and what is the risk (risk identification)?
  2. How severe is the current level of risk (risk analysis)?
  3. Is the current level of risk acceptable (risk evaluation)?
  4. What do I need to do to bring the risk to an acceptable level (risk treatment)?

RISK MANAGEMENT FRAMEWORK AND PROCESS
Structuring Risk Management

- **Risk Assessment**: the identification, analysis, and evaluation of risk as initial parts of risk management.
- **Risk Treatment**: the application of safeguards or controls to reduce the risks to an organization's information assets to an acceptable level. Also known as ***risk control***.

RISK MANAGEMENT FRAMEWORK AND PROCESS



- **RM Framework:** The overall structure of the strategic planning and design for the organization's RM efforts.
- **RM Process:** The identification, analysis, evaluation, and treatment of risk to information assets, as specified in the framework.

RISK MANAGEMENT FRAMEWORK
RM Policy

- It is a strategic document that formalizes much of the intent of the governance group.
  - Purpose and scope
  - RM intent and objectives
  - Roles and responsibilities
  - Resource requirements
  - Risk appetite and tolerances
  - RM program development guidelines
  - Special instructions and revision information
  - References to other key policies, plans, standards and guidelines

RISK MANAGEMENT FRAMEWORK
Framework Design

- The framework team begins designing the RM process by which the organization will understand its current levels of risk and determine what, if anything, it needs to do to bring those levels down to an acceptable level in alignment with the risk appetite.
- **Risk management (RM) Plan**: A document that contains specifications for the implementation and conduct of RM efforts.

RISK MANAGEMENT FRAMEWORK
Risk Tolerance and Risk Appetite

- **Residual risk**: the risk to information assets that remains even after current controls have been applied.
- **Risk appetite**: the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.
- **Risk tolerance**: The assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.

RISK MANAGEMENT FRAMEWORK
Risk Tolerance and Risk Appetite

- *A well-defined risk appetite should have the following characteristics:*
  - *Reflective of strategy, including organizational objectives, business plans, and stakeholder expectations.*
  - *Reflective of all key aspects of the business.*
  - *Acknowledges a willingness and capacity to take on risk.*
  - *Is documented as a formal risk appetite statement.*
  - *Considers the skills, resources, and technology required to manage and monitor risk exposures in the context of risk appetite.*
  - *Is inclusive of a tolerance for loss or negative events that can be reasonably quantified.*
  - *Is periodically reviewed and reconsidered with reference to evolving industry and market conditions.*
  - *Has been approved by the board.*

RISK MANAGEMENT FRAMEWORK
Risk Tolerance and Risk Appetite

- **Zero-tolerance risk exposure**: an extreme level of risk tolerance whereby the organization is unwilling to allow any successful attacks or suffer any loss to an information asset.
- **Risk appetite statement**: a formal document developed by the organization that specifies its overall willingness to accept risk to its information assets, based on a synthesis of individual risk tolerances.

RISK MANAGEMENT FRAMEWORK
Framework Implementation

- The organization may distribute the plan to all mid- to upper-level managers for a desk check prior to deployment.
- The organization could pilot-test the plan in a small area to gauge initial issues and success prior to deployment across the entire organization.
- The organization may use a phased approach in which only a portion of the RM program is initially implemented, such as initial meetings with key managers or initial inventory of information assets.
- The bold organization with a larger risk appetite may simply choose a direct cutover in which the new RM project is launched in totality across the entire organization.

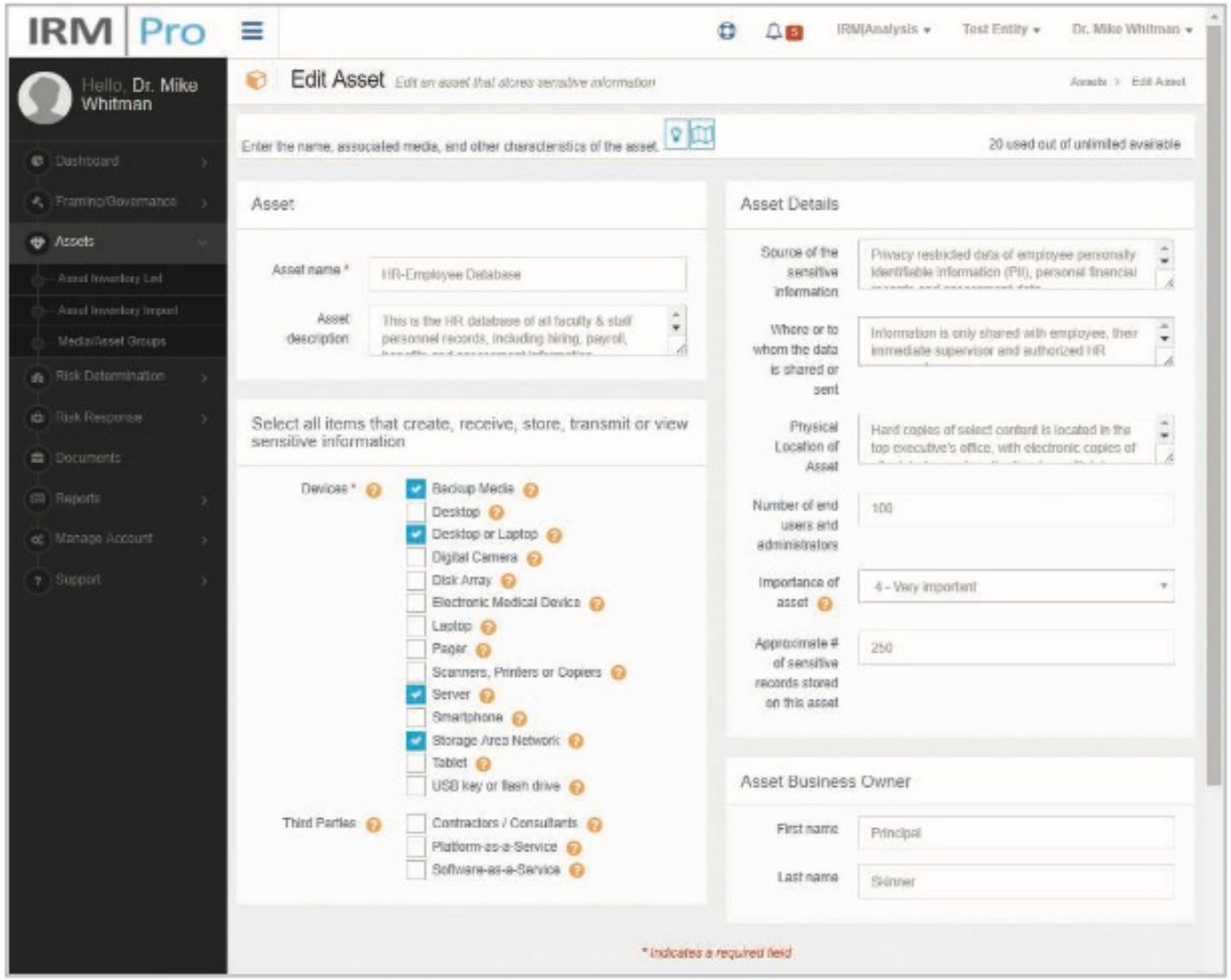
RISK MANAGEMENT PROCESS

ALDRIN P. OBSANGA
Polytechnic University of the Philippines
College of Computer and Information Sciences

RISK MANAGEMENT PROCESS
Step 1: Risk Identification

- **Risk Identification:** The recognition, enumeration, and documentation of risks to an organization's information assets.
- **Key Tasks**
  - Create an inventory of information assets (people, procedures, data, software, hardware, networks).
  - Classify and organize assets meaningfully.
  - Assign a value to each information asset.
  - Identify threats to these assets
  - Pinpoint vulnerable assets by linking specific threats to specific assets (Vulnerability Assessment).

Information System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business-standard procedures IT and business-sensitive procedures
Data	Data/information	Transmission Processing Storage
Software	Software	Applications Operating systems Utilities Security components
Hardware	Hardware	Systems and peripherals Security devices Network-attached process control devices and other embedded systems (Internet of Things)
Networking	Networking	Local area network components Intranet components Internet or extranet components Cloud-based components



Source: Clearwater Compliance IRM.

RISK MANAGEMENT PROCESS
Classifying and Categorizing Information Assets

- **Data Classification Scheme**: A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it.
  - **Confidential**: describes assets that must be protected as critical to the operations and reputation of the organization, such as strategic and marketing plans.
  - **Internal**: describe assets that are for official use and should not be released to the public, like an internal phone directory or memorandum.
  - **Public**: describe anything that can be shared with the general public, like Web content.

RISK MANAGEMENT PROCESS
What's It Worth? Valuing Information Assets

- Assigning relative value helps prioritize protection.
- Consider:
  - Criticality to organizational success?
  - Contribution to revenue/profit generation?
  - Cost to replace?
  - Cost to protect?
  - Embarrassment or liability from loss/compromise?

System Name: SLS E-Commerce

Date Evaluated: February 2022

Evaluated By: D. Jones

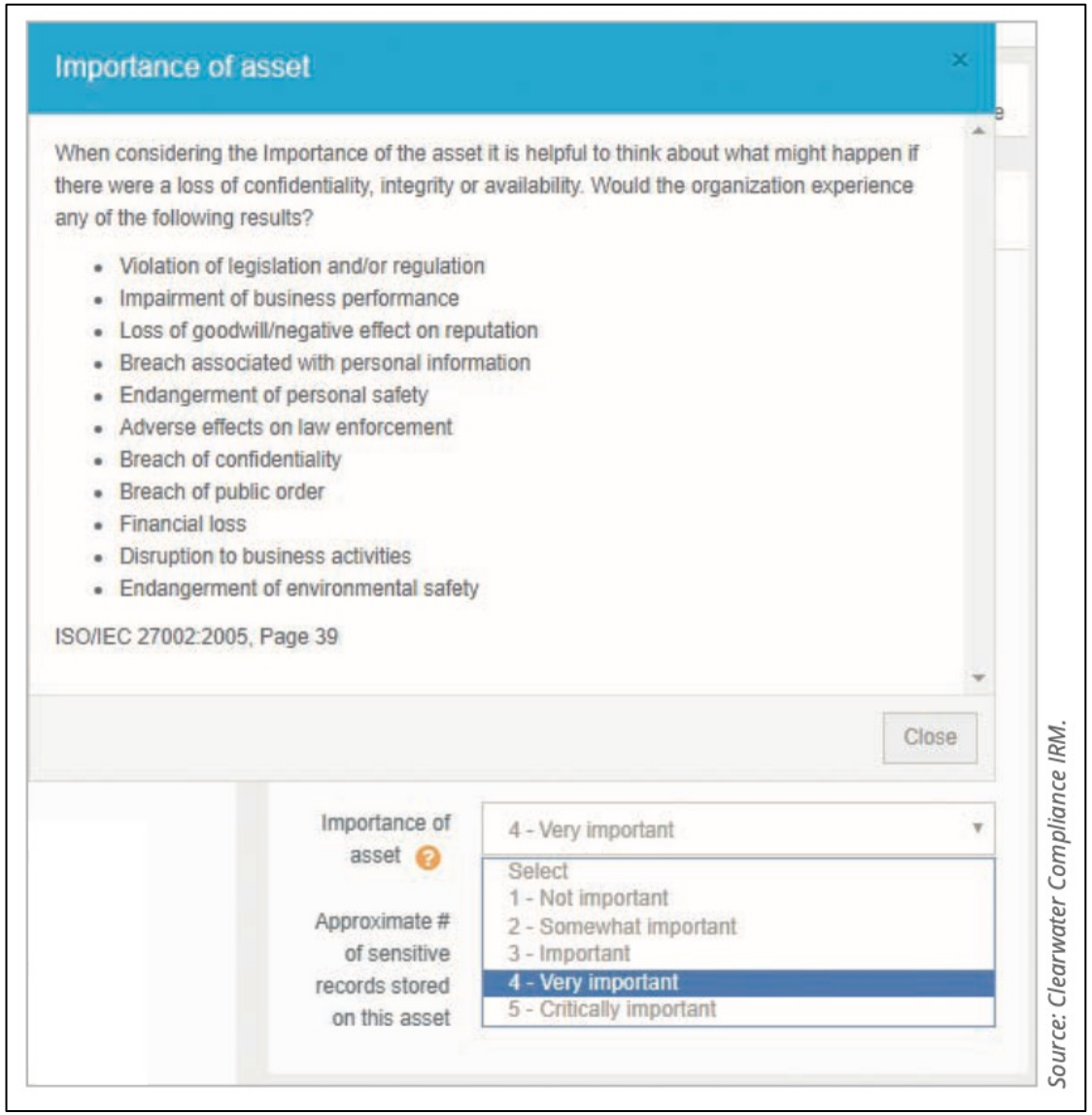
Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge router	Public	Critical
Web server #1 — Home page and core site	Public	Critical
Web server #2 — Application server	Private	Critical

Notes: BOL: Bill of Lading

DMZ: Demilitarized Zone

EDI: Electronic Data Interchange

SSL: Secure Sockets Layer



Source: Clearwater Compliance IRM.

#	Criterion → / Criterion Weight → / Information Asset ↓	*Impact on Revenue*	*Impact on Profitability*	*Impact on Reputation*	TOTAL (1.0)	Importance (0-5; Not Applicable to Critically Important)
		0.3	**0.4**	**0.3**		
1	Customer order via SSL (inbound)	*5*	*5*	*5*	5	Critically Important
2	EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	*5*	*5*	*3*	4.4	Very Important
3	EDI Document Set 2—Supplier orders (outbound)	*4*	*5*	*4*	4.4	Very Important
4	Customer service request via e-mail (inbound)	*3*	*3*	*5*	3.6	Very Important
5	EDI Document Set 3—Supplier fulfillment advice (inbound)	*3*	*3*	*2*	2.7	Important
						4.5 - 5: Critically Important 3.5 - 4.4: Very Important 2.5 - 3.4: Important 1.5 - 2.4: Somewhat Important 0.5 - 1.4: Not Important 0 - 0.4: Not Applicable

RISK MANAGEMENT PROCESS
Understanding Threats and Vulnerabilities

- **Threat Assessment:** An evaluation of the threats to information assets, including a determination of their likelihood of occurrence and potential impact of an attack.
  - Which threats represent the greatest danger?
  - Internal vs. External? Probability of attack? Probability of success? Severity of loss? Organizational preparedness? Cost to protect/recover?
- **Vulnerability Assessment:** Identify specific avenues threat agents can exploit to attack an information asset.
  - A flaw or weakness in an asset, security procedure, design, or control.
  - Compare information assets to threats

Threats to Information Security

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial of services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

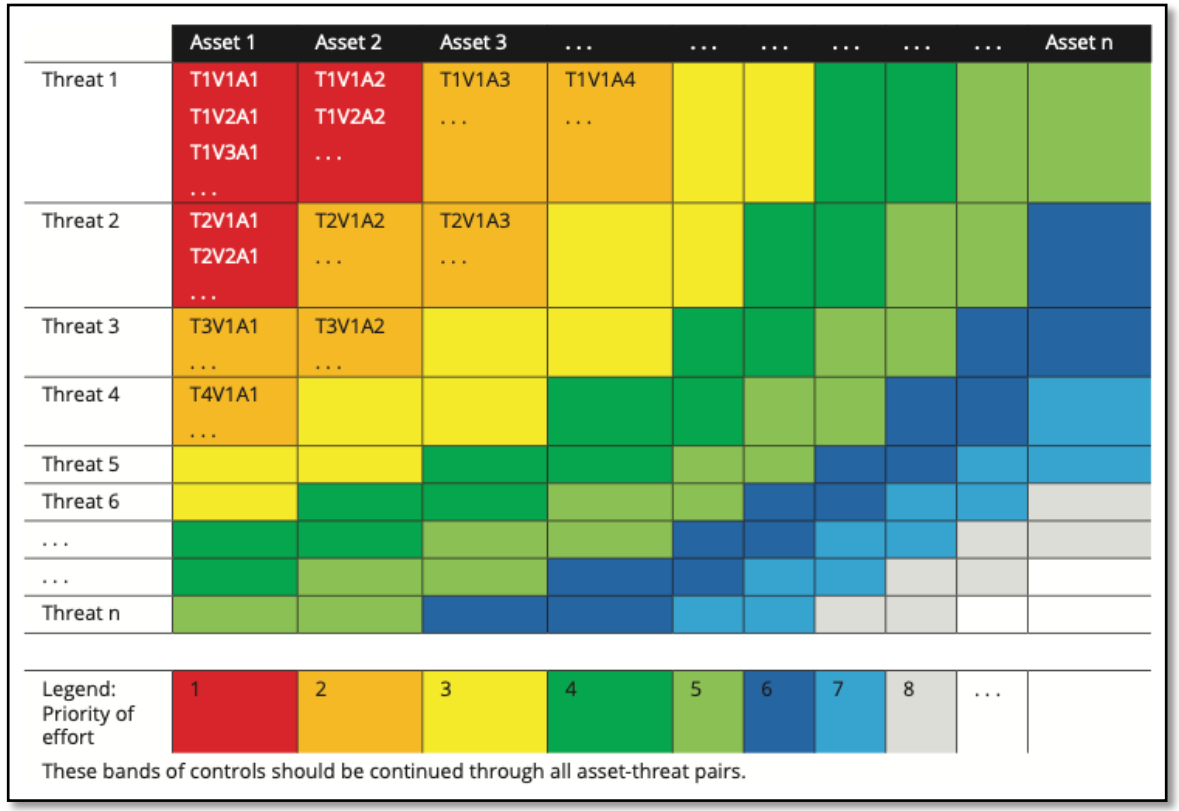
Source: CACM.

Vulnerability of a DMZ Router

Threat	Possible Vulnerabilities
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	Employees or contractors may cause an outage if configuration errors are made.
Information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time.
Sabotage or vandalism	IP is vulnerable to denial-of-service attacks. Device may be subject to defacement or cache poisoning.
Software attacks	IP is vulnerable to denial-of-service attacks. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	Hardware could fail and cause an outage. Power system failures are always possible.
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service.
Theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is stolen.

Step 1: Risk Identification

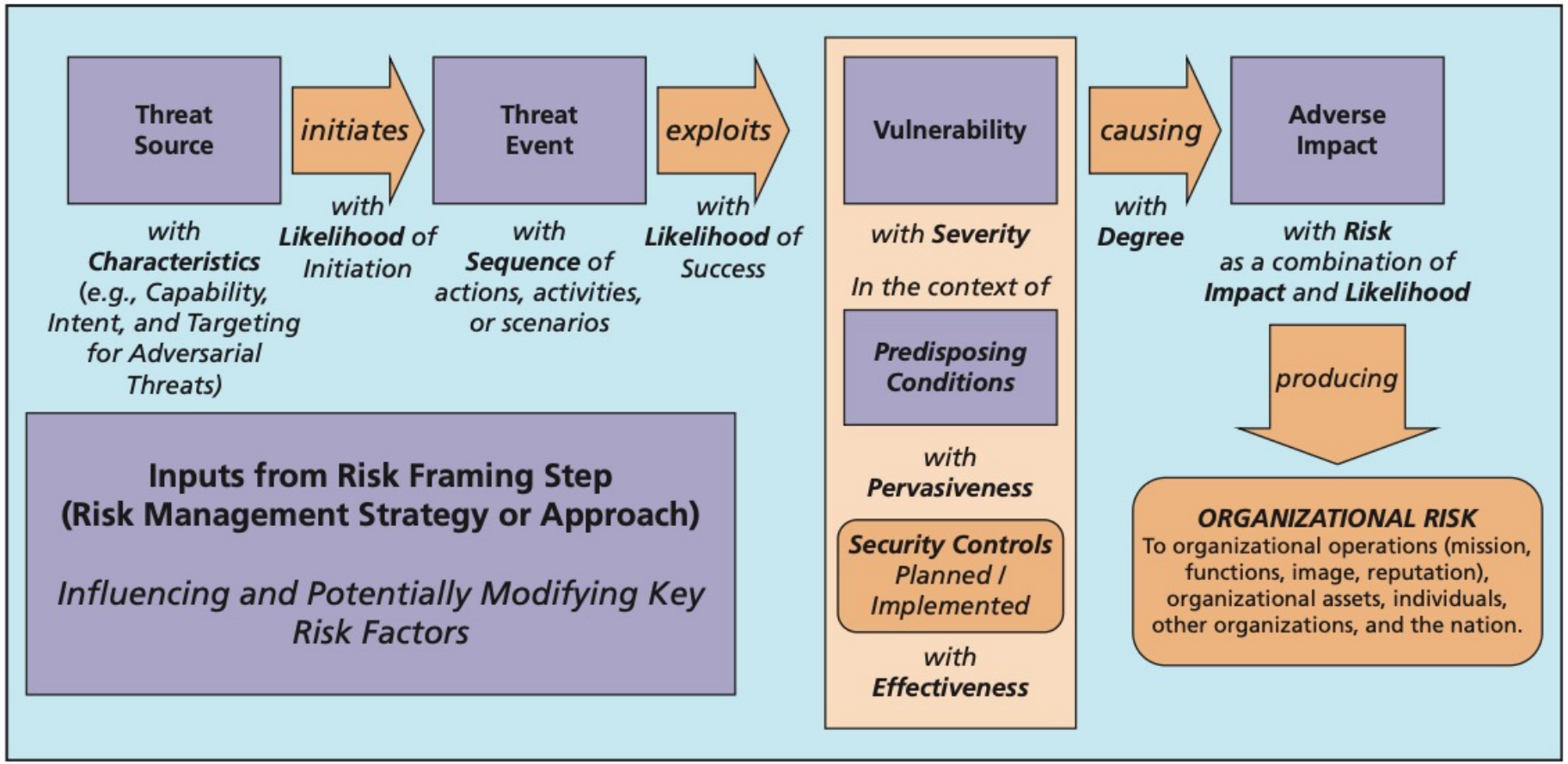
- At the end of the risk identification process, an organization should have (1) a prioritized list of assets and (2) a prioritized list of threats facing those assets.
- The prioritized lists of assets and threats can be combined into a **threats-vulnerabilities-assets (TVA) worksheet** in preparation for the addition of vulnerability and control information during risk assessment.



RISK MANAGEMENT PROCESS
Step 2: Risk Analysis

- **Risk Analysis:** A determination of the extent to which an organization's information assets are exposed tor risk. Assigns a risk rating or score to each specific vulnerability.
  - Goal: Evaluate relative risk of each vulnerability.
  - **Likelihood:** Probability a specific vulnerability within an organization will be attacked by a threat.
  - **Impact:** An understanding of the potential consequences of a successful attack on an information asset by a threat. Magnitude of harm from a successful attack.
  - **Risk Determination:** Risk = Likelihood × Impact (± Uncertainty).
    - **Uncertainty**: The state of having limited or imperfect knowledge of a situation, making it less likely that organizations can successfully anticipate future events or outcomes.

NIST generic risk model with key risk factors



Source: NIST SP 800-30, Rev.1.

Risk Likelihood

Rank	Description	Percent Likelihood	Example
0	Not Applicable	0% likely in the next 12 months	Will never happen
1	Rare	5% likely in the next 12 months	May happen once every 20 years
2	Unlikely	25% likely in the next 12 months	May happen once every 10 years
3	Moderate	50% likely in the next 12 months	May happen once every 5 years
4	Likely	75% likely in the next 12 months	May happen once every year
5	Almost Certain	100% likely in the next 12 months	May happen multiple times a year

Source: Clearwater Compliance IRM.

Risk Impact

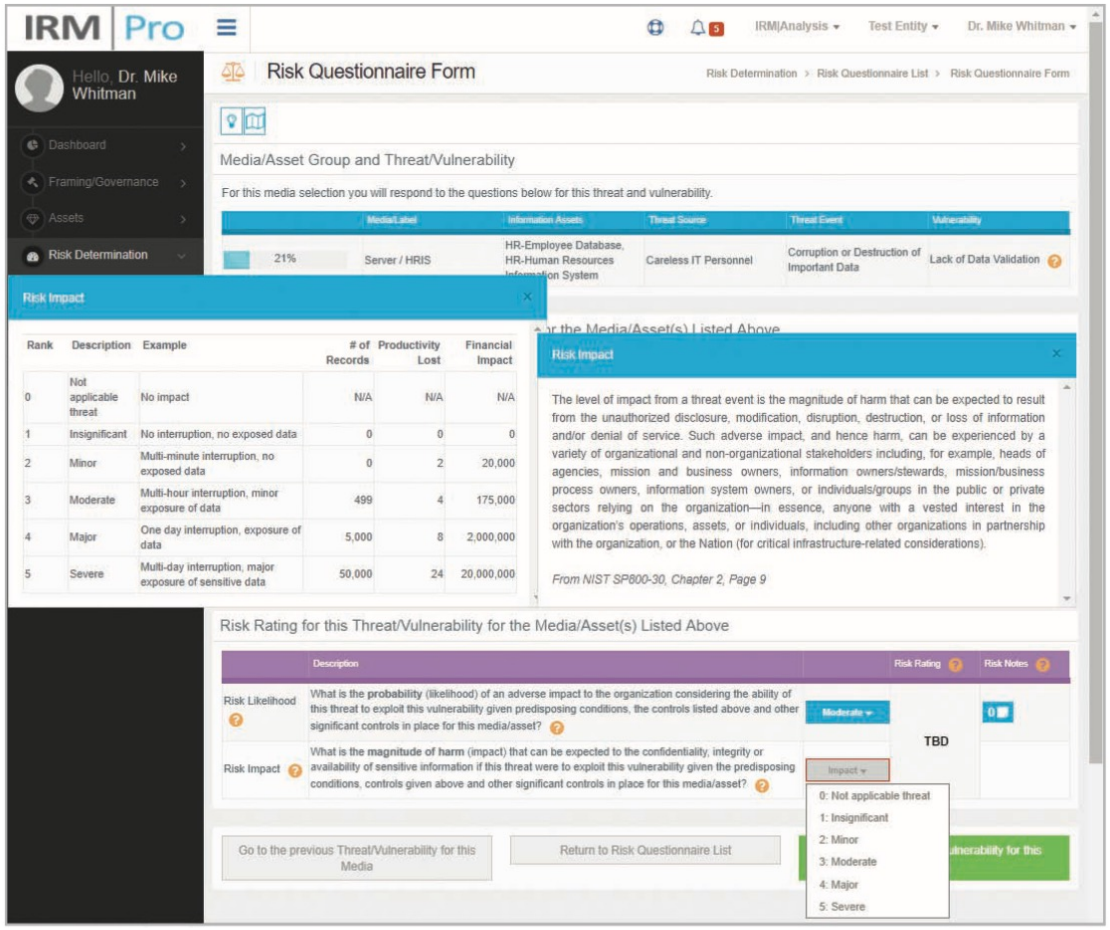


Figure 4-7 Clearwater IRM rating of risk impact

Source: Clearwater Compliance IRM.

Rank	Description	Example	# of Records	Productivity Hours Lost	Financial Impact
0	Not applicable threat	No impact	N/A	N/A	N/A
1	Insignificant	No interruption, no exposed data	0	0	0
2	Minor	Multi-minute interruption, no exposed data	0	2	$20,000
3	Moderate	Multi-hour interruption, minor exposure of data	499	4	$175,000
4	Major	One-day interruption, exposure of data	5,000	8	$2,000,000
5	Severe	Multi-day interruption, major exposure of sensitive data	50,000	24	$20,000,000

Source: Clearwater Compliance IRM.

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5

Figure 4-8 Clearwater IRM risk rating matrix

Source: Clearwater Compliance IRM.

RISK MANAGEMENT PROCESS
Step 2 & 3: Risk Evaluation

- **Risk Evaluation:** Compare the analyzed level of risk against the organization's risk appetite.
  - Is the current level of risk acceptable?
  - If not, risk treatment is required.

RISK MANAGEMENT PROCESS
Documenting Risk Assessment

- Essential for current decision-making and future iterations.

Deliverable	Purpose
Information asset and classification worksheet	Assembles information about information assets, their sensitivity levels, and their value to the organization
Information asset value weighted table analysis	Rank-orders each information asset according to criteria developed by the organization
Threat severity weighted table analysis	Rank-orders each threat to the organization's information assets according to criteria developed by the organization
Threats-Vulnerabilities-Assets (TVA) controls worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization, identifies potential vulnerabilities in the "triples," and incorporates extant and planned controls
Risk ranking worksheet	Assigns a risk-rating ranked value to each TVA triple, incorporating likelihood, impact, and possibly a measure of uncertainty

RISK MANAGEMENT PROCESS
Risk Treatment / Risk Response Strategies

- Reduce residual risk to align with risk appetite.
- Four basic strategies:
  - **Mitigation (or Defense/Risk Mitigation):** Apply controls and safeguards to eliminate or reduce uncontrolled risk.
    - Application of policy.
    - Security Education, Training, and Awareness (SETA) programs.
    - Application of technology.
  - **Transference (or Risk Sharing/Risk Transfer):** Shift risk to other areas or outside entities (e.g., outsourcing, insurance, SLAs).
  - **Acceptance:** Conscious decision to do nothing further after formal evaluation and acknowledgment of risk. Valid only if risk is understood and costs of other treatments are unjustified.
  - **Termination (or Risk Avoidance):** Remove or discontinue the information asset from the operating environment.

RISK CONTROL AND RISK MITIGATION

ALDRIN P. OBSANGA
Polytechnic University of the Philippines
College of Computer and Information Sciences

RISK CONTROL AND RISK MITIGATION
Classifying and Evaluating Controls

- **Categories of Controls**
  - **Managerial:** Policies, procedures, risk management, security planning.
  - **Operational:** Personnel security, physical security, education and training.
  - **Technical:** Logical access controls, cryptography, firewalls, IDPSs.
- **Feasibility and Cost-Benefit Analysis (CBA):** Is implementing the control worth it?
  - **Cost:** Development/acquisition, training, implementation, service, maintenance, potential loss of asset.
  - **Benefit:** Value of preventing loss (often expressed as Annualized Loss Expectancy - ALE).
  - **Asset Valuation:** Crucial for CBA. Can include cost to create, maintain, replace, protect, value to owners/adversaries, productivity/revenue loss.

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Single Loss Expectancy (SLE):** Calculated value associated with the most likely loss from a single occurrence of a specific attack (impact).

SLE = Asset Value (AV) × Exposure Factor (EF)

where EF = Percentage of loss from a given exploited vulnerability.

- Example: A Web site has an estimated value of PhP 1 million, as determined by asset valuation, and a sabotage or vandalism scenario shows that 10 percent of the Web site's value would be damaged or destroyed in such an attack (the EF).

1,000,000 * 0.10 = PhP 100,000 (SLE)

Cost-Benefit Analysis: Quantitative Approach

- **Annualized Rate of Occurrence (ARO):** Expected frequency of an attack per year.
- Example: A successful act of sabotage or vandalism occurs about once every two years, then the ARO would be 50 percent (0.5).
- Example: A network attack that can occur multiple times per second might be successful once per month and thus would have an ARO of 12.

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Annualized Loss Expectancy (ALE):** Overall loss potential per risk, per year.

$$\mathbf{ALE = SLE \times ARO}$$

SLE = PhP 100,000 and ARO = 0.5, then

ALE = PhP 100,000 * 0.5

ALE = PhP 50,000

Thus, the organization could expect to lose PhP 50,000 per year unless it increases its Web security.

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **CBA Formula:**

  CBA = ALE(pre-control) – ALE(post-control) – Annualized Cost of Safeguard (ACS)

where

ALE(pre-control) = ALE of the risk before the implementation of the control

ALE(post-control) = ALE examined after the control has been in place for a period of time

ACS = annualized cost of the safeguard

- A positive CBA suggests the control is financially justifiable.
- Once the controls are implemented, it is crucial to examine their benefits continuously to determine when they must be upgraded, supplemented, or replaced.

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Problem 1:** A popular e-commerce platform selling local crafts has projected annual revenues of ₱10,000,000. They are evaluating a new, advanced security suite to protect their operations.

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
DDoS Attack	₱200,000	1 per quarter
Customer Data Breach	₱1,500,000	1 per 2 years
Payment Fraud	₱5,000	2 per week

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Proposed Safeguard:**
  - **Control:** An advanced DDoS mitigation and fraud detection system.
  - **Annual Cost (ACS):** ₱500,000.
  - **Effectiveness:** This system is expected to reduce the frequency of DDoS attacks by 90% and payment fraud by 75%. It will not affect the likelihood of a customer data breach.

Based on a CBA, should the company invest in the new security suite?

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

1. Calculate the ALE before the control:

- **DDoS Attack:**
  - ARO = 4 (1 per quarter)
  - ALE = ₱200,000 × 4 = **₱800,000**
- **Payment Fraud:**
  - ARO = 104 (2 per week)
  - ALE = ₱5,000 × 104 = **₱520,000**
- **Total ALE (pre-control):** ₱800,000 + ₱520,000 = **₱1,320,000**

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

2. Calculate the ALE after the control:

- **DDoS Attack (90% reduction):**
  - New ALE = ₱800,000 × (1 - 0.90) = **₱80,000**
- **Payment Fraud (75% reduction):**
  - New ALE = ₱520,000 × (1 - 0.75) = **₱130,000**
- **Total ALE (post-control):** ₱80,000 + ₱130,000 = **₱210,000**

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

3. Calculate the Cost-Benefit Analysis (CBA):

- **CBA** = ALE (pre-control) – ALE (post-control) – ACS
- **CBA** = ₱1,320,000 – ₱210,000 – ₱500,000
- **CBA** = **₱610,000**

Yes, the company should invest. The positive CBA of **₱610,000** shows that the system provides a significant financial benefit beyond its cost.

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Problem 2:** A BPO company in Makati handles sensitive client data. The operational value of its main service contract is **₱50,000,000**. Management is considering a new Data Loss Prevention (DLP) system.

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Insider Data Theft	₱2,500,000	1 per 5 years
Ransomware Attack	₱4,000,000	1 per 2 years

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Proposed Safeguard**
  - **Control:** A comprehensive Data Loss Prevention (DLP) software.
  - **Annual Cost (ACS):** ₱750,000.
  - **Effectiveness:** The DLP is expected to reduce the likelihood of insider data theft by 80%. It is not expected to prevent ransomware attacks.

Is the DLP software a financially sound investment according to a CBA?

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

1. Calculate the ALE before the control:

- **Insider Data Theft:**
  - ARO = 0.2 (1 per 5 years)
  - ALE = ₱2,500,000 × 0.2 = **₱500,000**

2. Calculate the ALE after the control:

- **Insider Data Theft (80% reduction):**
  - New ALE = ₱500,000 × (1 - 0.80) = **₱100,000**

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

3. Calculate the Cost-Benefit Analysis (CBA):

- **CBA** = ALE (pre-control) – ALE (post-control) – ACS
- **CBA** = ₱500,000 – ₱100,000 – ₱750,000
- **CBA** = **-₱350,000**

Thus, the company should not invest based purely on this analysis. The negative CBA of **-₱350,000** suggests the annual cost of the DLP system outweighs the financial risk it mitigates for this specific threat. The company might still choose to invest for compliance or reputational reasons, but it's not financially justifiable on its own.

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Problem 3:** A rural bank in Batangas, with assets valued at **₱150,000,000**, is concerned about fraud targeting its employees and customers. They propose a mandatory security awareness training program.

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Phishing (employee)	₱50,000	1 per month
Social Engineering	₱150,000	1 per quarter

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

- **Proposed Safeguard:**
  - **Control:** A recurring security awareness and anti-phishing training program for all employees.
  - **Annual Cost (ACS):** ₱200,000.
  - **Effectiveness:** The training is expected to reduce incidents from both phishing and social engineering by 60%.

What is the result of the CBA for the training program?

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

1. Calculate the ALE before the control:

- **Phishing (employee):**
  - ARO = 12 (1 per month)
  - ALE = ₱50,000 × 12 = **₱600,000**
- **Social Engineering:**
  - ARO = 4 (1 per quarter)
  - ALE = ₱150,000 × 4 = **₱600,000**
- **Total ALE (pre-control):** ₱600,000 + ₱600,000 = **₱1,200,000**

RISK CONTROL AND RISK MITIGATION
Cost-Benefit Analysis: Quantitative Approach

2. Calculate the ALE after the control:

- **Combined Threats (60% reduction):**
  - New ALE = ₱1,200,000 × (1 - 0.60) = **₱480,000**

3. Calculate the Cost-Benefit Analysis (CBA):

- **CBA** = ALE (pre-control) – ALE (post-control) – ACS
- **CBA** = ₱1,200,000 – ₱480,000 – ₱200,000
- **CBA** = **₱520,000**

RISK CONTROL AND RISK MITIGATION
CP Mitigation Plans

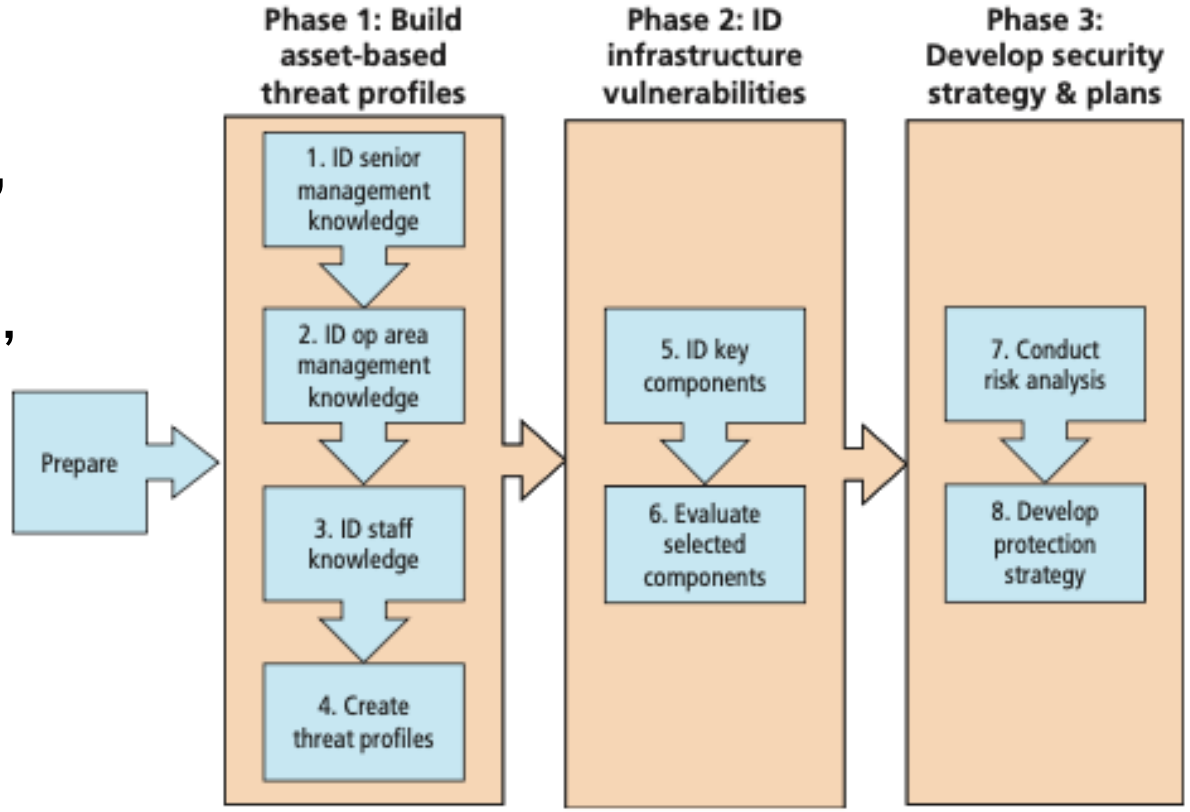
Plan	Description	Example	When Deployed	Time Frame
Incident response (IR) plan	Actions an organization takes during incidents (attacks or accidental data loss)	• List of steps to be taken during an incident • Intelligence gathering • Information analysis	As an incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery (DR) plan	• Preparations for recovery should a disaster occur • Strategies to limit losses before and during a disaster • Step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost technology infrastructure and services • Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery

RISK CONTROL AND RISK MITIGATION
CP Mitigation Plans

Plan	Description	Example	When Deployed	Time Frame
Business continuity (BC) plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DR plan's ability to quickly restore operations	• Preparation steps for activation of alternate data centers • Establishment of critical business functions in an alternate location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organizational stability
Crisis management (CM) plan	Steps to ensure the safety and welfare of the people associated with an organization in the event of an incident or disaster that threatens their well being	• Procedures for the notification of personnel in the event of an incident or disaster • Procedures for communication with associated emergency services • Procedures for reacting to and recovering from personnel safety threats	Immediately after the incident or disaster is deemed to threaten personnel safety	Both short-term safety and long-term personnel welfare stability

RISK CONTROL AND RISK MITIGATION
Alternative Risk Management Methodologies

OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Formerly from SEI, balances protection costs against asset criticality. Had variations for large (OCTAVE), small (OCTAVE-S), and streamlined (OCTAVE-Allegro) organizations.



Alternative Risk Management Methodologies

FAIR (Factor Analysis of Information Risk): A risk management framework developed by Jack A. Jones.

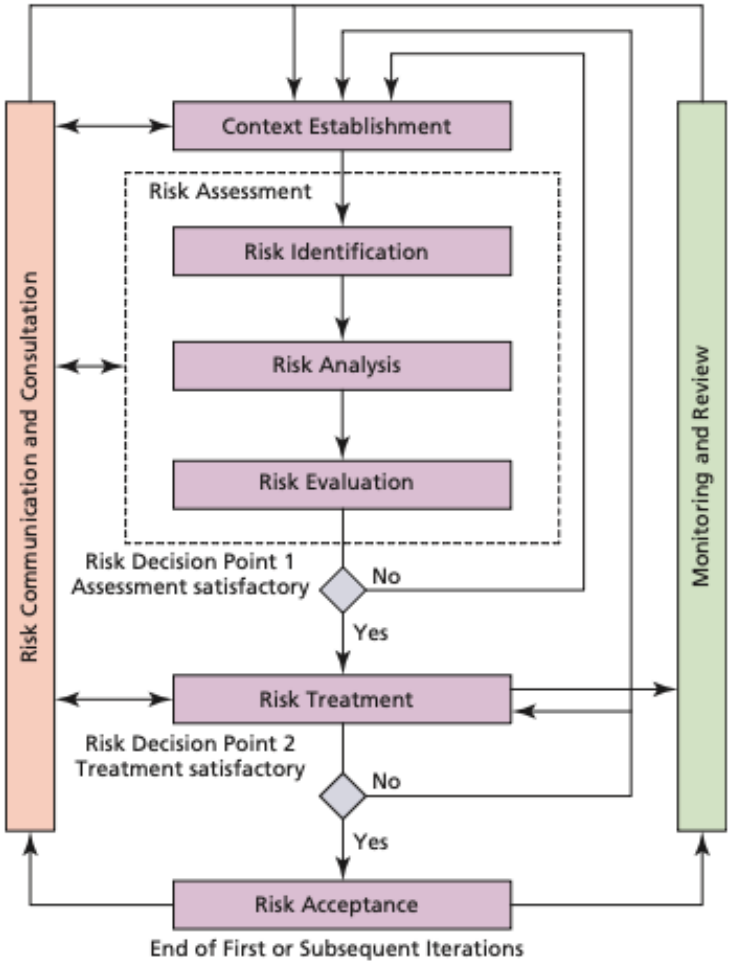
Focuses on understanding, analyzing, and measuring information risk. Now an Open Group standard (Open FAIR™).

FAIR Framework

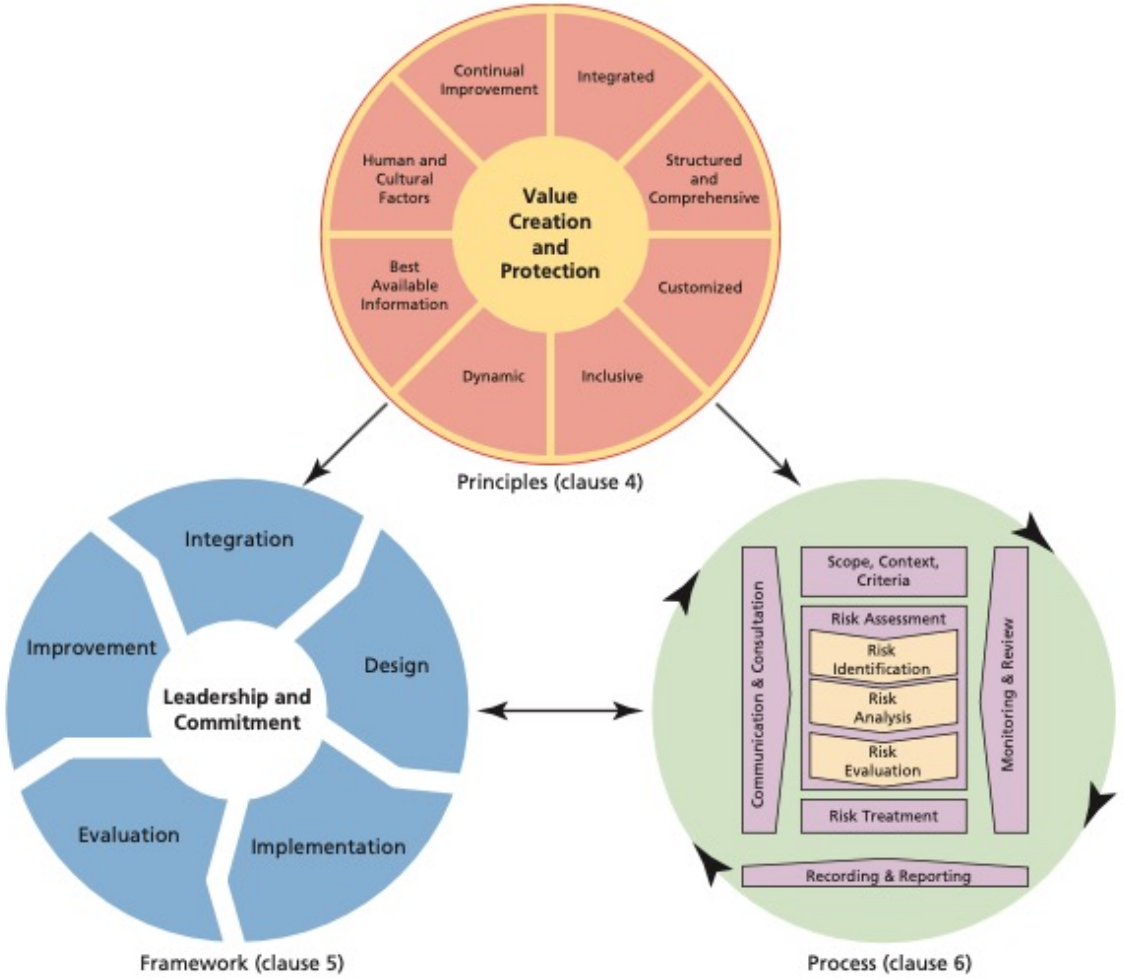
- A taxonomy for information risk
- Standard nomenclature for information risk terms
- A framework for establishing data collection criteria
- Measurement scales for risk factors
- A computational engine for calculating risk
- A modeling construct for analyzing complex risk scenarios

RISK CONTROL AND RISK MITIGATION
Alternative Risk Management Methodologies

- **ISO Standards**
  - **ISO 27005:** Focuses on the information security RM process.
  - **ISO 31000:** More general, includes RM framework and guiding principles for all types of risk.



ISO 31000 risk management principles, framework, and process

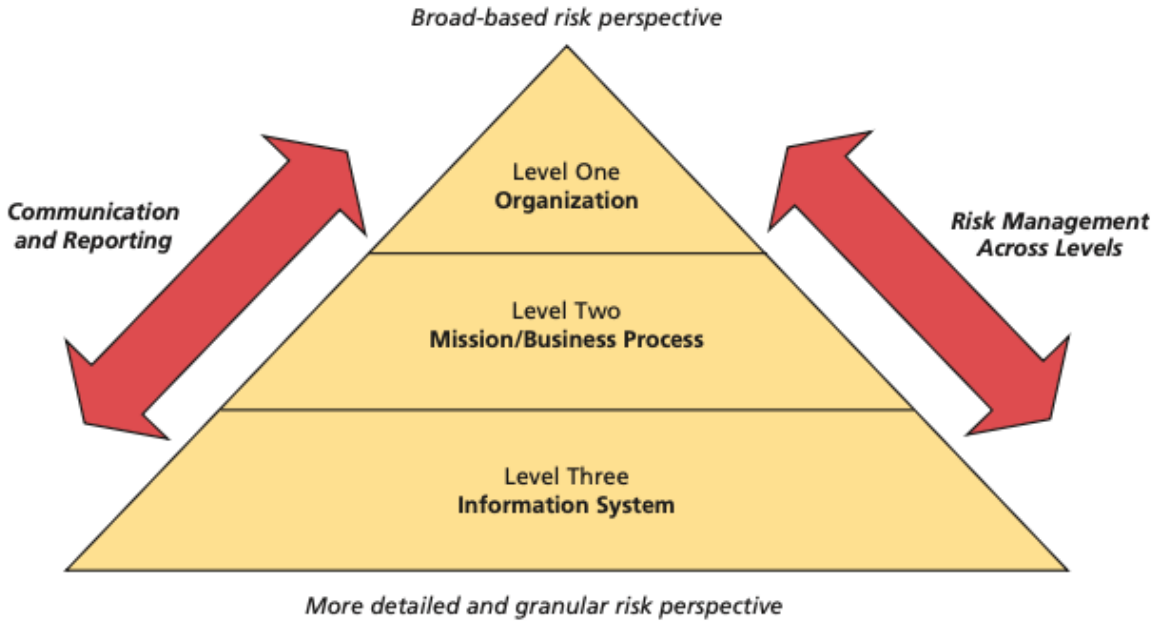


RISK CONTROL AND RISK MITIGATION
Alternative Risk Management Methodologies

NIST Risk Management Framework (RMF): (SP 800-37, SP 800-39) A comprehensive framework for federal systems, widely adopted elsewhere. Emphasizes building security into the system lifecycle and continuous monitoring. https://csrc.nist.gov/publications/sp

RISK CONTROL AND RISK MITIGATION
Alternative Risk Management Methodologies

- NIST's RMF follows a three-tiered approach.
  - Aspects that affect the entire organization, such as governance (Level 1).
  - Tactical issues around business processes (Level 2).
  - Dealing with information systems (and information security) (Level 3).



RISK CONTROL AND RISK MITIGATION
Maintaining and Perpetuating Risk Controls

- Risk management is **not a one-time project**; it's a continuous cycle.
- **Framework Monitoring & Review:** The RM framework itself needs to be assessed and improved. How well is the RM process working?
- **Process Monitoring & Review:** The operational RM process requires ongoing data collection and feedback.
  - Are controls still effective?
  - Has the threat landscape changed?
  - Have asset values or business priorities shifted?
- Results of monitoring feed into continuous improvement efforts for both the framework and the process.

Summary

- Risk Management is fundamental to protecting information assets and enabling organizational objectives.
- It involves a structured framework and a detailed process of identification, analysis, evaluation, and treatment.
- Knowing your assets, their value, the threats they face, and existing vulnerabilities is crucial (Know Yourself, Know Your Enemy).
- Risk assessment involves determining likelihood and impact to prioritize actions.
- Risk treatment strategies include Mitigation, Transference, Acceptance, and Termination.
- Controls are classified and selected based on feasibility and cost-benefit analysis.
- Risk management is a continuous, iterative process.

References

- Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Course Technology.

Thanks!

Keep safe everyone!

If you have question, send me an e-mail.