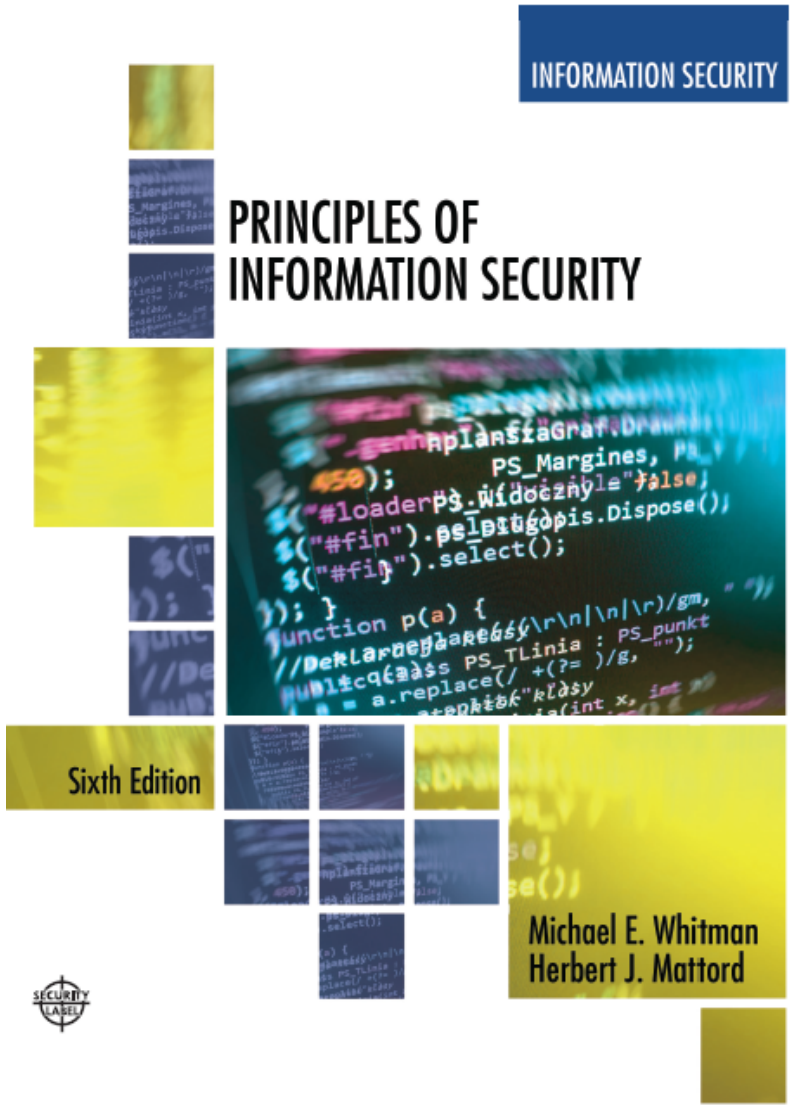


Source: Principles of Information Security

Chapter 5

Risk Management

Dr. Ibrahim Waziri Jr.

Learning Objectives

Upon completion of this material, you should be able to:

- Define risk management, risk identification, risk assessment, and risk control
- Describe how risk is identified and assessed
- Assess risk based on probability of occurrence and likely expected impact
- Explain the fundamental aspects of documenting risk via the process of risk assessment
- Describe various options for a risk mitigation strategy
- Define risk appetite and explain how it relates to residual risk
- Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis

Introduction - Risk Management Overview

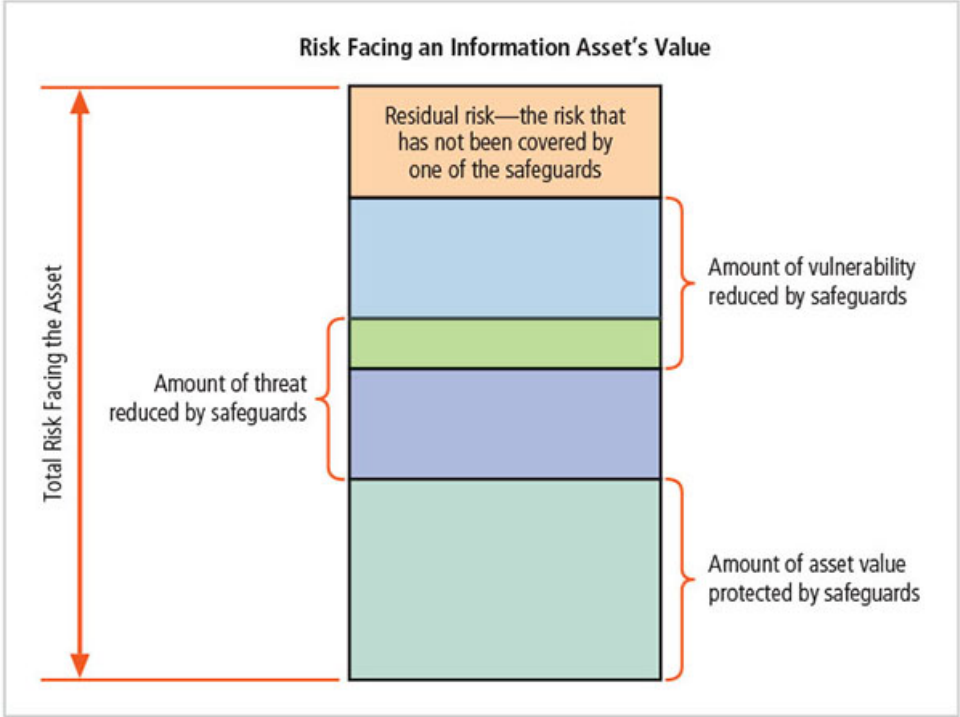
Risk management: The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.

Organizations must design and create safe environments in which business processes and procedures can function.

- Know yourself: identify, examine, and understand the information and systems currently in place
- Know the enemy: identify, examine, and understand the threats facing the organization
- Responsibility of each community of interest within an organization to manage the risks that are encountered - Information security, management and users, and information technology all must work together.

Risk Appetite and Residual Risk

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.



Residual risk: The risk to information assets that remains even after current controls have been applied.

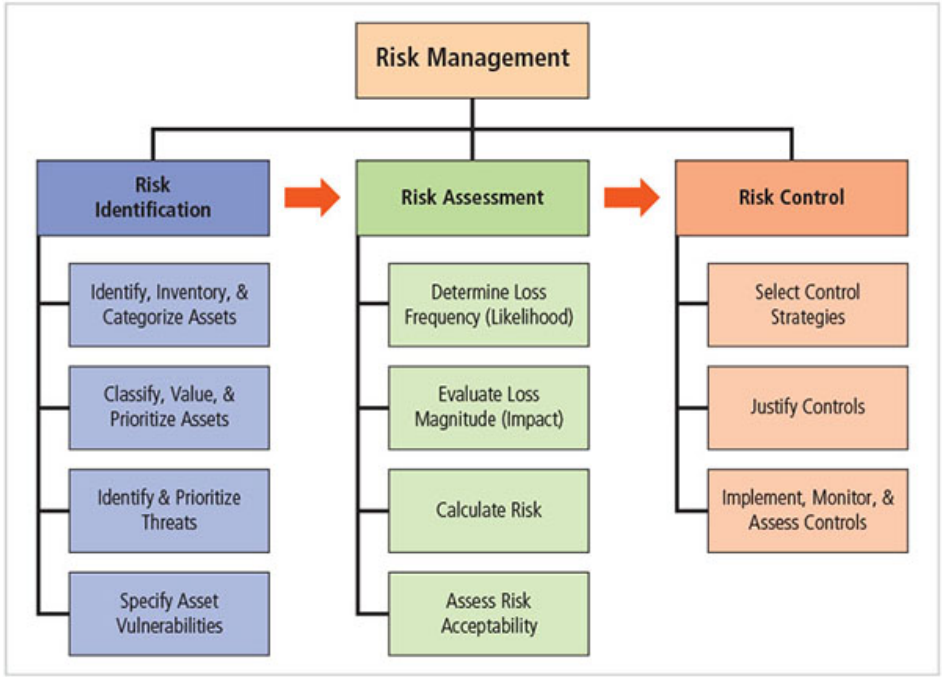
The goal of information security is to bring residual risk into line with risk appetite.

Components of Risk Management

1. **Risk Identification:** The recognition, enumeration, and documentation of risks to an organization's information assets.

2. **Risk Assessment:** A determination of the extent to which an organization's information assets are exposed to risk.

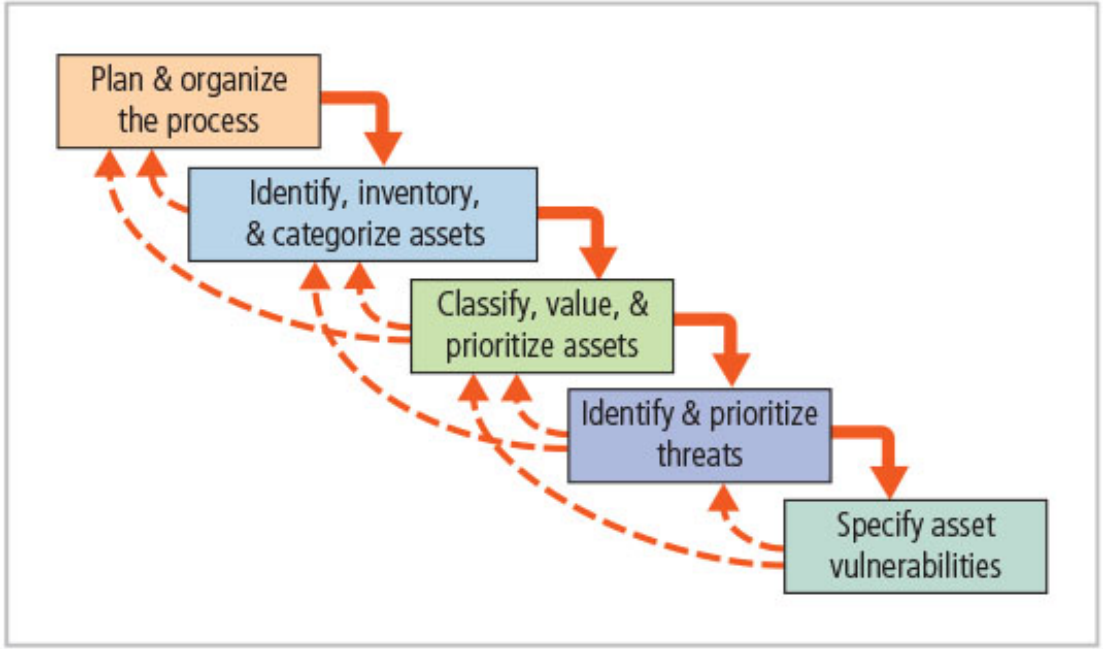
3. **Risk Control:** The application of controls that reduce the risks to an organization's information assets to an acceptable level.



1. Risk Identification

Risk management requires that InfoSec professionals know how to identify, classify, and prioritize an organization's information assets.

A threat assessment process identifies and evaluates the risks facing each asset



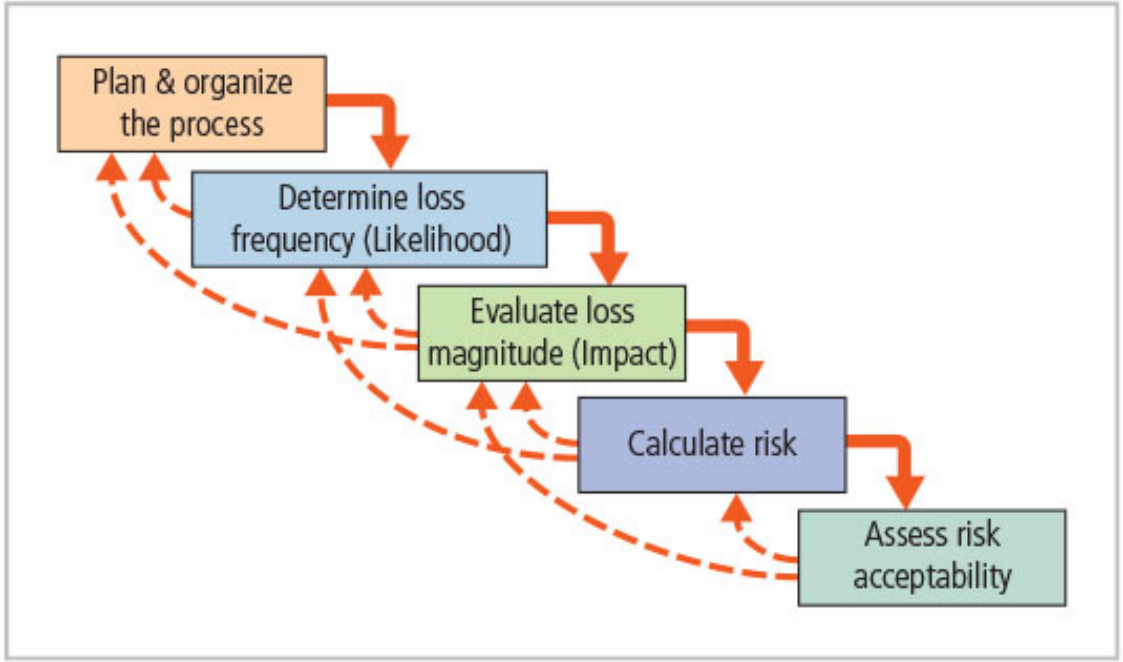
1. Planning and Organizing the Process
2. Identifying, Inventorying and Categorizing Assets
3. Classifying ,Valuing and Prioritizing Information Assets
4. Threat Identification and Prioritization
5. Asset Vulnerability Identification

Example: Vulnerability assessment of a hypothetical DMZ router

Threat	Possible vulnerabilities
Compromises to intellectual property	• Copyrighted works developed in-house and stored on intranet servers can be copied without permission unless the router is configured to limit access from outsiders. • Works copyrighted by others can be stolen: your organization is liable for that loss to the copyright holder.
Espionage or trespass	• This information asset (router) may have little intrinsic value, but other assets protected by this device could be attacked if it does not perform correctly or is compromised.
Forces of nature	• All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error of failure	• Employees or contractors may cause on outage if configuration errors are made.
Information extortion	• If attackers bypass the router or compromise it and then enter your network, they may encrypt your data in place. They may not have stolen it, but unless you pay them to acquire the encryption key, the data is inert and no longer of value to you.
Deviation in quality of service	• Power system failures are always possible. Unless suitable electrical power conditioning is provided, failure is probable over time. • ISP connectivity failures can interrupt internet bandwidth.
Sabotage or vandalism	• The internet protocol is vulnerable to denial of service. • This device may be subject to defacement or cache poisoning.
Software attacks	• The internet protocol is vulnerable to denial of service. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	• Hardware can fail and cause an outage.
Technical software failures or errors	• Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	• If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service.
Theft	• Data has value and can be stolen. Routers are important network devices; their controls are critical layers in your defense in depth. When data is copied in place, you may not know it has been stolen.

2. Risk Assessment

Risk assessment evaluates the relative risk for each vulnerability. Risk Assessment assigns a risk rating or score to each information asset.



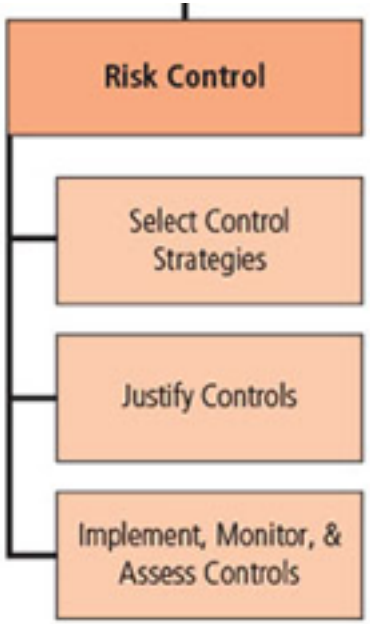
1. Planning and organizing the Process
2. Determine loss frequency (Likelihood)
3. Evaluate loss magnitude (Impact)
4. Calculate risk
   - Risk = Likelihood x Impact
5. Assess risk acceptability

Example: Ranked vulnerability risk worksheet

Asset	Asset relative value	vulnerability	Loss frequency	Loss magnitude
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
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to web server software failure	0.01	1

3. Risk Control

Involves selection of control strategies, justification of strategies to upper management, and implementation/monitoring/on going assessment of adopted controls.



3.1 - Select Control Strategies

Once the ranked vulnerability risk worksheet is complete, the organization must choose one of five strategies to control each risk:

- Defense
- Transference
- Mitigation
- Acceptance
- Termination

3.2 - Justify Control Strategies

3.3 - Implement, Monitor & Assess Controls

3-1: Selecting a Risk Control Strategy

Level of threat and value of asset should play a major role in the selection of strategy.

Rules of thumb on strategy selection can be applied:

- When a vulnerability exists
- When a vulnerability can be exploited
- When attacker's cost is less than the potential gain
- When potential loss is substantial

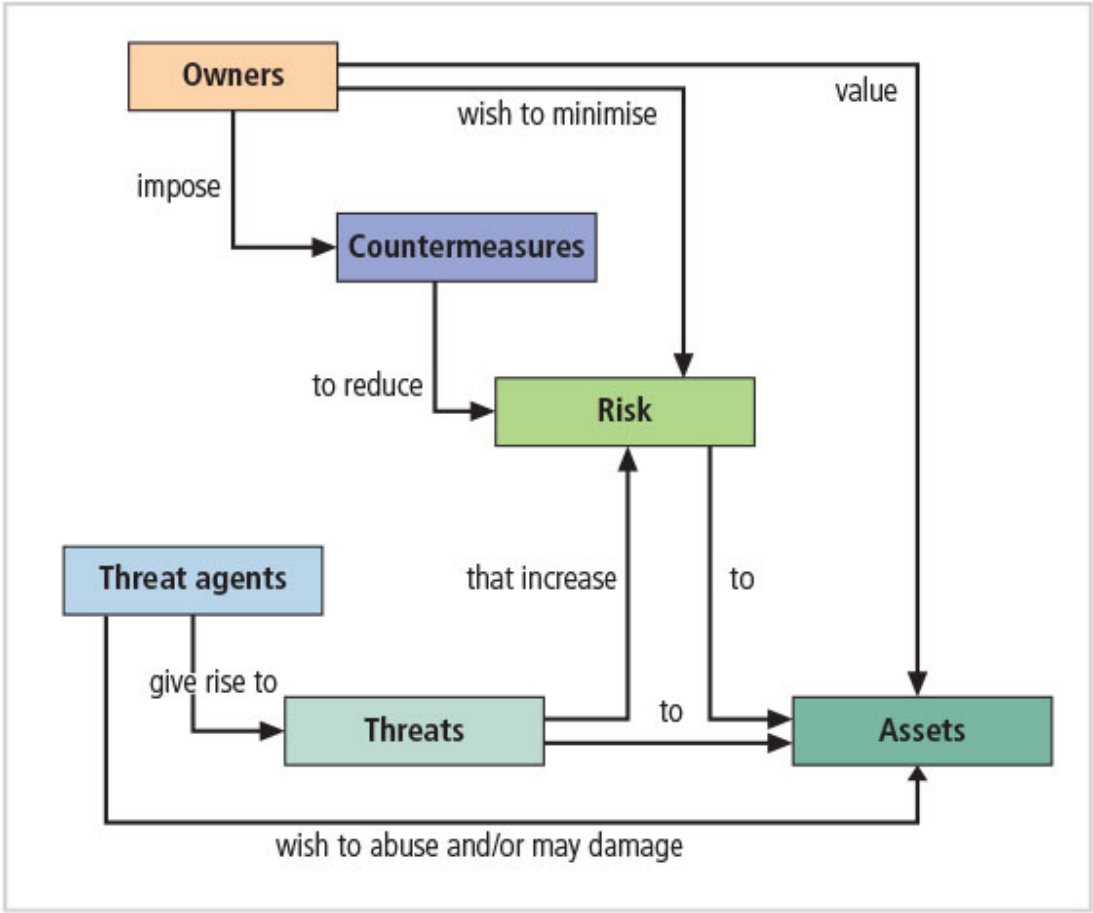


Figure: Relationship of risk to threats, assets, and countermeasures

3-2 - Justifying Risk Controls Strategies

Before implementing one of the control strategies for a specific vulnerability, the organization must explore all consequences of vulnerability to information asset. This includes Items that affect cost of a control or safeguard include cost of development or acquisition, training fees, implementation cost, service costs, and cost of maintenance.

The Two ways to justify risk controls are: **Process Results** and **Cost Benefit Analysis**

Process Results: is the estimate of potential loss per risk. Process result is calculated using:

- Asset Value (AV)
- Exposure Factor (EF)
- Single loss expectancy (SLE) = AV x EF
- Annualized rate of occurrence (ARO)
- Annualized loss expectancy (ALE) = SLE × ARO)

Cost Benefit Analysis (CBA): determines if an alternative being evaluated is worth the cost incurred to control vulnerability. The CBA is most easily calculated using the ALE from earlier assessments, before implementation of the proposed control:

- ALE(prior) is the annualized loss expectancy of risk before implementation of control.
- ALE(post) is the estimated ALE based on control being in place for a period of time.
- ACS is the annualized cost of the safeguard.
- CBA = ALE(prior) – ALE(post) – ACS

The two ways to calculate risk are:

Qualitative = This includes using a non-numerical approach (Survey etc.)
Quantitative = This includes using a numerical approach (Cost, Values & Estimates etc)

3-3: Implementation, Monitoring, and Assessment of Risk Controls

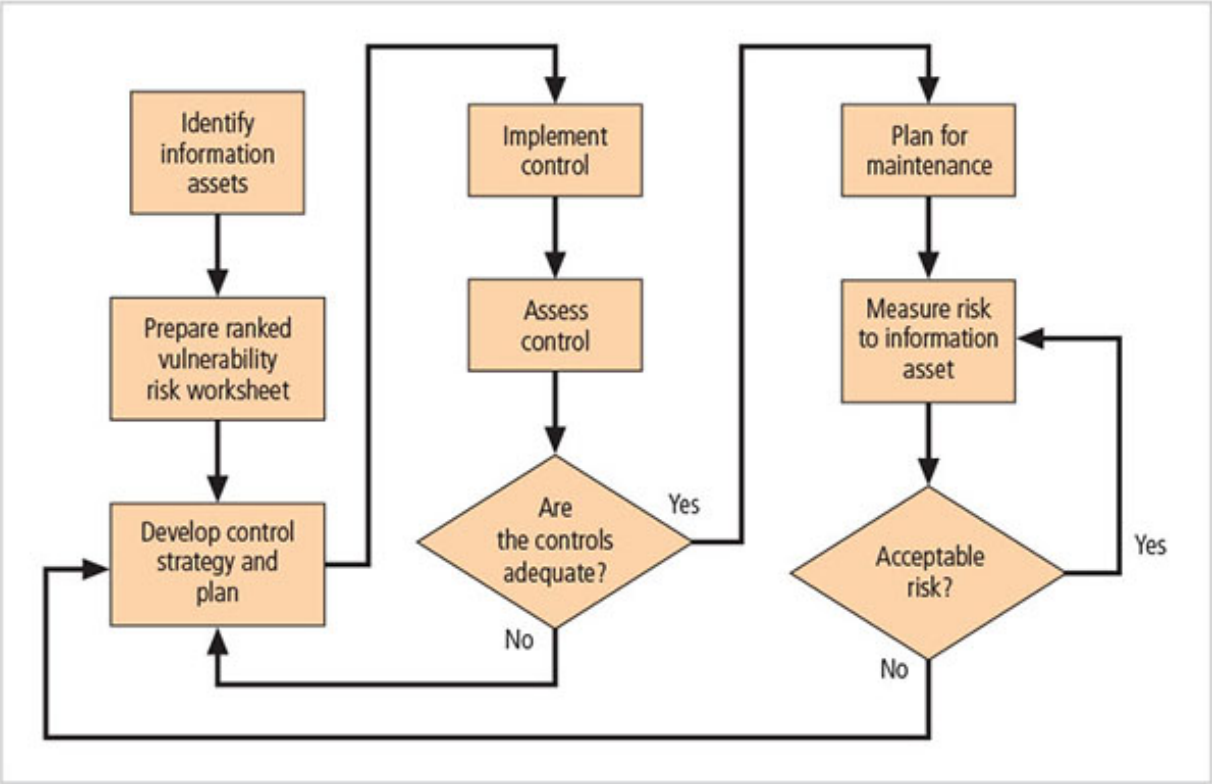


Figure: Risk Control Lifecycle

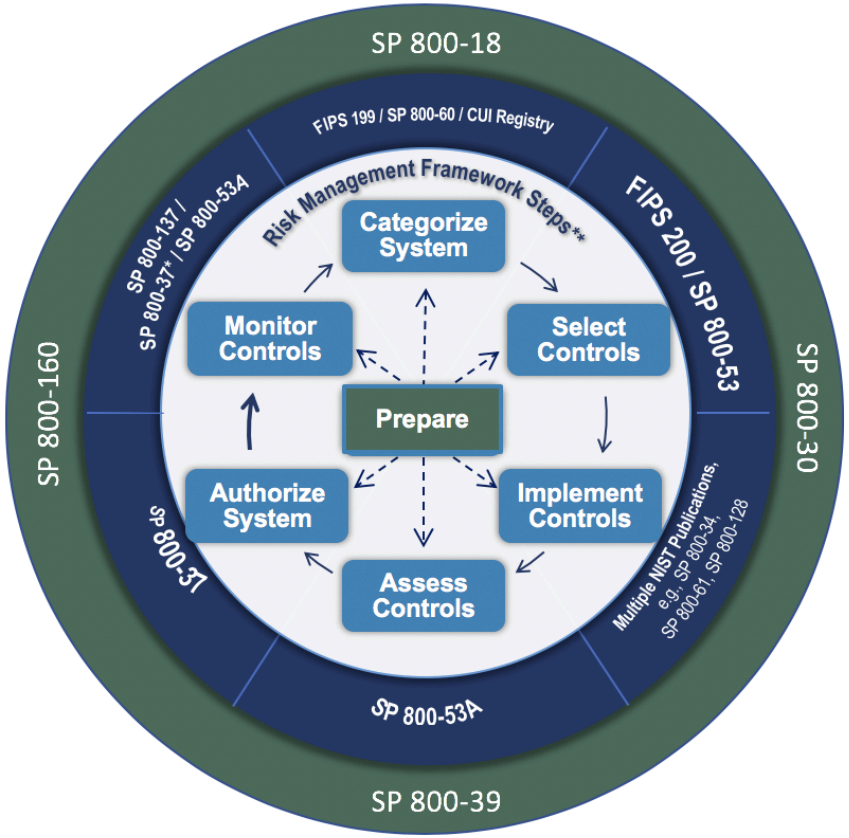
- The selection of the control strategy is not the end of a process.
- Strategy and accompanying controls must be implemented and monitored on on-going basis to determine effectiveness and accurately calculate the estimated residual risk.
- Process continues as long as the organization continues to function.

The NIST Risk Management Framework

The Risk Management Framework provides a process that integrates security and risk management activities into the U.S Federal system development life cycle.

Steps:

1. Prepare
2. Categorize
3. Select
4. Implement
5. Assess
6. Authorize
7. Monitor



Reference: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Benchmarking , Baselining and Best Practices

Benchmarking: process of seeking out and studying practices in other organizations that one's own organization desires to duplicate

- Metrics-based measures - based on numerical standards
- Process-based measures - more strategic and less focused on numbers
- Due Diligence – Knowing what is right
- Due Care – Doing what is right

Baselining: In information security, baselining is comparison of past security activities and events against an organization's future performance.

Best business practices: security efforts that provide a superior level of information protection.

Problems with the application of benchmarking and best practices

- Organizations don't talk to each other (biggest problem).
- No two organizations are identical.
- Best practices are a moving target.
- Researching information security benchmarks doesn't necessarily prepare a practitioner for what to do next.

Recommended Risk Control Practices

- Convince budget authorities to spend up to the value of an asset to protect it from identified threat.
- Chosen controls may be a balanced mixture that provides greatest value to as many asset-threat pairs as possible.
- Organizations looking to implement controls that don’t involve such complex, inexact, and dynamic calculations.

Documenting Results

- At minimum, each information asset-threat pair should have documented control strategy clearly identifying any remaining residual risk.
- Another option: Document the outcome of the control strategy for each information asset-vulnerability pair as an action plan.
- Risk assessment may be documented in a topic-specific report.

Summary

Risk Management: The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level

Residual Risk: risk remaining to the information asset even after the existing control is applied.

Components:

- Risk Identification
- Risk Assessment
- Risk Control
    - Strategies: Defend, Transference, Mitigate, Accept and Terminate

Cost Benefit Analysis (CBA): A formal documentation process of feasibility. The economic feasibility study determines the costs associated with protecting an asset.

Benchmarking, Baselining and Best Practices