SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M2.1 - Planning for Cybersecurity

Contents

Contents

Governance

GENERAL DEFINITION

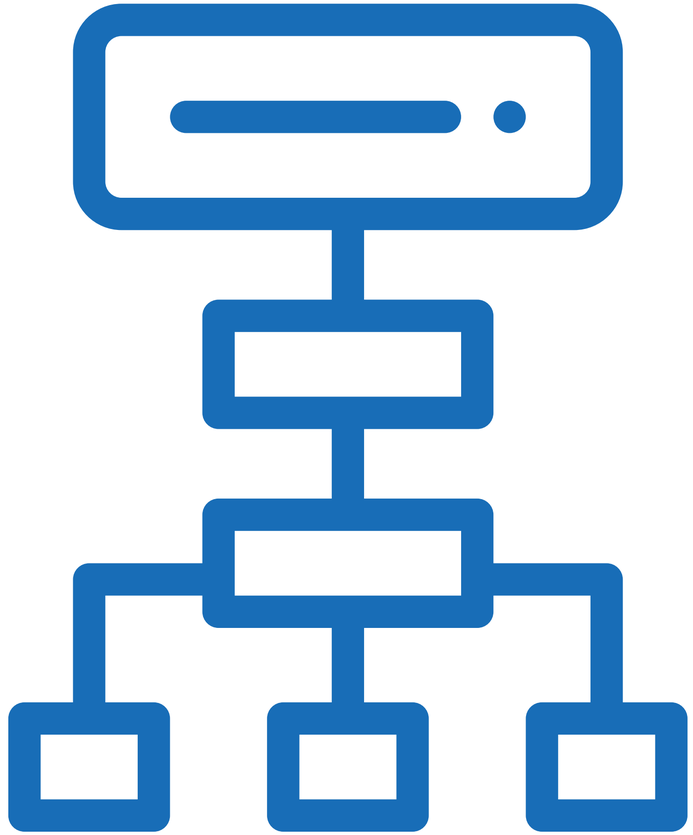
Establish of **policies** and **continuous monitoring** of their proper implementation by the members of the governing body of an organization.

Governance includes the mechanisms required to **balance the powers** of the members (with the associated accountability) and their primary duty of **enhancing** the prosperity and viability of the organization.

Information Security Governance

NIST SP 800-100, INFORMATION SECURITY HANDBOOK: A GUIDE FOR MANAGERS

Security Governance: The **process** of establishing and maintaining a framework and supporting management structure and processes to **provide assurance that information security strategies** are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and **provide assignment** of responsibility, all in an effort to manage risk.



Information Security Governance

ITU-T X.1054, GOVERNANCE OF INFORMATION SECURITY

Security Governance: the **system** by which an organization's information security-related activities are directed and controlled

Another definition

but the same meaning!

Governance vs Management (1/2)

DISTINCTION

To better understand the role of security governance, it is useful to **distinguish** between:

- information security **governance** (previously defined)
- information security **management**
- information security **implementation/operations**

Governance vs Management (2/2)

DISTINCTION

Information security management:

The **supervision** and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. **Management** of information security is expressed through the **formulation and use of information security policies, procedures and guidelines**, which are then applied throughout the organization by all individuals associated with the organization.

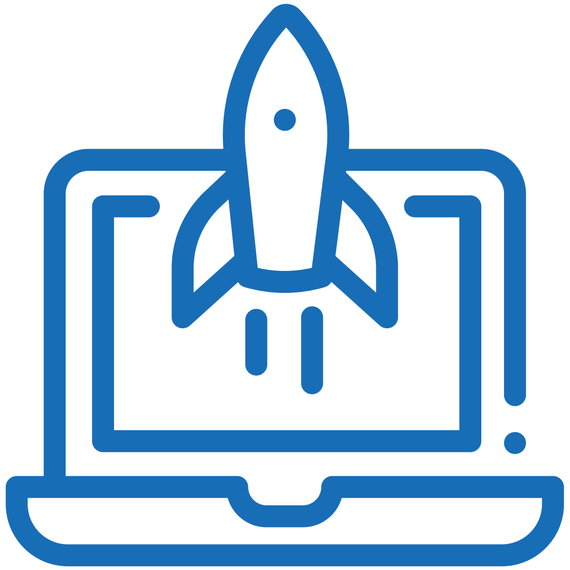
Information security implementation/operations

The implementation, deployment and ongoing operation of security controls defined within a cybersecurity framework.

Security Program

PRODUCED BY SECURITY GOVERNANCE

The **security governance** is the process that develops the **security program** that **adequately meets** the strategic needs of the business.



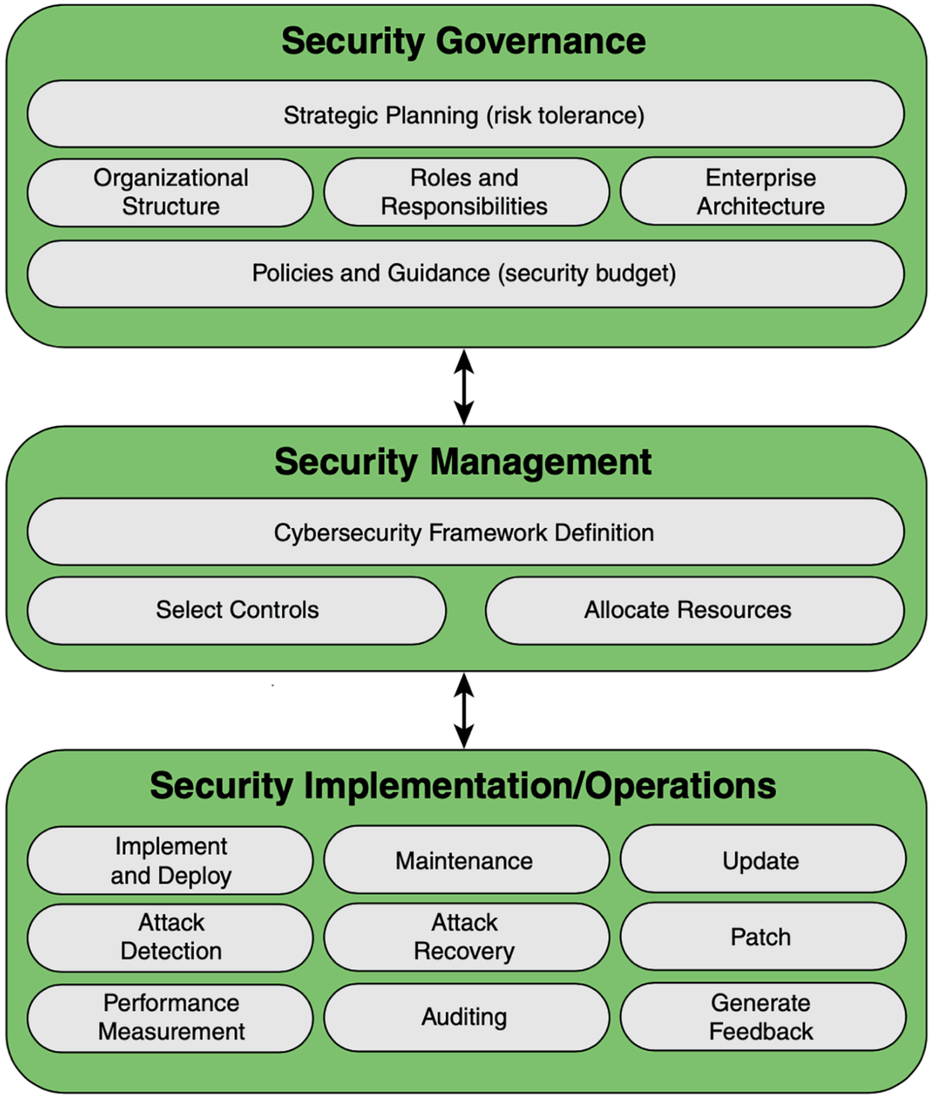
The **security program is** the management, operational, and technical aspects of protecting information and information systems.

A **security program consists of** policies, procedures, and management structure and mechanism for coordinating security activity.

Information Security Management System (ISMS)

KEY RESPONSIBILITIES AT EACH LEVEL

- The **security governance** level **communicates** the mission priorities, available resources, and overall risk tolerance to the security management level
- The **security management** level uses the information as inputs into the risk management process that **realizes** the security program and define the cybersecurity profiles.
- The **implementation/operations** level **integrates** this profile into the system development **life cycle** and continuously **monitors** security performance.



Elements affecting ISMS

EACH FACTOR PLAY A ROLE ON ISMS

Internal incident and global vulnerabilty reports

These reports **help to define** the threat and level of risk that the organization faces in protecting its information assets.

Standards and Best Practices

Standards and best practice **provide guidance** on managing risk.

User Feedback

This feedback helps **improve the effectiveness** of policies, procedures, and technical mechanisms.

Security Governance Principles (1/2)

PROVIDES USEFUL CONTEXT

ITU-T X.1054 establishes as a **key objective** of information security governance the alignment of information security objectives and strategy with overall business objectives and strategy.

X.1054 lists **six principles** for achieving this objective

Security Governance Principles (2/2)

6 PRINCIPLES

Establish organization wide information security

- **Management at all levels** should ensure that information security is integrated with information technology (IT) and other activities. **Top-level management should ensure that information security serves overall business objectives** and should establish responsibility and accountability throughout the organization

Adopt a risk-based approach

- Security governance, including allocation of resources and budgets, should be **based on the risk readiness of an organization**, considering the loss of competitive advantage, compliance and responsibility risks, operational disruptions, reputational harm, and financial loss.

Set the direction of investment decisions

- Security governance involves ensuring that information security is **integrated with existing organization processes** for capital and operational expenses, for legal and regulatory compliance, and for risk reporting

Ensure conformance with internal and external requirements

- **External requirements** include mandatory legislation and regulations, standards leading to certification, and contractual requirements.
  Internal requirements comprise broader organizational goals and objectives. **Independent security audits** are the accepted means of determining and monitoring conformance

Promote a security-positive environment for all stakeholders

- Security governance should be **responsive to stakeholder expectations**, keeping in mind that various stakeholders can have different values and needs. The governing body should take the lead in **promoting a positive information security culture**, which includes requiring and supporting security education, training, and awareness programs

Review performance in relation to business outcomes

- Governance executives should mandate **reviews of a performance measurement program for** monitoring, audit, and improvement that links information security performance to business performance

Definitions

JUST USED

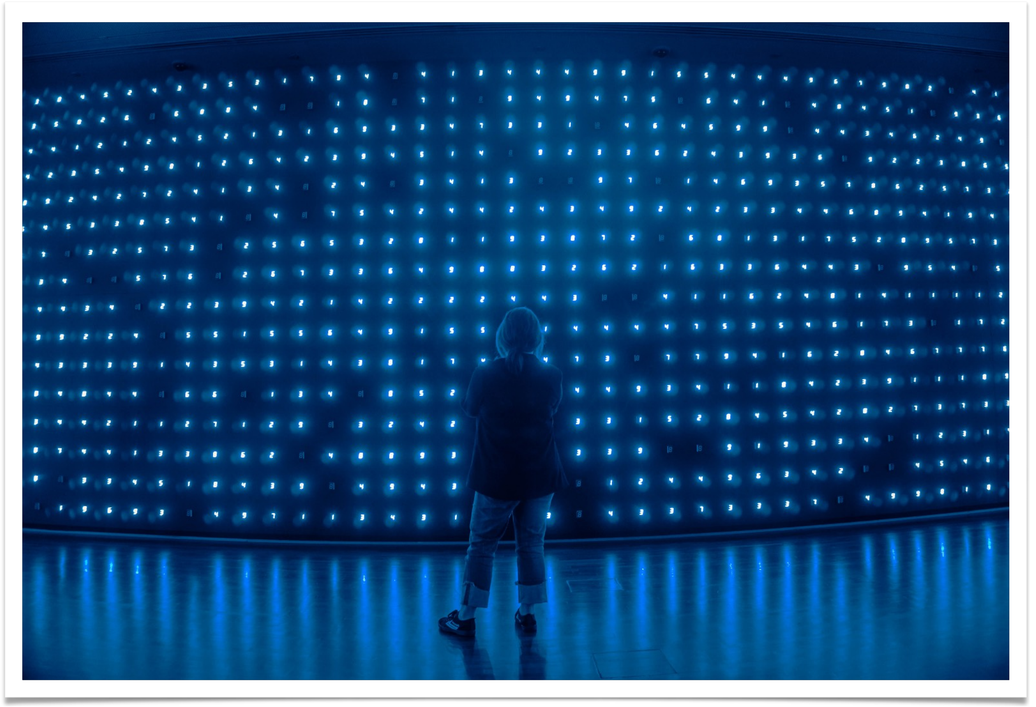
INFORMATION TECHNOLOGY (IT)

Applied computer systems, both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. IT is often the name of the part of an enterprise that deals with all things electronic.

STAKEHOLDER

A person, a group, or an organization **that has interest or concern in an organization.** Stakeholders can affect or can be affected by the organization's actions, objectives, and policies.

Some examples of stakeholders are creditors, directors, employees, government (and its agencies), owners (shareholders), suppliers, unions, and the community from which the business draws its resources



Security Governance Desired Outcomes (1/2)

LEAD TO SUCCESSFUL INTEGRATION

The IT Governance Institute defines **five basic outcomes** of information security governance that lead **to successful integration of information security with the organization's mission!**

Security Governance Desired Outcomes (2/2)

5 BASIC OUTCOMES

- **Strategic alignment**
  - The support of strategic organizational objectives requires that information **security strategy and policy be aligned with business strategy**
- **Risk management**
  - The **principal driving force for information security governance is risk management**, which involves mitigating risks and reducing or preventing potential impact on information resource
- **Resource management**
  - The resources spent on information security (e.g., personnel time and money) are somewhat open and a **key goal of information security governance is to align information security budgets with overall enterprise requirements**
- **Value delivery**
  - Not only should resources spent on information security be constrained within overall enterprise resource objectives, but also **information security investments need to be managed to achieve optimum value**
- **Performance measurement**
  - The enterprise **needs metric against which to judge information security policy** to ensure that organizational objectives are achieved

Security Governance Components

KEY ACTIVITIES

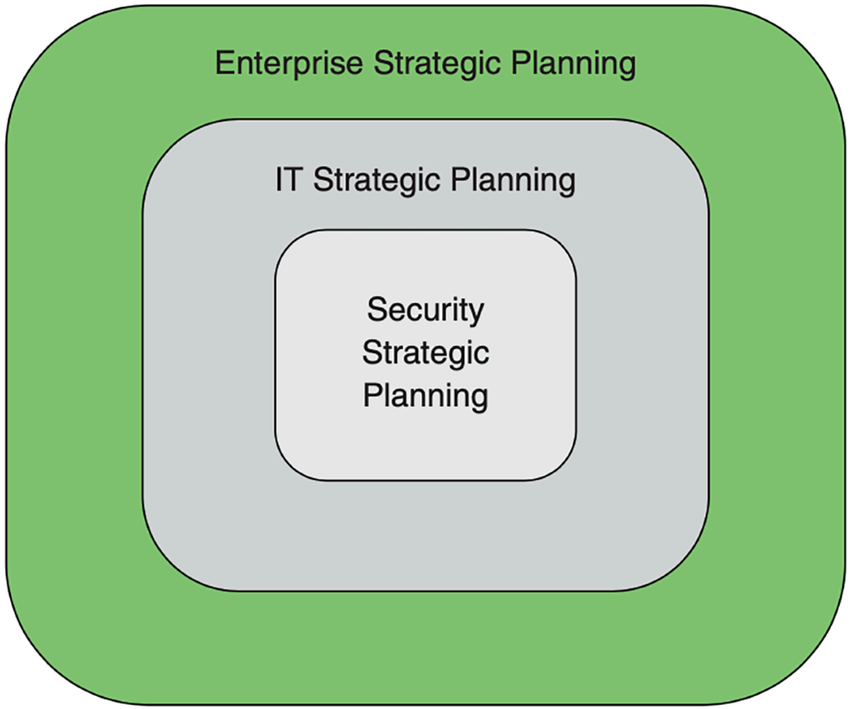
SP 800-100 lists the following key activities, or **components** that **constitute effective security governances**:

- **Strategic planning**
- **Organizational structure**
- **Establishment of roles and responsibilities**
- **Integration with the enterprise architecture**
- **Documentation of security objectives in policies and guidance**

Strategic Planning

FIRST COMPONENT

Let’s define three hierarchically related aspects of strategic planning



- **Enterprise strategic planning**
- **IT strategic planning**
- **Information security strategic planning**

Strategic plan: A document **used to communicate**, within the organization, the organization’s **goals**, the **actions** needed to achieve those goals, and all the other **critical elements** developed during planning exercises.

Enterprise Strategic Planning

FIRST

Enterprise strategic planning involves defining **long-term goals** and objectives for an organization and the development of plans to achieve these goals and objectives

It involves the development of a **strategic plan** and the ongoing oversight of the implementation of that plan.

IT Strategic Planning

SECOND

IT strategic planning is the alignment of IT management and operation with **enterprise strategic planning**.

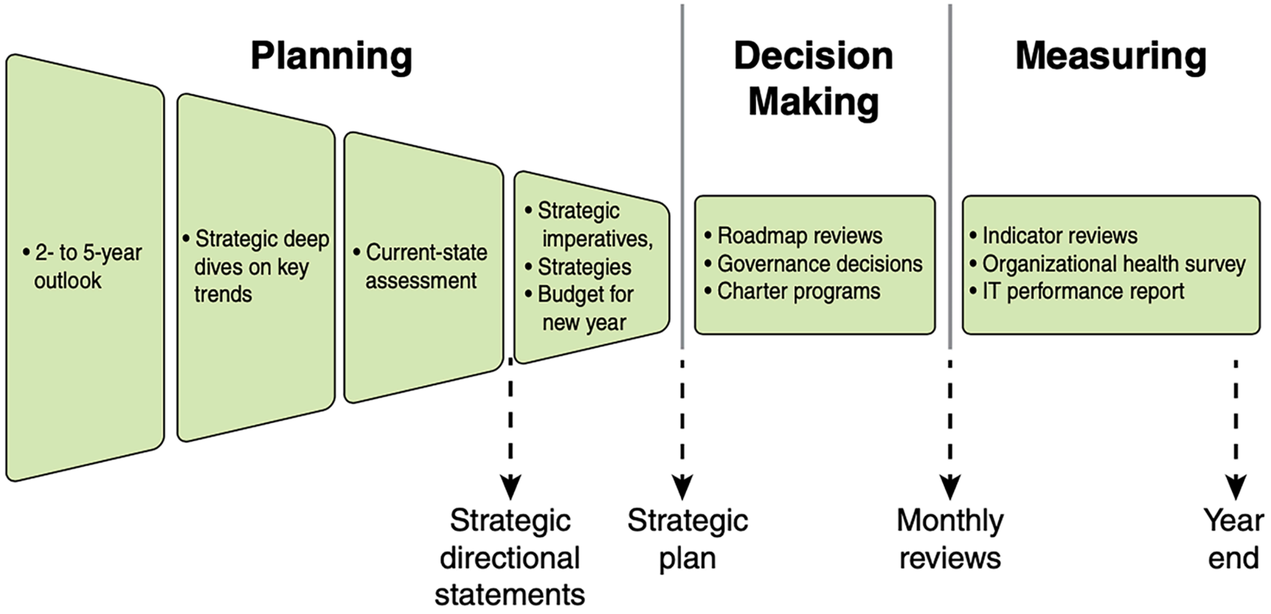
IT **infrastructure develops and changes**, meeting enterprise strategic goals is likely to involve **new arrangements** with outside providers (Cloud), **more use of mobile** devices, and reliance on a variety of new hardware and software to develop Internet of Things (IoT) capability.

These activities may create unintended barriers to flexibility and introduce new areas of risk.

IT management must be guided by strategic planning to meet these challenges.

IT Strategic Planning Process (1/6)

THIRD: INTEL'S EXAMPLE

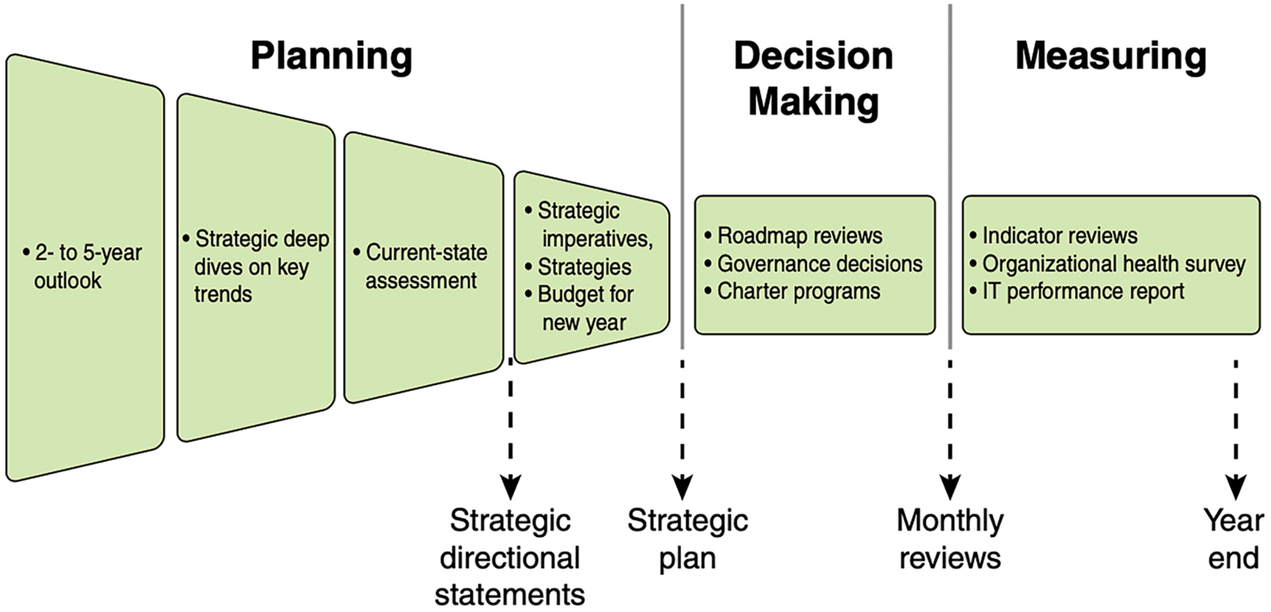


1

Two- to five-year business and technology outlook: IT subject matter experts from throughout the organization are recruited to help **define the major trends** that may be critical in shaping the organization and its decision making in the next few years.

IT Strategic Planning Process (2/6)

THIRD: INTEL'S EXAMPLE

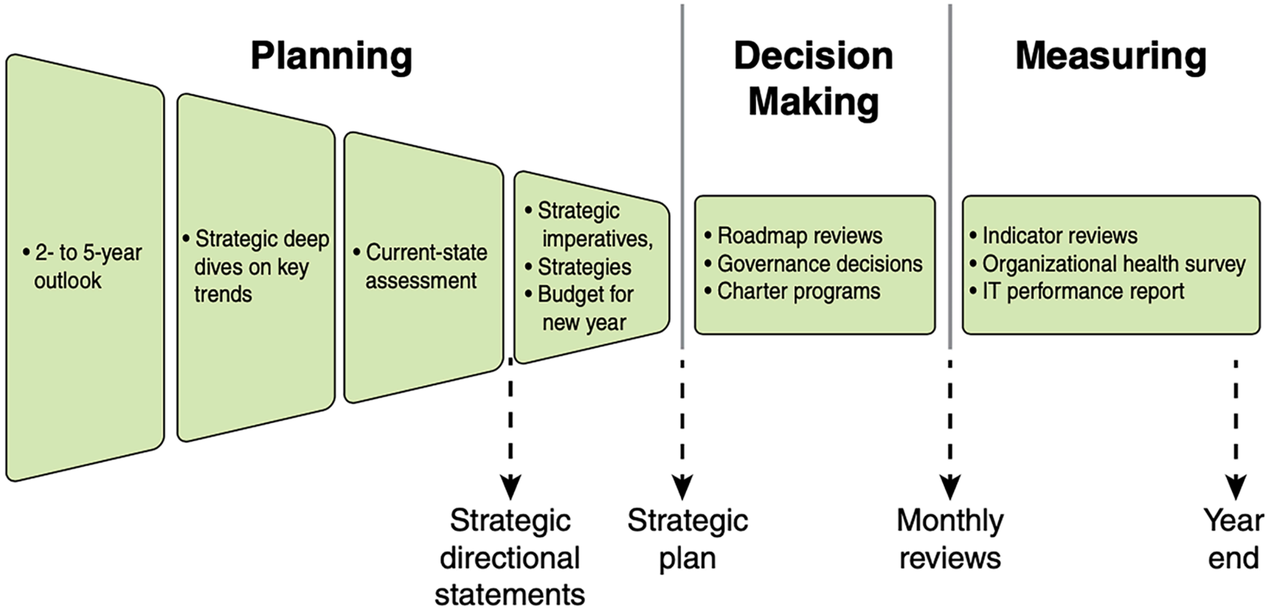


2

Strategic deep dive: The team identifies a **small number of high-impact areas** that require more in-depth analysis to inform the overall strategic planning process. Depending on circumstances at a given point in time, these may include IoT, social media trends, and changing regulatory compliance rules.

IT Strategic Planning Process (3/6)

THIRD: INTEL'S EXAMPLE

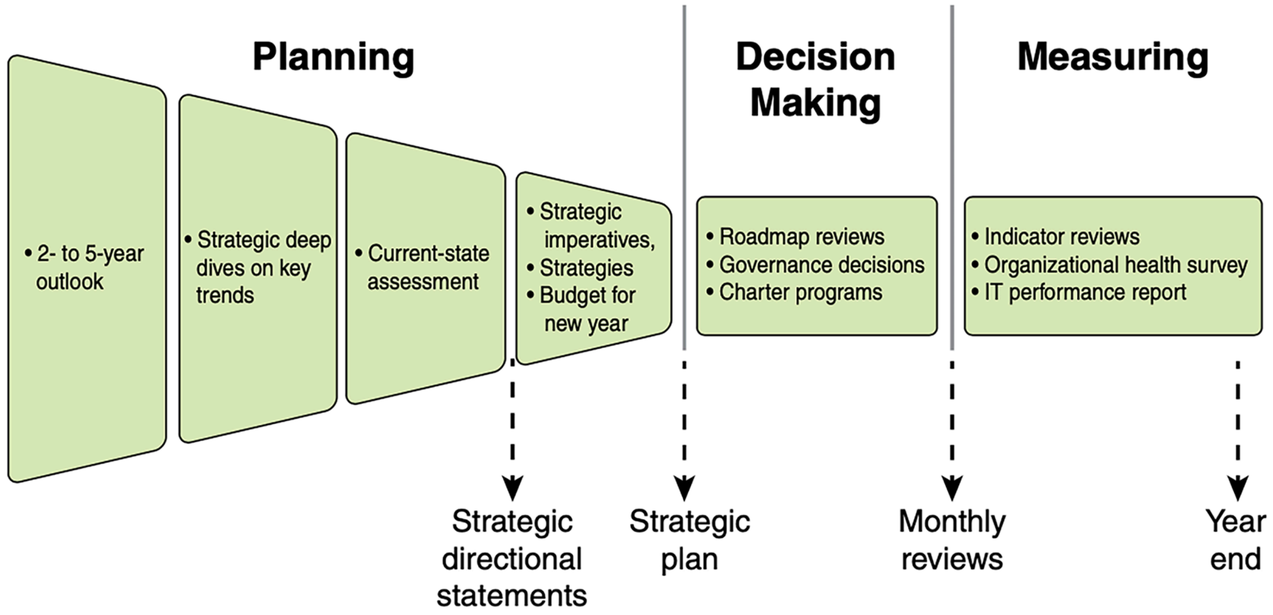


3

Current-state assessment: The planning team analyzes the **current state** of all the IT-related systems and policies and compares these with the long-range outlook, paying special attention to the **key drivers** developed in the preceding phase. The result is a **set of recommendations** for adjustments to IT's focus areas and spending plans.

IT Strategic Planning Process (4/6)

THIRD: INTEL'S EXAMPLE

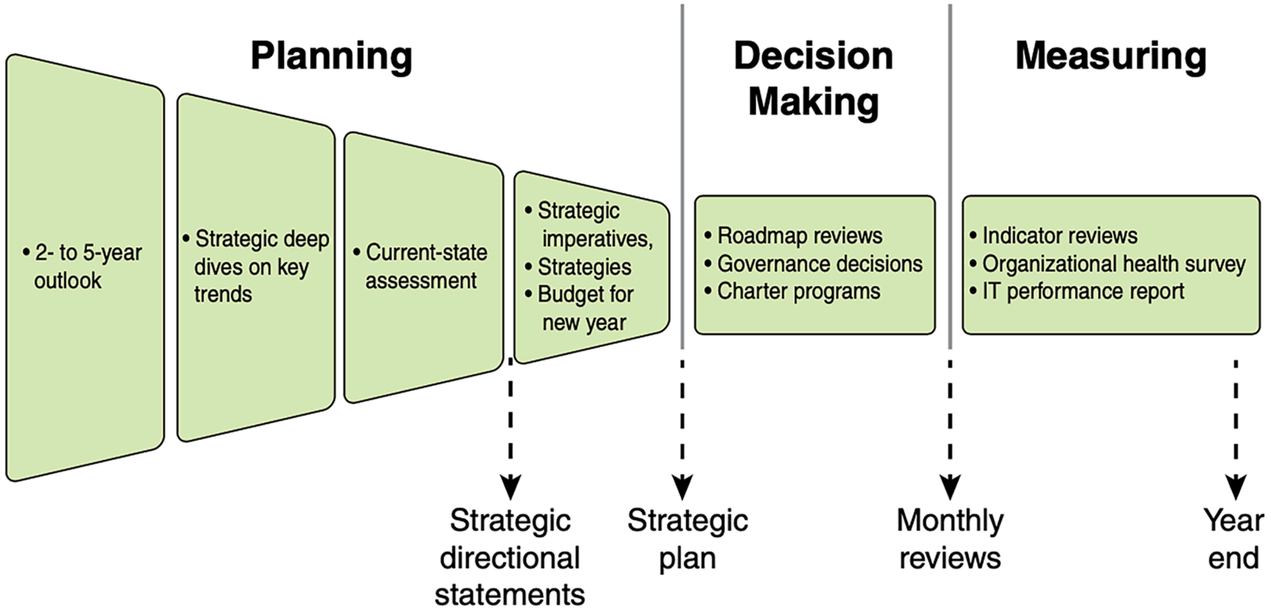


4

Imperatives, roadmaps, and finances: Development of a strategic plan for IT. The plan includes a discussion of strategic objectives and a budget and investment plan. The **plan reflects IT's highest-priority items** and provides an outcome framework for defining success. Each item includes a roadmap that can influence budget and organization decisions in the upcoming year.

IT Strategic Planning Process (5/6)

THIRD: INTEL'S EXAMPLE

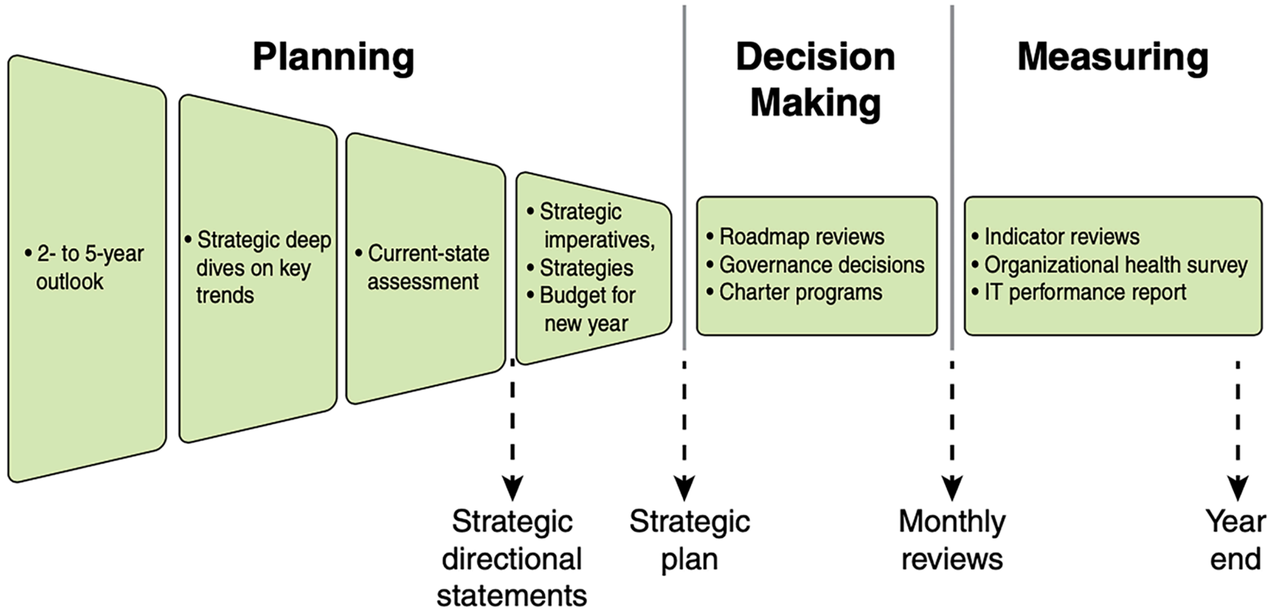


5

Governance process and decision making: Once the annual **budget is approved**, the **information from the preceding phases is used to guide the governance process** and the many decisions made across the organization to implement the strategic plan and one-year strategic objectives. These decisions include project rental, supplier selection, sourcing, investment trade-off decisions, and so on.

IT Strategic Planning Process (6/6)

THIRD: INTEL'S EXAMPLE



6

Regular reviews: Monthly reviews based on a wide variety of input help ensure that the strategic plan and governance decisions are followed. **This culminates in a year-end assessment**. Reviews continue into the following year until a new strategic plan and new governance decisions provide input for modifying the review process.

Information Security Strategic Planning

THIRD

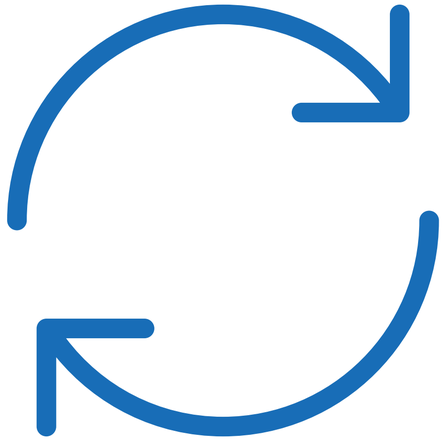
IT strategic planning may include the **information security strategic planning.**

Information security strategic planning is **alignment** of information security management and operation with **enterprise** and **IT** strategic planning.

An information security strategic plan should be embodied in a **document that is approved by the appropriate executives and committees** and is regularly reviewed.

Organizational Structure

SECOND COMPONENT



- The organizational **structure** to deal with cybersecurity **depends** on the **size** of the organization, its **type**, and the organization's **degree of dependence** on IT.

- The Information Security Governance Framework includes the **governing cycle** to direct, monitor, and evaluate the ISMS

  The evaluation incorporates both the results of the monitoring and proposals from security management to dictate changes and improvements

  This cycle is in accordance with Requirement 4.4 in **ISO 27001** that the organization shall establish, implement, maintain, and **continually improve an ISMS**.

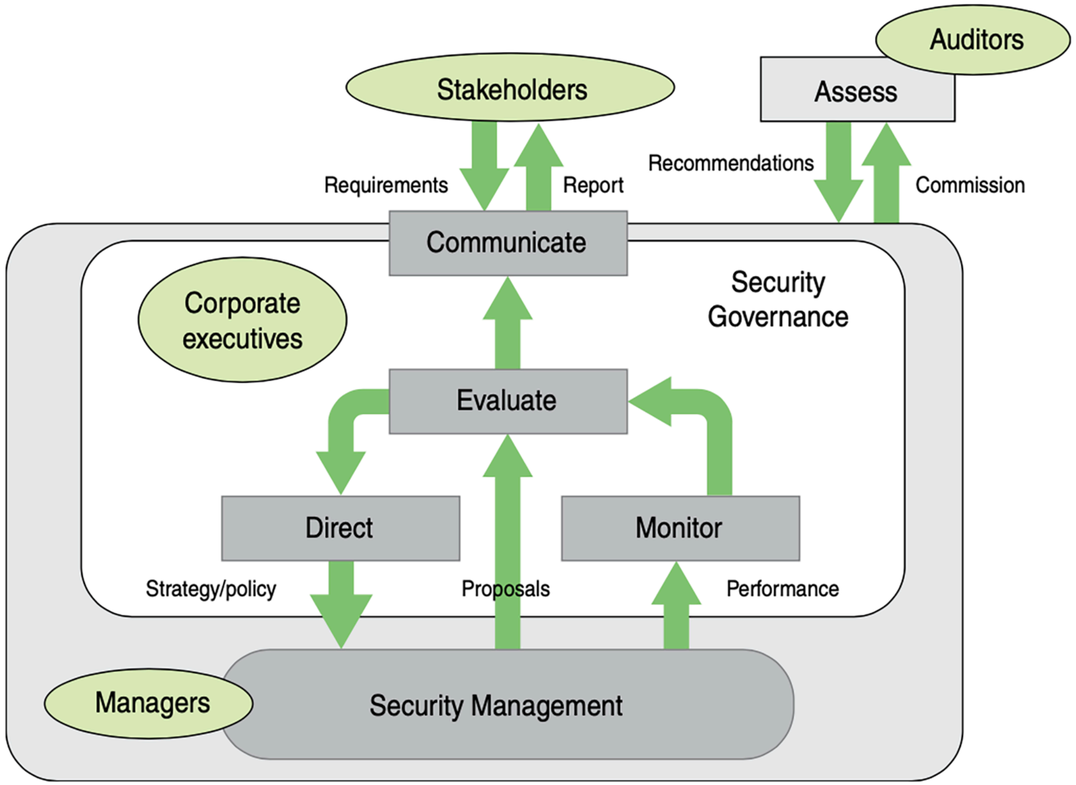
- The evaluation function triggers communication with stakeholders in the form of a **report**, which can be issued annually, more frequently, or based on a security incident.

  Reporting to stakeholders serves two purposes:

  - **Accountability**
  - **Effect on corporate value**

Organizational Structure: Cycle

SECOND COMPONENT



Direct:

Leading security management from the point of view of enterprise **strategies** and risk management. Developing a **security policy**.

Monitor:

Monitoring the **performance** of security management with measurable indicators

Evaluate:

Assessing and **verifying** the results of security performance **monitoring** in order to ensure that objectives are met and to determine future changes to the ISMS and its management.

Communicate:

Reporting enterprise security status to stakeholders and evaluating stakeholder's **requirements**

Why do we need to Report?

ACCOUNTABILITY

Reporting **enables stakeholders** to ensure that information security is **being managed effectively**, and **it should include** the following:

- Information security policy
- Risk evaluation
- Risk measures and response
- Management systems

REPORTING SHOULD DISCLOSE THE FOLLOWING

- Estimates of the **costs** and **benefits** of making an inventory of information assets
- Estimates of the **value of an inventory of information assets** that is developed as a result of information security activities
- The measure to which information security activities increase the brand value as well as the trust of the customers and partners
- The **economic value** of protected information assets
- The amount by which the security implementation **reduces the risk** of damaging the information assets

Security Status Report Structure

Report structure (example)

X.1054 provides an example of information security status report structure **that includes the following detailed contents**

- **Introduction**
  Scope (strategy, policies, standards), perimeter (geographic/organizational units), period covered (month/quarter/six months/year)
- **Overall status**
  Satisfactory/not yet satisfactory/unsatisfactory
- **Updates**
  Progess toward the security strategy, Elements completed/planned, ISMS policy revision and organisational structure to implement ISMS, progress to security certification, budgeting, other information on security activities.
- **Significant issues (if any)**
  Results of information security reviews, management action plans and target dates, Information about security incidents and their impact, compliance with security regulations.
- **Decision(s) required (if any)**
  Additional resources for security to support business initiatives

C-Level Function

ORGANIZATION

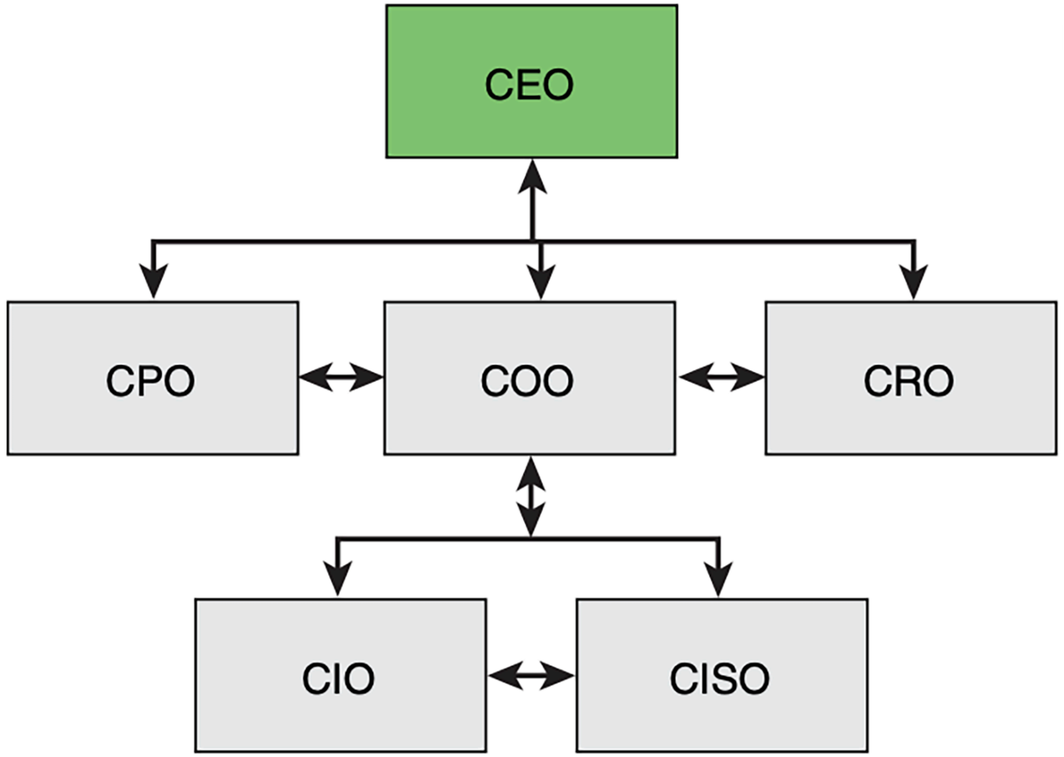
C-LEVEL

Refers to **high-ranking** executives in an organization.

Officers who hold C-level positions set the company's **strategy**, make high-stakes **decisions**, and **ensure** that the day- to-day operations align with fulfilling the company's strategic goals

Security Governance Reporting Relationship

C-LEVEL ORGANIZATION



A **key aspect** of security governance is **defining the roles and responsibilities** of executives related to information security

Executive positions that play a role in security governance include the following:

- **Chief executive officer (CEO)**: Responsible for the success or failure of the organization
- **Chief operating officer (COO)**: Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations
- **Chief information officer (CIO)**: In charge of IT strategy and the computer, network, and third-party (for example, cloud) systems required to support the enterprise's objectives and goals
- **Chief security officer (CSO)/Chief information security officer (CISO)**: Tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security and a CISO in charge of digital security
- **Chief risk officer (CRO)**: Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings
- **Chief privacy officer (CPO)**: Charged with developing and implementing policies designed to protect employee and customer data from unauthorized access

Security Governance Roles & Responsibilities (1/2)

It is important to have a structure with **clear responsibilities.**

But it's also important to have **metrics** to measure the goals we want to achieve!

- **Governance/business drivers:**

  What am I required to do? What should I do?

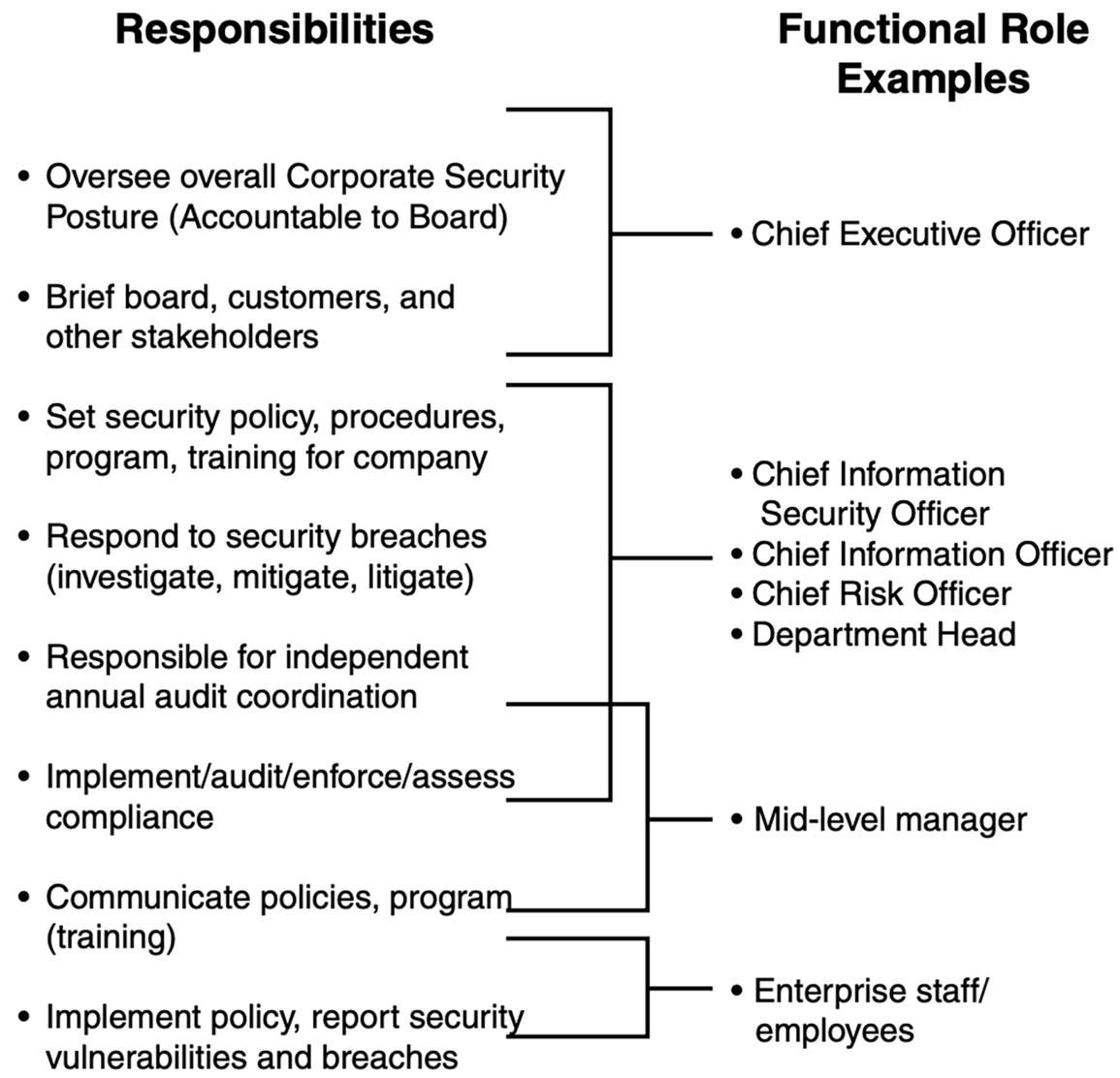
- **Roles and responsibilities:**

  How do I accomplish my objectives?

- **Metrics/audit:**

  How effectively do I achieve my objectives? What adjustments do I need to make?

Security Governance Roles & Responsibilities (2/2)



Security Governance: Policies and Guidance

NIST 800-53 A CONCRETE SUPPORT FOR THE SECURITY GOVERNANCE

NIST SP 800-53 - "Security and Privacy Controls for Federal Information Systems and Organizations"

defines an information security policy as:

*"an aggregate of directives, rules, and practices that prescribes **how** an organization manages, protects, and distributes information"*

- It is an **essential component of security governance**, providing a concrete expression of the security goals and objectives of the organization
- The policies, together with guidance documents on the implementation of the policies, **are put into practice through the appropriate selection of controls** to mitigate identified risks
- The policies and guidance need to cover information security roles and responsibilities, a **baseline** of required security controls, and **guidelines** for rules of behavior for all users of data and IT assets

Security Governance Approach

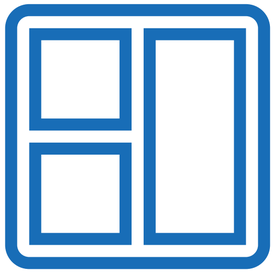
CLEAR PROCESS FOR AN EFFECTIVE SECURITY GOVERNANCE

Effective security governance requires the development of a **framework**, which is a **structured approach** for overseeing and managing risk for an enterprise.

The implementation and ongoing use of the **governance framework enables** the organization's governing body **to set clear direction** for and demonstrate their commitment **to information security and risk management**.

Security Governance Framework

AS A CONCRETE EXAMPLE OF AN APPROACH

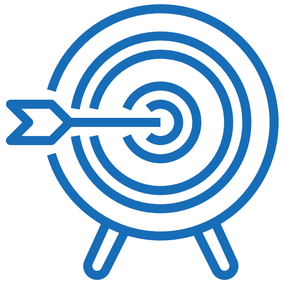


The definition, monitoring, and maintenance of a **security governance framework involves a number of tasks**:

- **Appoint** a single executive to be ultimately responsible for security governance
- **Decide** and **communicate** to top executives the objectives of the security governance framework
- **Ensure integration** of the security architecture with the enterprise architecture
- **Include a process** that enables the governing body to evaluate the operation of the information security strategy
- **Regularly** review the organization's risk willingness to ensure that it is appropriate for the current environment in which the organization operates
- **Formally** approve the information security strategy, policy, and architecture

Security Governance Direction

GOVERNING BODY SHALL INDICATE IT



A governing body is responsible for ensuring that there is effective security direction

The Standard of Good Practice for Information Security (SOGP) recommends that effective security direction be provided by a combination of **a single individual responsible for information security supported by a governing body**

- The **single individual is a CISO** or equivalent executive whose responsibilities implementing the organization's overall approach and ensuring that a security mind-set permeates the organization
- The SOGP also recommends that the **governing body include the CISO** and have a mission to support the CISO as well as review the activities that are under the CISO's direction
- Other members of the governing body could include the CIO, key department heads, and heads of business support functions such as human resources
- The **governing body assists in the coordination of security activities** and ensuring that the CISO has the resources and authority required to effect needed changes

Security Governance Evaluation

INDICATORS OF A SECURITY GOVERNANCE EFFECTIVENESS

Those who are responsible for enterprise governance and information security governance **need to be open to evaluation of their efforts at governance.**

The **metrics fall into three categories**:

- **Executive management support:** This is a critical component for cybersecurity program success. **Strong executive management** security awareness and support promotes a culture of secure practices.
- **Business and information security relationship:** An effective security governance program conveys a s**trong relationship between business goals and objectives** and information security. When information security is incorporated into the enterprise planning process, **employees tend to feel a greater responsibility for the security** of their assets and view security not as an impediment but as an enabler.
- **Information protection:** These indicators of security governance effectiveness deal with the relevance and strength of information security mechanisms. These indicators reflect the **degree of awareness** of information security issues and the **level of training to deal with attacks**.

Security Governance Best Practices (1/2)

FOR THE GOVERNANCE APPROACH

Best practices for Security Governance Approach

This area provides guidance for establishing, maintaining, and monitoring an information security governance framework, which enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management

- **Security Governance Framework**

  This topic provides a checklist of action for establishing a security governance framework and ensuring that the organization's overall approach to information security supports high standards of governance

- **Security Direction**

  This topic outlines a recommended top-down management structure and mechanism for coordinating security activity and supporting the information security governance approach. It includes discussion of a CISO, a working group, and the tasks of each

Security Governance Best Practices (2/2)

FOR THE GOVERNANCE COMPONENTS

Best practices for Security Governance Components

This area provides guidance for supporting the information security governance framework by creating an information security strategy and implementing an information security assurance program that are aligned with the organization's strategic objectives

- **Information Security Strategy**

  Provides a checklist for developing an information security strategy

- **Stakeholder Value Delivery**

  Focuses on how the organization should implement processes to measure the value delivered by information security initiatives and report the results to all stakeholders

- **Information Security Assurance**

  Discusses actions to assure that information risk is being adequately addressed

Contents

2. Risk Assessment

- Concepts
- Asset, Threat, Control, and Vulnerability Identification
- Risk Assessment Approaches
- Likelihood and Impact Assessments
- Risk Determination
- Risk Treatment

Security Risk Terminology

A GOOD WAY TO BEGIN

Risk assessment is a complex subject and **a good way to begin looking at risk assessment is to consider the terminology** listed in Table.

These terms are based largely on definitions in **ISO 27005** *"Information Security Risk Management System Implementation Guidance"*.

Nearly **identical terminology** is used in two other important documents: **NIST SP 800-30** *"Guide for Conducting Risk Assessments."*

Term	ISO 27005 Definition
asset	Anything that has value to the organization and which therefore requires protection
impact	Adverse change to the level of business objectives achieved ISO 27005 uses **consequence** SP800-30 uses **impact level** and equivalently **impact value**
event	Occurrence or change of a particular set of circumstances
threat	Potential cause of an unwanted incident, which may result in harm to a system or organization
vulnerability	Weakness of an asset or control that can be exploited by one or more threats
threat action	A realization of a threat, i.e., an occurrence in which vulnerability is exploited as the result of either an accidental event or an intentional act.
threat agent	A system entity that performs a threat action, or an event that results in a threat action.
security incident	Adverse event whereby some aspect of security could be threatened
risk	A combination of the consequences of an information security event and the associated likelihood of occurrence.
likelihood	Chance of something happening, especially likelihood of a security incident. X.1055 uses **risk of exposure (RoE)**
level of risk	Magnitude of a risk, expressed in terms of the combination of consequences and their likelihood
security control	The management, operational, and technical countermeasures prescribed to protect the confidentiality, integrity, and availability or other security property of an asset.
residual risk	Risk remaining after risk treatment
risk identification	Process of finding, recognizing and describing risks
risk analysis	Process to comprehend the nature of risk and to determine the level of risk
risk criteria	Terms of reference against which the significance of a risk is evaluated
risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
risk assessment	Overall process of risk identification, risk analysis, and risk evaluation
risk treatment	Process to modify risk SP800-30 uses **risk response**
risk management	Coordinated activities to direct and control an organization with regard to risk

Threats and Vulnerabilities

TOGETHER

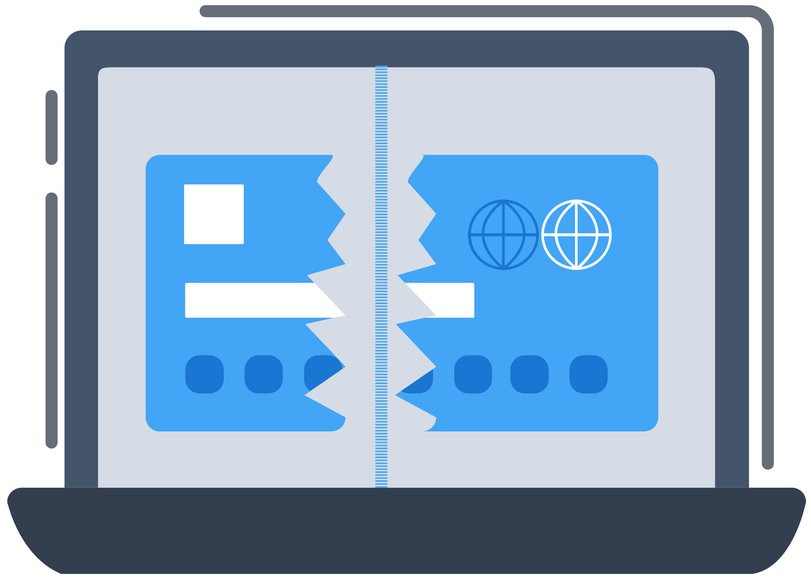
Threats and vulnerabilities need to be considered together

THREAT

An agent that intentionally or accidentally exploits a vulnerability

VULNERABILITY

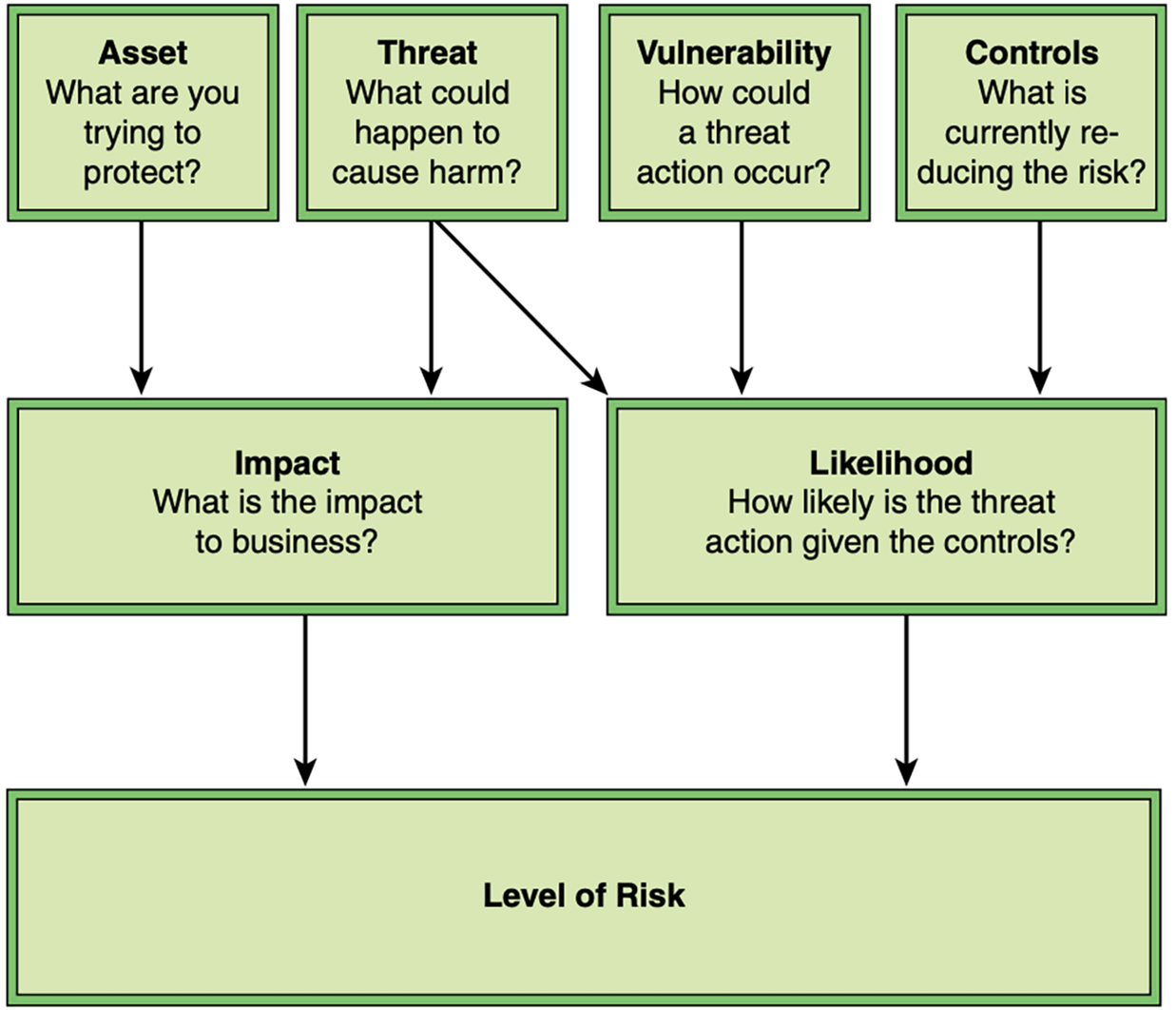
A weakness in a system's security procedures, design, implementation, or internal controls



- A **threat acting on a vulnerability** produces a security violation, or breach
- The **level of risk** is a measure that an organization can use in assessing the need for and the expected cost of taking remedial action in the form of risk treatment

Determining the Level of Risk

UNIVERSAL METHOD



Security Risk: Impact

FIRST TERM

IMPACT

Consider these **two elements** in **determining impact**:

- **Asset**

  Develop an **inventory** of the organization's assets, which includes an itemization of the **assets and an assigned value for each asset**. These include intangible assets such as reputation and goodwill, as well as tangible assets, such as databases, equipment, business plans, and personnel.

- **Threat**

  For each asset, **determine the possible threats** that could reduce the value of that asset

*Then, for each asset, **determine the impact** to the business, in terms of **cost** or **lost** value, **of a threat action occurring**.*

Security Risk: Likelihood

SECOND TERM

LIKELIHOOD

Consider the **three elements** in **determining likelihood**:

- **Threat**

  For each asset, determine **which threats are relevant** and need to be considered.

- **Vulnerability**

  For each threat to an asset, **determine the level of vulnerability** to the threat. That is, determine specifically for an asset how a threat action could be achieved.

- **Controls**

  Determine what security **controls** are currently in place **to reduce the risk**.

*Then determine **how likely** it is that a threat action **will cause harm**, based on the likelihood of a threat action and the effectiveness of the corresponding controls that are in place.*

Security Risk = Impact x Likelihood

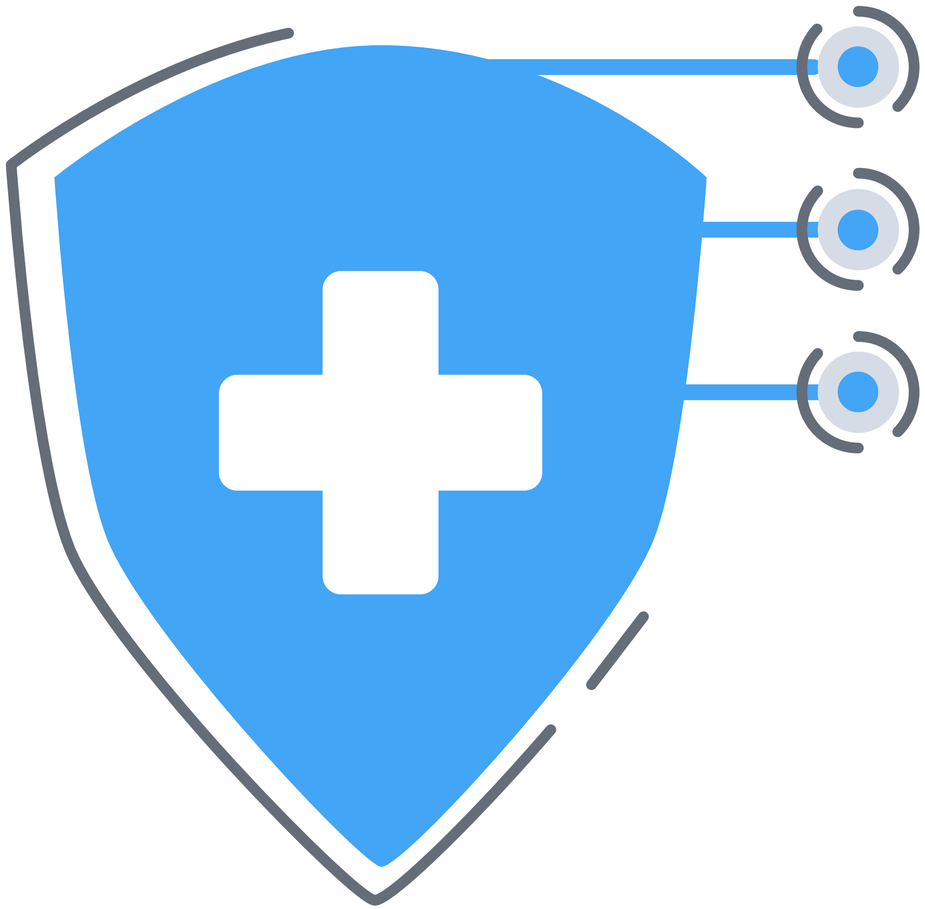
Security Risk =

Impact x Likelihood

The **level of risk** is determined as the **combination** of the cost of the threat occurring combined with the likelihood of the threat occurring

*Note that both factors, impact and likelihood, **are necessary in determining a budget allocation** for security controls. For instance, If a relatively rare security event that has very high impact costs is ignored, the organization is exposed to a very high security loss.*

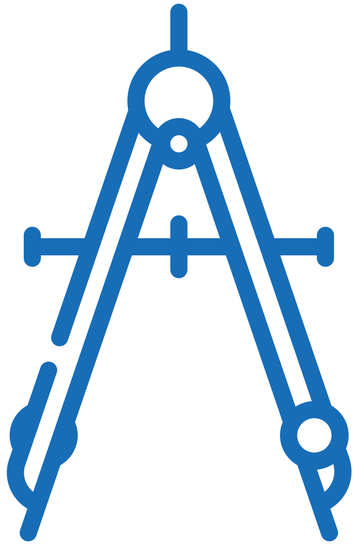
Risk Assessment Challenges



Challenges that an organization faces in determining the level of risk fall into two categories:

- **The difficulty of estimating**
- **The difficulty of predicting**

First challenge: Estimating



Consider first **the problem of estimation of each of the four elements** that contribute to determining risk:

- **Asset**: An organization needs to **put a value on individual assets** and how that value may be reduced by a specific threat—in other words, the impact value.

- **Threat**: It is **difficult to determine the entire range of threats** that are faced as well as the likelihood of any threat being realized.

- **Vulnerability**: An organization may face security **vulnerabilities that it is not aware of.**

- **Controls**: Controls are implemented to reduce vulnerability and therefore reduce the likelihood of particular threats being realized. However, **it may be very difficult to assess the effectiveness of given controls**, including software, hardware, and personnel training.

Second challenge: Predicting Future Conditions

Another challenge in risk assessment is the **difficulty of predicting future conditions**

- **Asset**: **Changes** in the value of an organization's assets **complicate the effort to estimate the impact** of a security threat. Company expansion, software or hardware upgrades, relocation, and a host of other factors may come into play

- **Threat**: It is difficult enough to assess the current threat capability and intentions of potential adversaries and future projections are even more subject to uncertainty. **Without complete knowledge of the threat**, it is impossible to provide a precise assessment of impact

- **Vulnerability**: **Changes** within the organization or its IT assets **may create unexpected vulnerabilities.** (i.e. if an organization migrates a substantial portion of its data assets to a cloud service provider, the degree of vulnerability of that provider may not be known to the organization with a high level of confidence)

- **Controls**: New technologies, software techniques, or networking protocols **may provide opportunities** for strengthening an organization's defenses. **It is difficult to predict the nature of these new opportunities**, much less their cost, and so resource allocation over the planning period may not be optimal

Risk Management

RISK ASSESSMENT IS ONE PART OF THE BROADER SECURITY TASK OF RISK MANAGEMENT

NIST Cybersecurity SP 800-37 “Risk Management Framework for Information Systems and Organizations” states that:

- **Risk management includes** a **disciplined**, structured, and flexible process for organizational **asset evaluation**; security and privacy **control** selection, implementation, and assessment; system and control authorizations; and continuous **monitoring**.

- It also includes **enterprise-level activities** to help better prepare organizations to execute a risk management framework at the system level.

Risk Management Life Cycle

AS DEFINED BY X.1055

Risk management is an iterative process.

The steps are as follows:

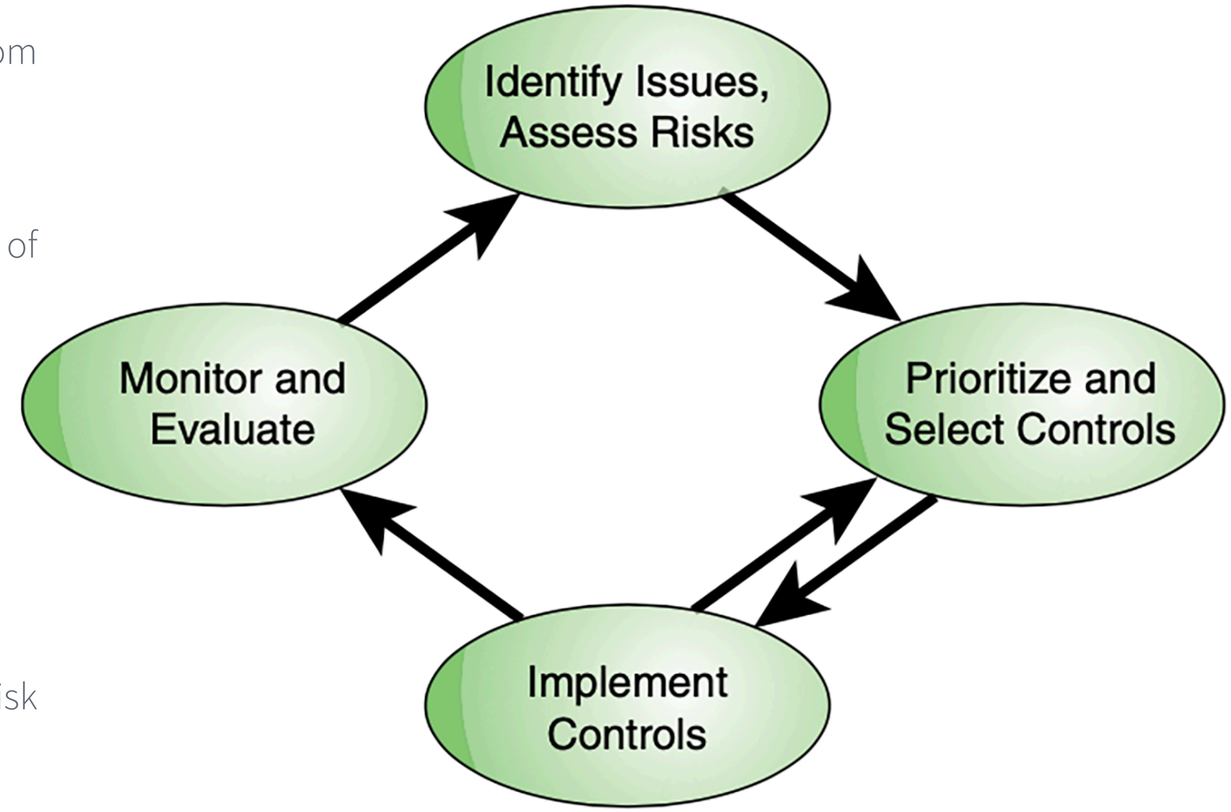
1. **Assess** risk based on assets, threats, vulnerabilities, and existing controls. From these inputs, **determine impact** and **likelihood** and then the level of risk.

2. Identify potential **security controls to reduce** risk and **prioritize** the use of these controls.

3. **Allocate** resources, roles, and responsibilities and **implement** controls.

4. **Monitor** and **evaluate** risk treatment effectiveness.

The results of the final step are **fed back into the next iteration** of the risk management life cycle.



For small organization!

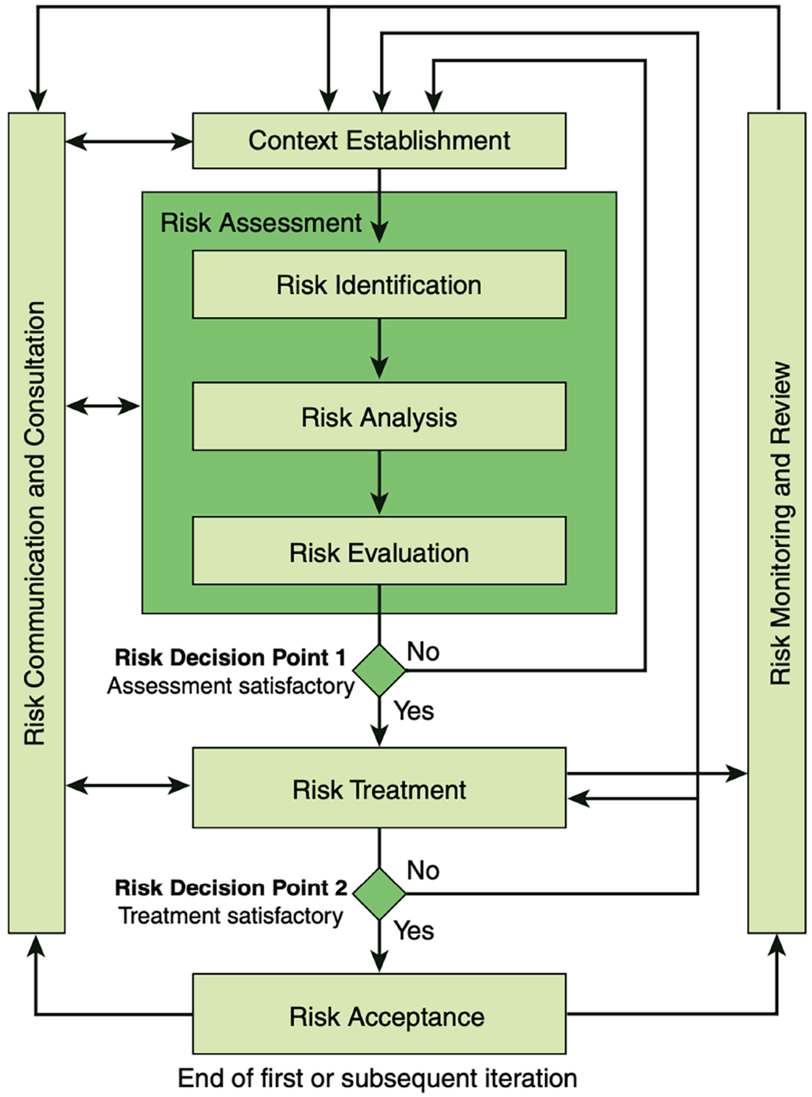
Risk Management Life Cycle

AS DEFINED BY ISO 27005

Risk management for large organization use a broader framework (ISO 27005) and the process consist of separate activities.

1. **Context establishment**
2. **Risk assessment (ISO 27001)**
   i. **Risk identification**
   ii. **Risk analysis**
   iii. **Risk evaluation**
3. **Risk Treatment**
4. **Risk Acceptance**
5. **Risk communication and consultation**
6. **Risk monitoring and review**

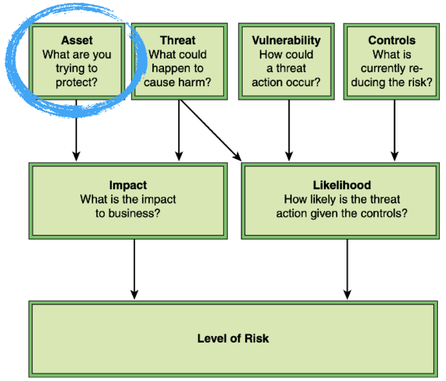
The risk management process is an **iterative** process. There are **continual changes in business** asset valuation, threat capability and frequency, vulnerability magnitude, and control technologies and techniques. Thus, the assessment and treatment of risk must be an ongoing activity.



For large organization!

Asset Identification

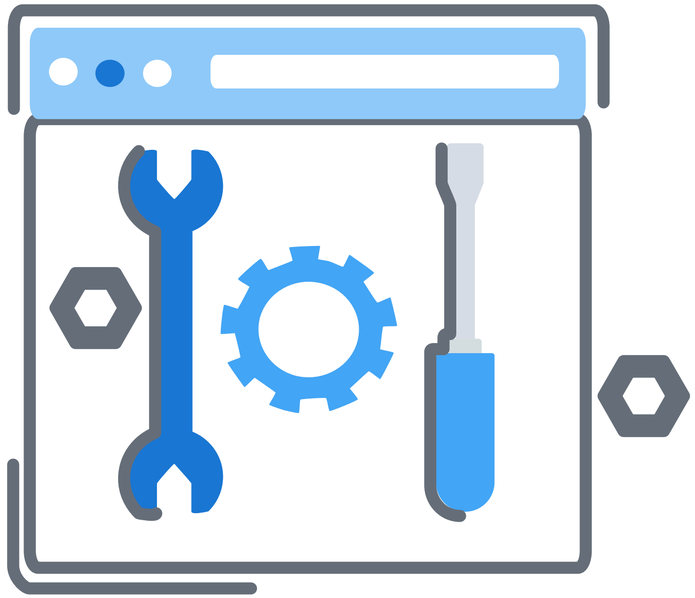
THIS LIST SERVES AS AN INPUT TO RISK ANALYSIS



An asset can be many things!

- A first step in risk assessment is to document and **determine values** for the organization's assets
- An asset **is anything of value to the business** that requires protection, including hardware, software, information, and business assets
- The **challenge** is to develop a **uniform way of documenting the assets**, the security implications of each, and the costs associated with security incidents related to each
- Asset evaluation relates directly to business needs
- The input for asset evaluation **needs to be provided by owners and custodians of assets**, not by members of the risk assessment team

What is Asset ? Hardware Asset

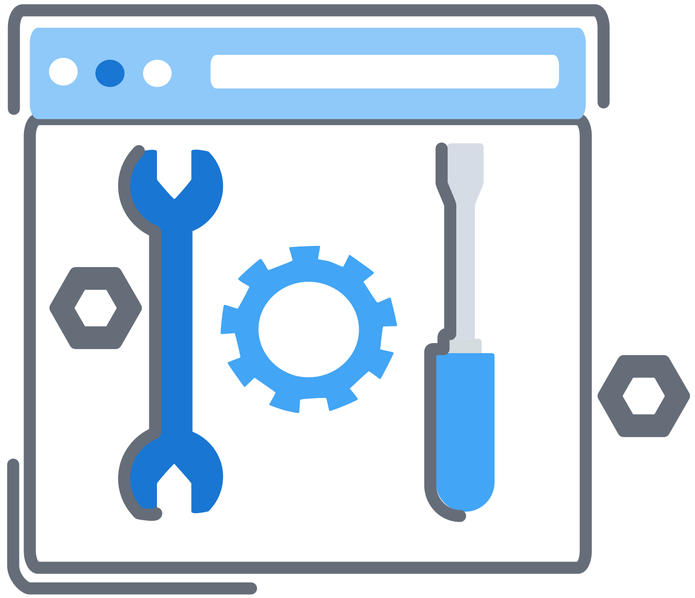


Hardware assets include **servers**, workstations, laptops, mobile devices, removable media, networking and **telecommunications equipment**, and peripheral equipment.

Key **concerns** are **loss of a device**, through theft or damage, and lack of availability of the device for an extended period.

Another concern is **device malfunction**, due to deliberate malfunction or other causes.

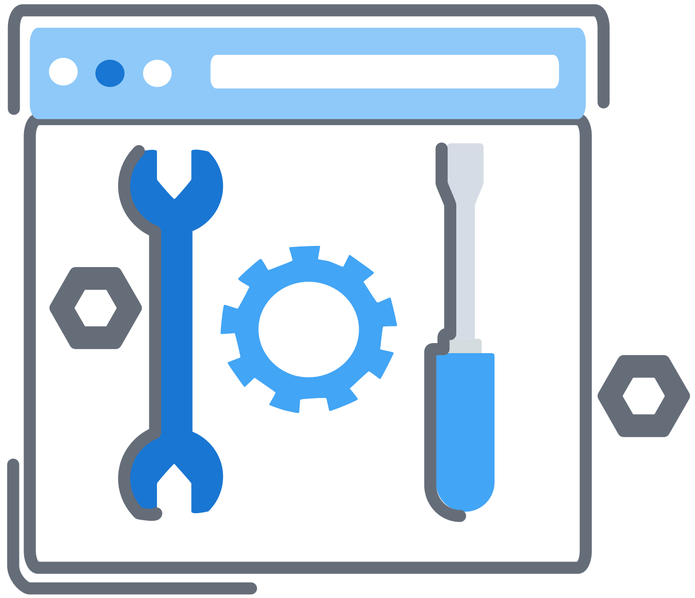
What is Asset ? Software Asset



Software assets include **applications**, **operating systems** and other system software, virtual machine and container virtualization software, software for software-defined networking (SDN), database management systems, file systems, and client and server software.

Availability is a key consideration here, and asset evaluation must take account of **disruption losses** and **recovery expenses**.

What is Asset ? Information Asset



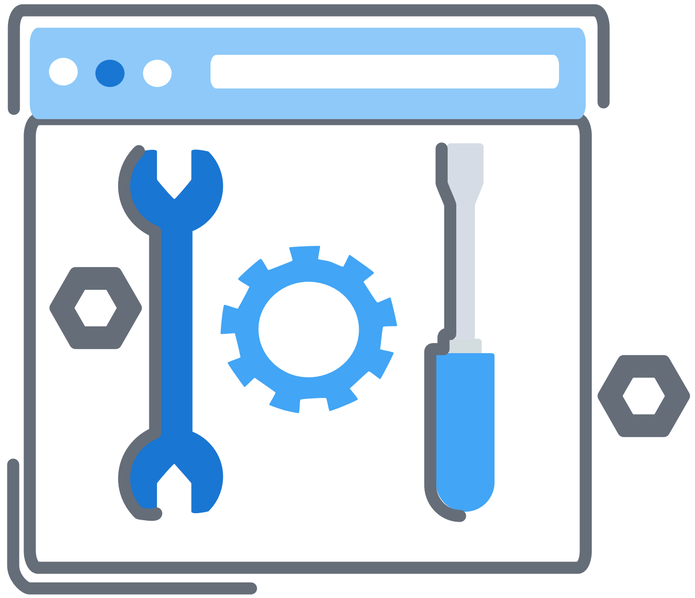
Information assets **comprise the information stored** in databases and file systems, both on-premises and remotely in the cloud.

Types of information data are: Communication data, Routing information, Traffic statistical information, Customer information, Training materials, etc.

Asset valuation needs to take into account **the impact of threats to confidentiality, privacy, integrity, and authenticity**.

- What would happen to my business if this information **were made public**?
- What would happen to my business **if this information were incorrect**?
- What would happen to my business if my customers or I **couldn't access this information**?

What is Asset ? Business Asset



The business assets category includes organization **assets that don’t fit into the other categories**, including human resources, business processes, and physical plant.

This category also includes **intangible assets, such as organization** control, **know-how**, **reputation**, and image of the organization.

Asset Register

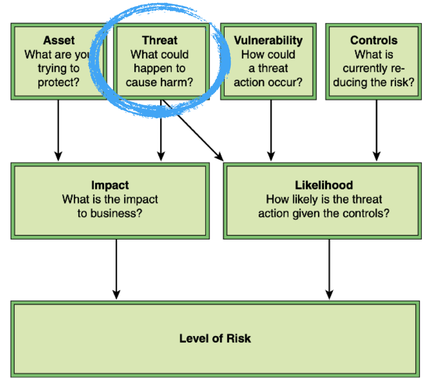
IN ORDER TO EFFECTIVELY PROTECT ASSETS

Asset Name/ Description	Asset Classification	Disaster Recovery Priority	Description	Exposure Level
Personnel	High	1	Employees	Medium
Client PII	High	1	Personally Identifiable Information	Low
Production Web server	Medium	1	Company primary web site (no sensitive data)	High

- In order to effectively protect assets, an **organization needs to provide a systematic method of documenting assets** and their security implications
- This is done in an **asset register that documents important security-related** information for each asset
- **Examples of items that may be included** for each asset are as follows:
  - Asset name/description
  - Asset type
  - Information risk assessment
  - Information assets
  - Data type/classification
  - Asset value classification
  - Disaster recovery priority
  - Asset owner

Threat Identification

PROCESS OF IDENTIFYING THREAT SOURCES



Threat identification is the process of **identifying sources with the potential to harm system assets**

Threat sources are categorized into three areas:

- **Environmental**
  - Examples include floods, **earthquakes**, tornadoes, landslides, avalanches, electrical storms, and power failure
- **Business resources**
  - Examples include **equipment failure**, supply chain disruption, and unintentional harm caused by employees
- **Hostile actors**
  - Examples include hackers, **hacktivists**, insider threats, criminals, and nation-state actors

Threat Types

CHALLENGING PROCESS

Many efforts have been made to categorize types of threats, and there is considerable **overlap in the definition** of some common terms. A **large category** of threat is malicious software, or **malware**, which is a general term encompassing many types of software threats, including the following

- Malware
- Virus
- Worm
- Ransomware
- Spam
- Logic bomb
- Trojan horse
- Backdoor (trapdoor)
- Mobile code
- Exploit
- Exploit kit
- Downloader
- Dropper
- Auto-rooter
- Kit (virus generator)
- Spammer program
- Flooder
- Keyloggers
- Rootkit
- Zombie or bot
- Spyware
- Adware
- Remote access attacks
- Denial-of-service (DoS)
- Distributed denial-of-service (DDoS) attack
- DNS attacks
- Hacker or cracker
- Injection flaw
- Code injection
- Social engineering
- Phishing
- Password attack
- Website exploit

These lists are not exhaustive **but give you an idea of the scale of the challenge organizations face**.

Source of Information (1/2)

DIFFICULT

Information about Threats!

It is difficult to get reliable information on past events and **to assess future trends** for a variety of reasons, including:

- Organizations are often **reluctant to report security events in an effort to save corporate image**, avoid liability costs, and, in the case of responsible management and security personnel, avoid career damage
- Some attacks may be carried out or at least attempted **without being detected by the victim until much later**, if ever
- **Threats continue to evolve** as adversaries adapt to new security controls and discover new techniques

Thus, **keeping informed on threats is an ongoing and never-ending battle**

Source of Information (2/2)

DIFFICULT

Information about Threats!

Three important categories of threat information sources are:

- **In-house experience**

  An important source of information on threats is the **experience an organization has already had on identifying** attempted and successful attacks on its assets

- **Security alert services**

  These are concerned **with detecting threats as they develop** to enable organizations to patch code, change practices, or otherwise react to prevent a threat from being realized

- **Global threat surveys**

  Of great value for threat identification is the various **global threat surveys** that are readily available

Global Threat Survey

THE MOST IMPORTANT

Verizon Data Breach Investigations Report [2021]

One of the most important source of information

Threats are broken in

3 dimensions: Patter, Action, Asset.

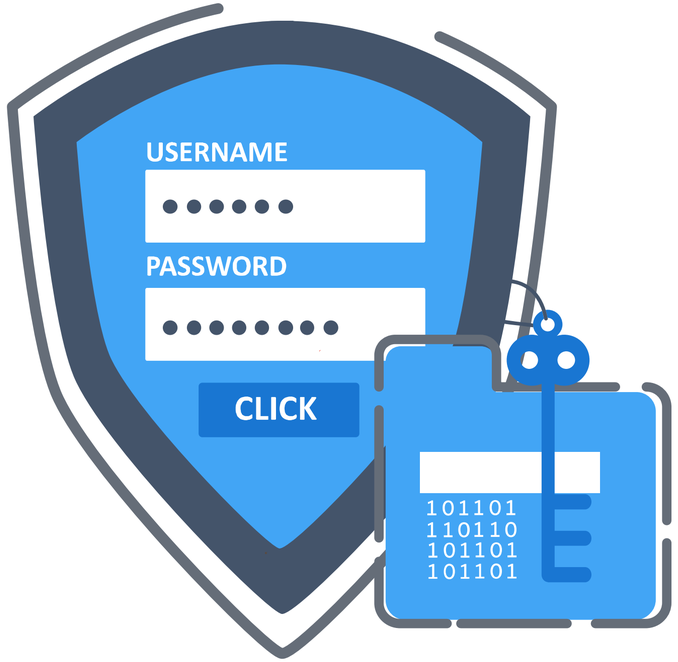
Key aspects of attacks: Actors, Tactics, common factors.

ENISA Threat Landscape Report [2021]

Very useful and based on ENISA Threat Taxonomy

For each threat the report provides the **kill chain**.

The phase of a kill chain: Reconnaissance, Weaponization, Delivery, Exploit, Installation,Command and control.



Trustwave Global Security Report [2020]

Report based on finding on extensive data sources

Trustwave operates a number of security operations centers (SOCs) as a managed security service

Fortinet Threat Landscape Report [2021]

Report based on Fortinet's vast array of devices

Three measures are reported: Volume, Prevalence, Intensity.

Cisco Cybersecurity Reports

Excellent resources

Report are often based on the **kill chain concepts**.

Global Threat Survey: example

ENISA THREAT LANDSCAPE REPORT

Table 3.5 Top Cybersecurity Threats Reported by ENISA

Threat	Trend	Threat	Trend
1. Malware	→	9. Insider threat (malicious, accidental)	→
2. Web based attacks	↑	10. Physical manipulation/damage/ theft/loss	→
3. Web application attacks	↑	11. Data breaches	↑
4. Phishing	↑	12. Identity theft	↑
5. Spam	↑	13. Information leakage	↑
6. Denial of service	↑	14. Exploit kits	↓
7. Ransomware	↑	15. Cyber espionage	↑
8. Botnets	↑		

Trend: ↓ Declining, → Stable, ↑ Increasing

The 15 threats are ranked according to the **volume of security incidents surveyed**, and the Trend column refers to the relative change in the severity of consequences from each threat.

For each threat, **the report provides a kill chain for each specific threat**, which defines the phases of a cyber attack.

Kill Chain

A systematic process used to target and engage an adversary to create desired effects.

In the context of cybersecurity, it consists of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action.

WHY ?
The kill chain is useful for selecting security controls to counter a particular threat.

Security Operation Center (SOC)

USEFUL DEFINITION

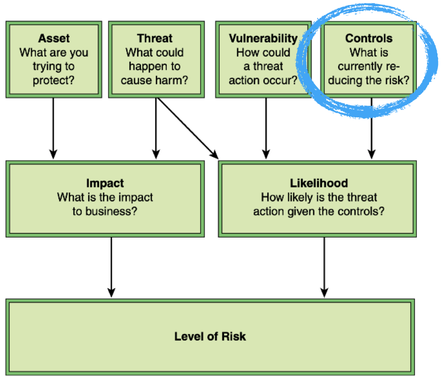
SOC

A facility that tracks and integrates multiple security inputs, **checks** risk, **determines** the targets of an attack, **contains** the impact of an attack, and **recommends** and/or **executes** responses appropriate to any given attack.

In some cases, an organization **establishes a SOC** for **itself**. In other cases, SOC services are **outsourced** to a private company that specializes in providing such services

Control Identification

CONTROLS FOR CYBERSECURITY



- **Controls for cybersecurity include any process**, policy, procedure, guideline, practice, or organizational structure that **modifies information security risk**
- **Controls are** administrative, technical, management, or legal in nature

- **Control identification is defined in ISO 27005** as the process of identifying existing and planned security controls, and suggests the following steps:

  (1) Review documents containing information about the controls

  (2) Check with the people with responsibility related to information security and the users about which controls **are really implemented** for the information process or information system under consideration

  (3) Conduct an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented to determine **whether they are working correctly and effectively**

  (4) Review results of audits

Controls NIST SP 800-53

SEVERAL DETAILS ABOUT CONTROLS

NIST SP 800-53 *"Recommended Security Controls for Federal Information Systems and Organizations"* provides an invaluable and extraordinarily detailed discussion of controls and **should be consulted in the development of any risk treatment plan**

The controls are organized into the following **families**:

- **AC**: Access Control
- **AU**: Audit and Accountability
- **AT**: Awareness and Training
- **CM**: Configuration Management
- **CP**: Contingency Planning
- **IA**: Identification and Authentication
- **IR**: Incident Response
- **MA**: Maintenance
- **MP**: Media Protection
- **PS**: Personnel Security
- **PE**: Physical and Environmental Protection
- **PL**: Planning
- **PM**: Program Management
- **RA**: Risk Assessment
- **CA**: Security Assessment and Authorization
- **SC**: System and Communications Protection
- **SI**: System and Information Integrity
- **SA**: System and Services Acquisition

For each control, **the catalog provides a description of the control, supplemental guidance on implementation, a description of control enhancements**, and references to other documents.

Group controls by aligning them with FAIR

GROUP CONTROLS FOR THE RISK ASSESSMENT PROCESS

For purposes of risk assessment, it is useful to **group security controls** in a manner that **reflects the risk assessment process**.

The **FAIR (Factor Analysis of Information Risk)** risk analysis document, **groups controls into four categories**.

(1) Avoidance control: These controls affect the frequency and/or likelihood of **encountering threats**

- Firewall filters, physical barriers, the relocation of assets, the reduction of threat populations

(2) Deterrent controls: These controls **affect the likelihood of a threat acting** in a manner that results in harm

- Policies, logging and monitoring, enforcement practices, asset hardening, physical obstacles

(3) Vulnerability controls: These controls affect the probability that a **threat's action will result in loss**

- Authentication, access privileges, patching, configuration settings

(4) Responsive controls: These controls affect **the amount of loss** that result from a threat's action

- Backup and restore media and processes, forensics capabilities, incident response processes, credit monitoring for persons whose private information has been compromised

FAIR is a risk assessment approach that we discuss later on...

Useful checklist of controls for small business

NIST INTERAGENCY REPORT (NISTIR) 7621

This NIST Interagency Report (NISTIR) **provides guidance on how small businesses** can provide basic security for their information, systems, and networks.

NISTIR 7621 provides the following **useful checklist of controls**:

Identity

- Identify and control who has access to your business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for information security

Detect

- Install and update antivirus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs
- Respond
- Develop a plan for disasters and information security incidents (for example, incident response plan)

Protect

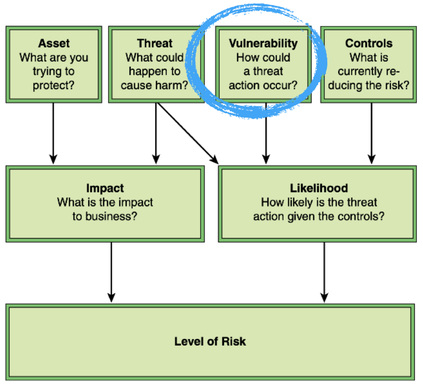
- Limit employee access to data and information
- Install surge protectors and uninterruptible power supplies (UPSs)
- Patch your operating systems and applications
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

Recover

- Make full backups of important business data/information
- Make incremental backups of important business data/information
- Consider cyber insurance
- Make improvements to processes/procedure /technologies

Vulnerability Identification

PROCESS



Vulnerability identification is **the process of identifying vulnerabilities** that can be exploited by threats to cause harm to assets

A vulnerability **is a weakness or a flaw** in a system's security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited when a threat is manifested

Vulnerability Categories

PROCESS

Technical vulnerabilities

Flaws in the **design**, **implementation**, and/or configuration of software and/or hardware components, including application software, system software, **communications** software, computing equipment, communications equipment, and embedded devices.

Human-caused vulnerabilities

Key person dependencies, gaps in **awareness** and training, gaps in discipline, and improper termination of access.

Physical and environmental vulnerabilities

Insufficient physical access controls, poor siting of equipment, inadequate **temperature**/humidity controls, and inadequately conditioned electrical power.

Operational vulnerabilities

Lack of change management, **inadequate separation of duties,** lack of control over software installation, lack of control over media handling and storage, **lack of control over system communications**, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, **inadequate control over encryption keys**, inadequate reporting, handling and/or resolution of security incidents, and inadequate monitoring and evaluation of the effectiveness of security controls.

Business continuity and compliance vulnerabilities

Misplaced, missing, or **inadequate processes for appropriate management of business risks**; inadequate business continuity/contingency planning; and inadequate monitoring and evaluation for compliance with governing policies and regulations.

In many of the areas listed here, vulnerability identification depends critically on management initiative!

Vulnerability, can we be more specific?

CVE - CVSS - NVD

In the area of technical vulnerabilities, it is possible to be more precise and exhaustive!

National Vulnerability Database (NVD) https://nvd.nist.gov/

The NVD is a comprehensive **list** (maintained by NIST) of known technical vulnerabilities in systems, hardware, and software.

Common Vulnerability Scoring System (CVSS) https://www.first.org/cvss/

CVSS indicates the **severity** of an information security vulnerability, and is an integral component of many vulnerability scanning tools.

Common Vulnerabilities and Exposures (CVE) https://cve.mitre.org/cve/search_cve_list.html

CVE is a **list** of publicly disclosed vulnerabilities and exposures that is maintained by MITRE

Differences: CVE vs CVSS vs NVD

CVE - CVSS - NVD

CVSS vs CVE

CVSS is the **overall score assigned** to a vulnerability.

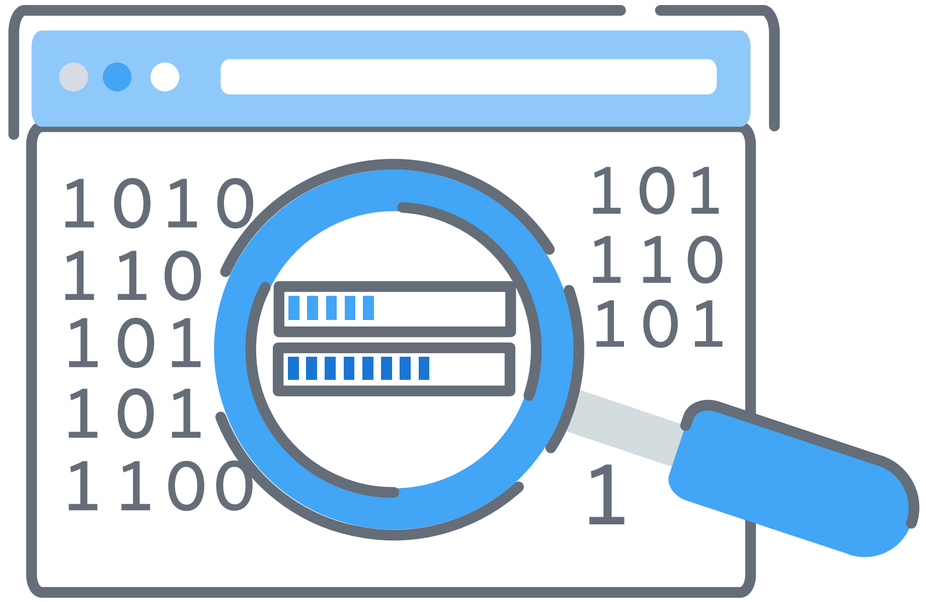
CVE is simply a list of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments. The CVSS score is not reported in the CVE listing – you must use the NVD to find assigned CVSS scores.

CVE vs NVD

The CVE list feeds into the NVD, so both are synchronized at all times.

The **NVD provides enhanced information** above and beyond what's in the CVE list, **including patch availability and severity scores**.

NVD also provides an easier mechanism to search on a wide range of variables. Both CVE and NVD are sponsored by the US Federal Government and are available for free use by anyone.



Example of Vulnerability Scoring in NVD

NVD (NIST)

Current Description
An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.
Source: MITRE **Last Modified:** 02/01/2017 View Analysis Description

CVSS Severity (version 3.0):
CVSS v3 Base Score: 8.8 High
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 2.8

CVSS Version 3 Metrics:
Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

i Quick Info
CVE Dictionary Entry: CVE-2017-3823
Original release date: 02/01/2017
Last revised: 04/04/2017
Source: US-CERT/NIST

In essence, the scoring is done as follows: for each identified vulnerability, the **NVD provides a level for each metric** in the base group, based on the characteristics of the vulnerability.

Example of Vulnerability CVSS metrics

CVSS (FIRST.ORG)

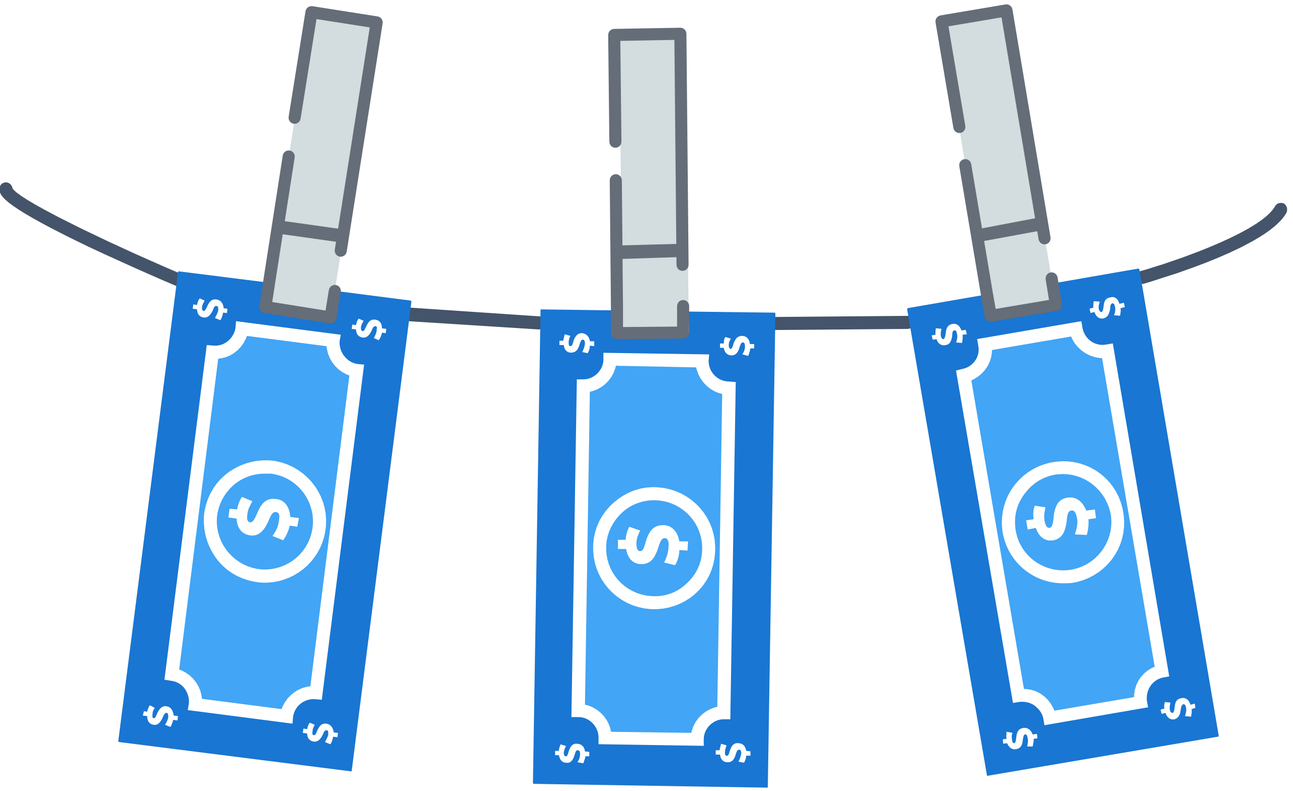
Base Metric Group		Temporal Metric Group	Environmental Metric Group
Exploitability	**Impact**		
Attack Vector •Network •Adjacent •Local •Physical **Attack Complexity** •Low •High **Privileges Required** •None •Low •High **User Interaction** •None •Required	**Confidentiality Impact** •High •Low •None **Integrity Impact** •High •Low •None **Availability Impact** •High •Low •None	**Exploit Code Maturity** •Not Defined •High •Functional •Proof-of-Concept •Unproven **Remediation Level** •Not Defined •Workaround •Temporary Fix •Official Fix **Report Confidence** •Not Defined •Confirmed •Reasonable •Unknown	**Confidentiality Requirement** •Not Defined •High •Medium •Low **Integrity Requirement** •Not Defined •High •Medium •Low **Availability Requirement** •Not Defined •High •Medium •Low
Scope •Unchanged •Changed			

Each level of a metric has a descriptive name. In addition, **the CVSS assigns a numeric value on a scale of 0.0 to 10.0**, with 10.0 being the most severe security issue.

The numeric scores for the metrics in the base metric group are put into an **equation** defined in the CVSS that **produces an aggregate base security score** ranging from 0.0 to 10.0

Risk Assessment Approaches

QUANTITATIVE VERSUS QUALITATIVE



Two factors of risk assessment, **impact** and **likelihood**, can be treated either **quantitatively** or **qualitatively**

IMPACT

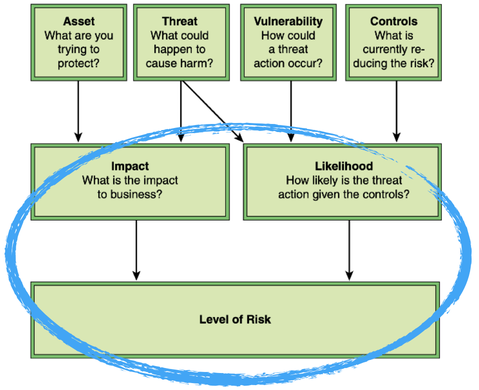
In a **quantitative** approach we can assign a specific **monetary cost** to each of the impact areas, then the overall impact can be expressed as a monetary cost. Otherwise, **qualitative** terms, such as **low, moderate, and high,** are used.

LIKELIHOOD

The **quantitative** version of likelihood is simply a **probability value**, and again the **qualitative** likelihood can be expressed in such categories as **low, medium, and high**.

Quantitative Risk Assessment (1/2)

WE CAN USE EQUATIONS



If all factors are expressed quantitatively, then it is possible to develop **a formula that measure of the cost of security breaches** as follows:

$$\text{Level of risk} = (\text{Probability of adverse event}) \times (\text{Impact value})$$

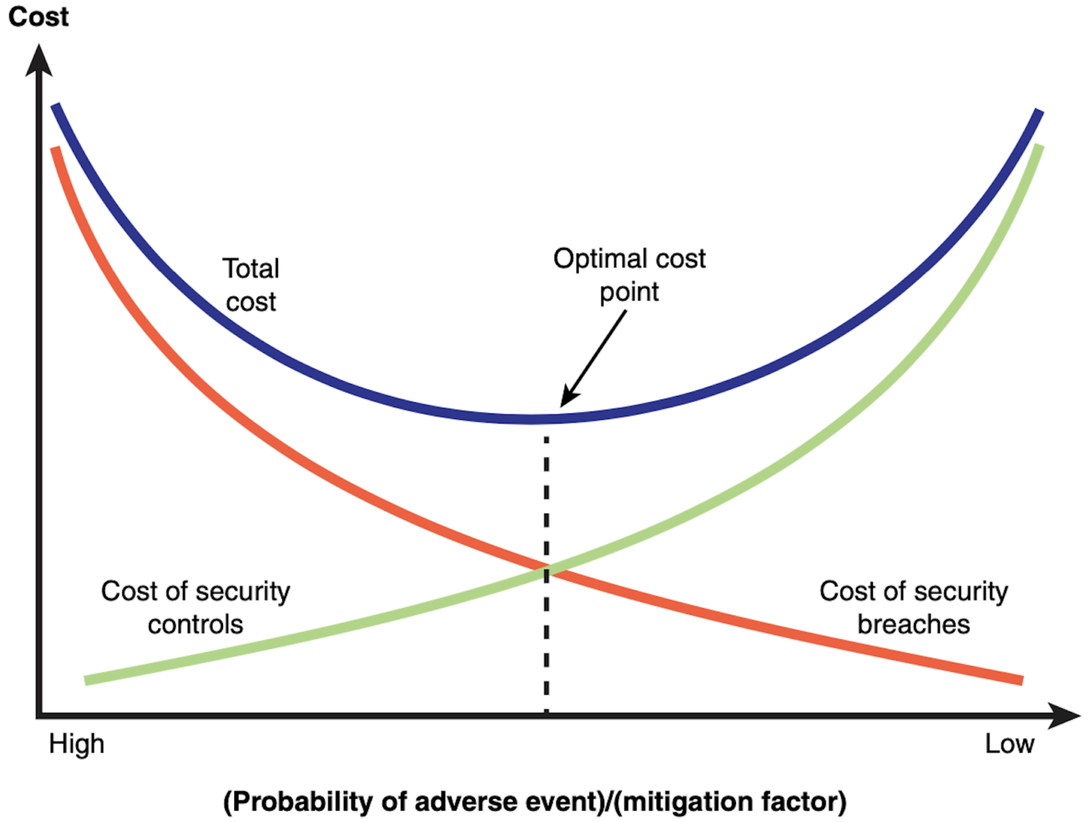
We can express the **residual risk level** using the mitigation factor that reflects the reduction in the probability of an adverse event due to the implementation of security controls. Thus, **the residual risk level is equivalent to the expected cost of security breaches with the implementation of controls**.

$$\text{Residual risk level} = \frac{(\text{Probability of adverse event})}{(\text{Mitigation factor})} \times (\text{Impact value})$$

Quantitative Risk Assessment (2/2)

WE CAN USE EQUATIONS

If the various **factors can be quantified** with a reasonable degree of confidence, then **previous equations should be used to guide decisions concerning how much to invest in security controls**



As **new security controls are implemented**, the residual probability of an adverse event declines and, the **cost of security breaches declines**. However, at the same time, the **total cost of security controls increases as new controls are added**.

The upper curve represents the total security cost, consisting of the cost of security breaches plus the cost of security controls. **The optimal cost point represents a level of risk that is tolerable** and cannot be reduced further without the expenditure of costs that are disproportionate to the benefit gained.

Qualitative Risk Assessment

USING REASONABLE JUDGMENT

It is not reasonable to suppose that all impact costs and likelihoods can be expressed quantitatively. At the same time, the **total cost** or potential loss due to a **security breach is hard to quantify**.

Qualitative assessment determines a **relative risk rather than an absolute risk**. This considerably simplifies the analysis, producing rough estimates of risk levels.

Qualitative risk assessment **is usually sufficient for identifying the most significant risks** and allowing management to set priorities for security expenditures with a reasonable degree of confidence that all the significant risks have been mitigated.

Quantitative vs Qualitative

COMPARISON

	Quantitative	Qualitative
Benefits	•Risks are prioritized by financial impact; assets are prioritized by financial values. •Results facilitate management of risk by return on security investment. •Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage). •Accuracy tends to increase over time as the organization builds historic record of data while gaining experience	•Enables visibility and understanding of risk ranking. •Easier to reach consensus. •Not necessary to quantify threat frequency. •Not necessary to determine financial values of assets. •Easier to involve people who are not experts on security or computers.
Drawbacks	•Impact values assigned to risks are based on subjective opinions of participants. •Process to reach credible results and consensus is very time consuming. •Calculations can be complex and time consuming. •Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. •Process requires expertise, so participants cannot be easily coached through it.	•Insufficient differentiation between important risks. •Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis. •Results are dependent upon the quality of the risk management team that is created.

“impact values assigned to risks are based on subjective opinions of participants” is listed as a drawback of quantitative risk assessment.

But it is clear that **subjective estimates are inherent in the process**!

At the end for the qualitative risk we need to define levels fo risk!

Qualitative Risk: Impact Category

AN ORGANIZATION NEED SHOULD CLEARLY DEFINE THEM

FIPS 199

"Standards for Security Categorization of Federal Information and Information Systems"

defines three security categories of impact:

Low

Expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals, including the following:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
- Result in minor damage to organizational assets
- Result in minor financial loss
- Result in minor harm to individuals

Moderate or Medium

Expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals, including the following:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
- Result in significant damage to organizational assets
- Result in significant financial loss
- Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries

High

Expected to have a **severe** or catastrophic adverse effect on organizational operations, organizational assets, or individuals, including the following:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
- Result in major damage to organizational assets
- Result in major financial loss
- Result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries

Qualitative Risk: Impact Assessment

AN ORGANIZATION NEED SHOULD CLEARLY DEFINE THEM

Ranges of probability are assigned to qualitative likelihood categories.

NIST SP 800-100 *"Information Security Handbook: A Guide for Managers"* suggests the following categories

- **Low**: ≤0.1
- **Medium**: 0.1 to 0.5
- **High**: 0.5 to 1.0

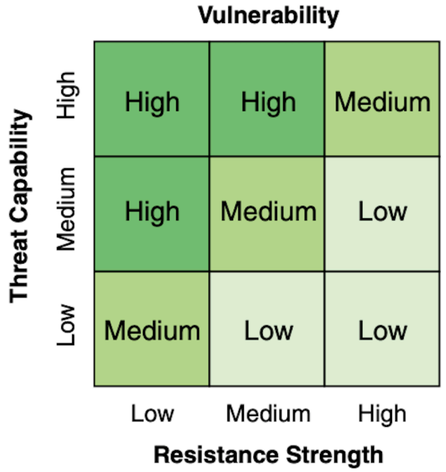
Another possible categorization **is based on an estimate of the number of times per year an event occurs**:

- **Low**: <1 time per year
- **Medium**: 1 to 11 times per year
- **High**: >12 times per year

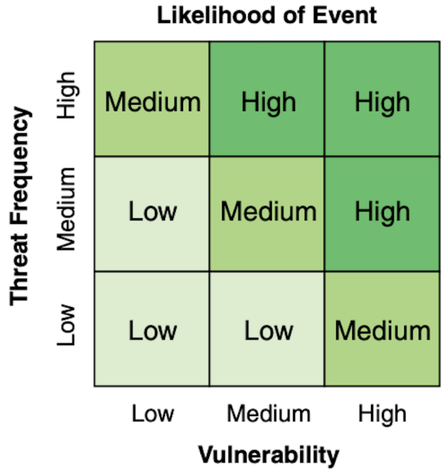
Qualitative Risk Determination

MATRICES TO DETERMINE RISK

The **vulnerability** to a particular threat is a function of the capability, or strength, of the threat and the resistance strength of a system or an asset to that particular threat.



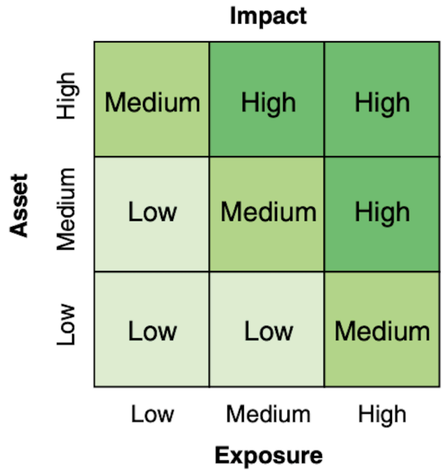
(a) Vulnerability as a function of threat and resistance



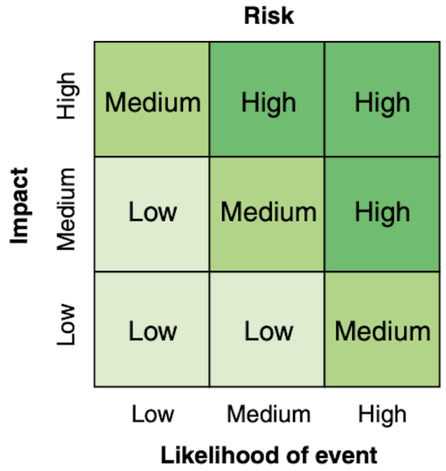
(b) Likelihood as a function of threat and vulnerability

The **likelihood of an adverse security event** causing a particular threat is a function of the frequency, or likelihood, of the threat occurring and the vulnerability to that threat

Impact is determined as a function of asset class and the exposure to loss that a particular threat could cause



(c) Impact as a function of asset and exposure



(d) Risk as a function of impact and likelihood

And finally, **the risk can be expressed as a function of impact and the likelihood!**

Qualitative Risk: keep in mind!

The results of such a coarse analysis **must be subject to judgment**.

For example, a low-likelihood, high- impact breach and a high-likelihood, low-impact breach **are both rated as medium risk**.

Which should be given priority for scarce security resources?

- **On average, each type of breach may be expected to yield the same amount of annual loss.**

  Question: Is it more important to deal with a **low-likelihood, high- impact breach** — because although rare, if it does occur, it could be catastrophic for the organization — **or** deal with the **high-likelihood, low-impact breach** — which could produce a steady stream of losses.

That is for management to decide!

Simple Risk Analysis Worksheet

A **simple approach** to risk assessment is to use a risk analysis **worksheet**, which is

a table with one row for each potential threat/vulnerability pair.

This **worksheet**, prepared by the risk assessment team, contains the following **columns**:

- **Security issue:** A brief statement of each security issue or area of concern. There should be **one row for each threat/vulnerability pair**.
- **Likelihood:** Estimated likelihood for an occurrence of this threat/vulnerability pair. The estimate should be based on the team's judgment of the value of the affected assets and the magnitude of the exposure, using the matrices explained before.
- **Impact:** Estimated impact for this threat/vulnerability pair. The estimate should be based on the team's judgment of the affected assets value of the magnitude of the exposure, using the matrices explained before.
- **Risk level:** Risk level, based on the matrix showed before.
- **Recommended security controls:** Specific security control(s) that the team is recommending to address this particular issue.
- **Control priorities:** Relative priority of each recommended control.
- **Comments:** Any other information that is considered relevant to the security risk management decision-making process for this particular security issue.

Simple Risk Analysis Worksheet: Compliance Issue

COMPLIANCE ISSUES CAN BE DOCUMENTED ON THE SAME WORKSHEET

- **Compliance requirements** include **those imposed by the organization's security policy**, government regulations, and applicable accreditation standards

- **Compliance** should be rated as follows:
  - **0** = not implemented
  - **1** = partially implemented
  - **2** = implemented but not yet documented
  - **3** = implemented and documented

- For compliance issues, the Likelihood and Impact fields are irrelevant

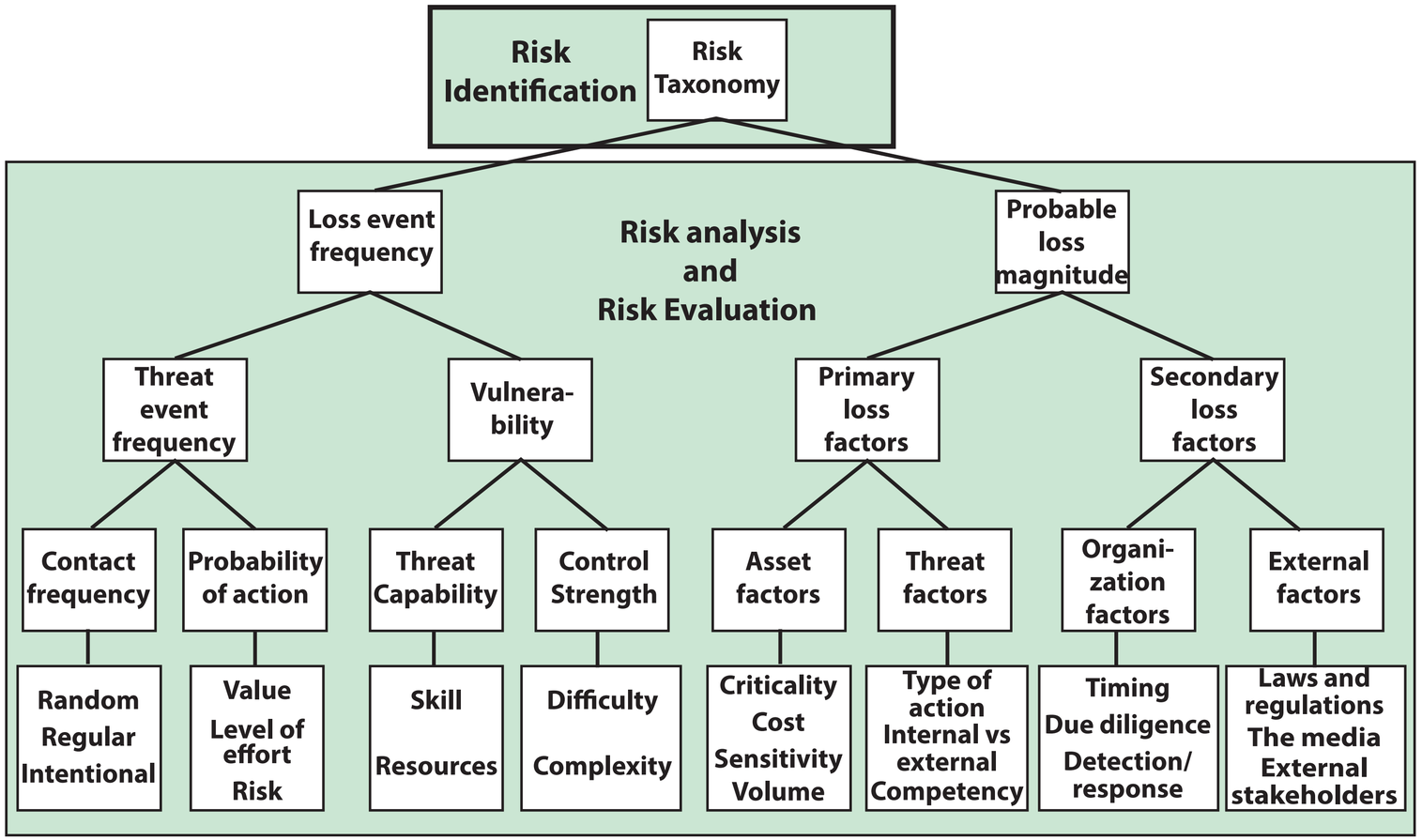
- **An issue with a compliance score of less than 3 should be included in the worksheet with a risk level of high**

Factor Analysis of Information Risk (FAIR) Process

APPROACH FOR THE RISK ASSESSMENT

- FAIR is an important contribution to risk assessment first introduced in 2005
- FAIR, which has been standardized by The Open Group, has received wide acceptance
- Its relationship to International Organization for Standardization (ISO) risk standards are summarized as follows:
  - **ISO 27001 describes a general process** for creating an information security management system (ISMS)
  - In that context, **ISO 27005 defines the approach to managing risk**
  - **FAIR provides a methodology for analyzing risk**
- Thus, **FAIR provides more specific guidance that can be used within the framework defined by ISO 27005**

Risk Assessment using FAIR



- FAIR provides a **more detailed set of guidelines than ISO 27005** for all aspects of risk assessment.
- FAIR provides definitions of the key terms that are **less vague and more specifically tied to the risk analysis** process than does ISO 27005.

The FAIR methodology is based on a belief that subjective **qualitative analysis is inadequate** in most situations and that all risk, tangible and intangible, is measurable and quantifiable.

Likelihood Assessment

PROCESS

- The process of developing some sort of agreed-upon **likelihood score that estimates the chance of a threat action**
- The **assessment considers** the presence, tenacity, and strengths **of threats** as well as the **presence of vulnerabilities** and the effectiveness of **security controls already in place**
- This assessment is **applied to each identified potential threat action**
- The essence of **likelihood assessment for a given threat** to a given asset is shown in the following steps:
  - **Step 1.** Determine **the likelihood that a threat event will occur**. That is, determine the likelihood that this threat will develop into an attack on the given asset
  - **Step 2.** Determine the **degree of vulnerability** of the asset to the threat
  - **Step 3.** Based on Step 1 and Step 2, **determine the likelihood that a security incident will occur**

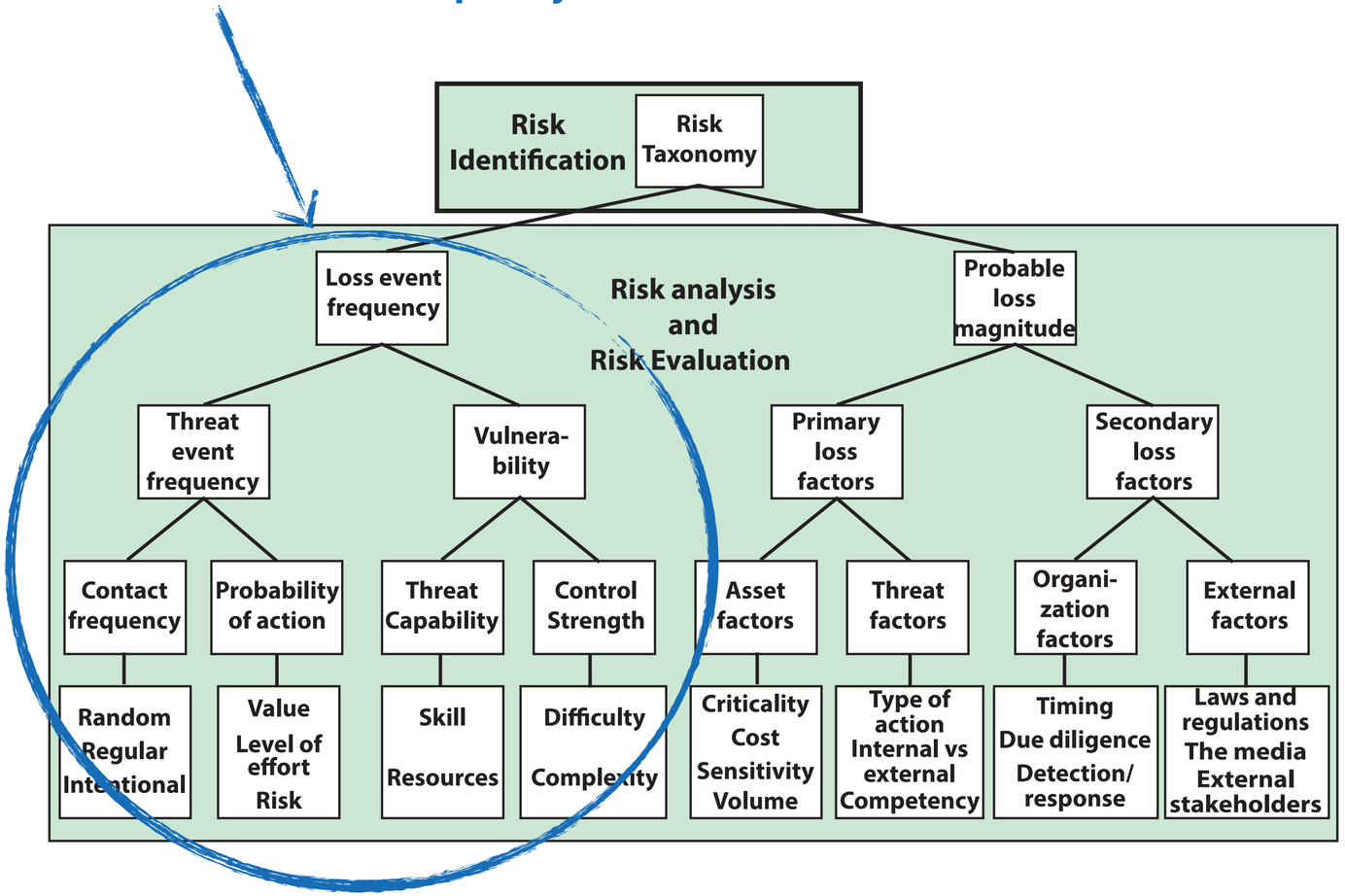
This analysis needs to be repeated for every threat to every asset.

FAIR Risk Assessment Levels (1/3)

A GUIDANCE ON LIKELIHOOD ASSESSMENT

ISO 27005 provide limited guidance on how to perform this function.

FAIR provides detailed guidance on how to systematically characterize event likelihood, referred to in the FAIR documents as **loss event frequency**.



FAIR Risk Assessment Levels (2/3)

	Loss Magnitude	Event Frequency	Threat Capability	Resistance Strength	Secondary Loss Probability
Very High (VH)	>1000X	> 100 times per year	Top 2% when compared against the overall threat population	Protects against all but the top 2% of an average threat population	90% to 100%
High (H)	100X to 1000X	Between 10 and 100 times per year	Top 16% when compared against the overall threat population	Protects against all but the top 16% of an average threat population	70% to 90%
Moderate (M)	10 X to 100X	Between 1 and 10 times per year	Average skill and resources (between bottom 16% and top 16%)	Protects against the average threat agent	30% to 70%
Low (L)	X to 10X	Between 0.1 and 1 times per year	Bottom 16% when compared against the overall threat population	Only protects against bottom 16% of an average threat population	10% to 30%
Very Low (VL))	<X	< 0.1 times per year (less than once every 10 years)	Bottom 2% when compared against the overall threat population	Only protects against bottom 2% of an average threat population	0% to 10%

X = monetary value assigned by organization

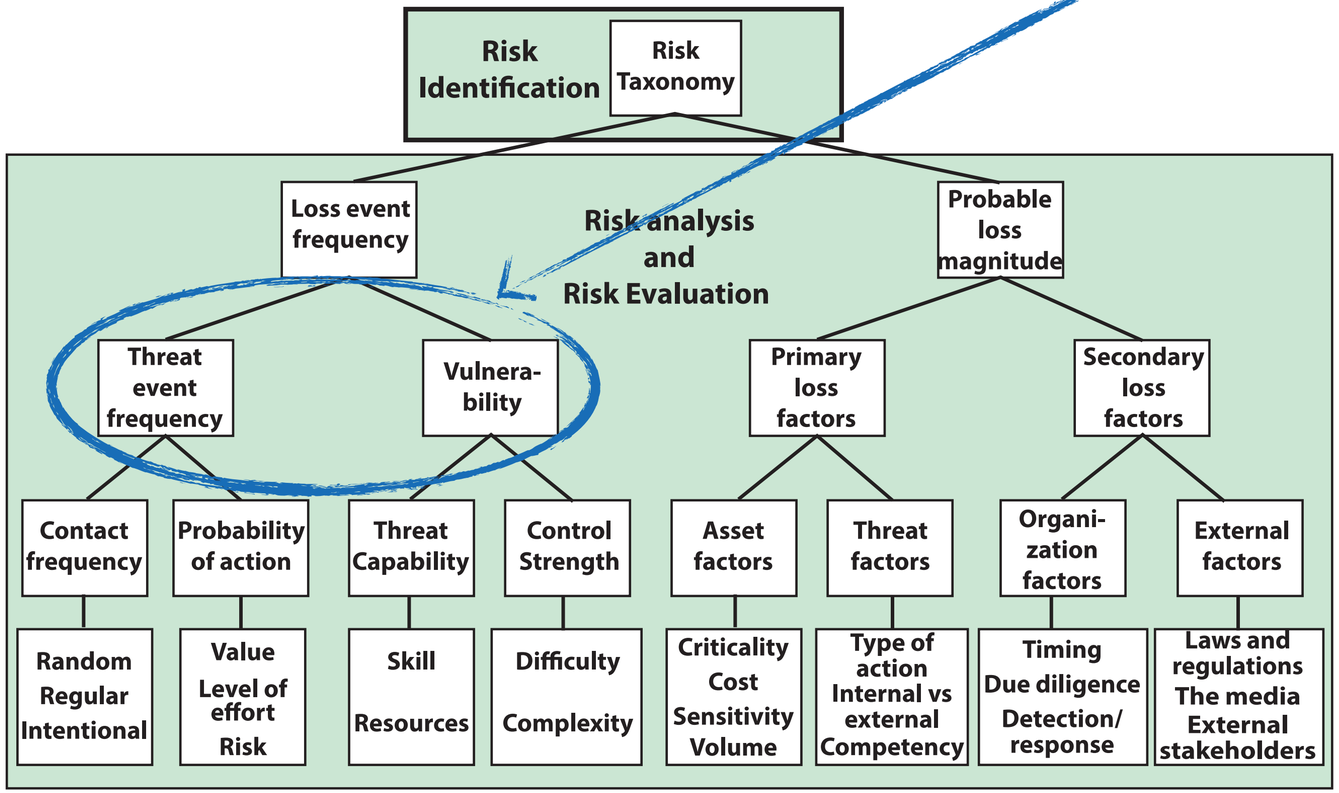
FAIR adopts a **top-down approach** to determining loss event frequency.

At the top level, it may be possible, **based on historical data, to develop an estimate of loss event frequency,** simply on the basis of how frequently a loss event has occurred in the past.

FAIR Risk Assessment Levels (1/3)

A GUIDANCE ON LIKELIHOOD ASSESSMENT

If the organization's management or security analysts **do not have confidence that a good loss event frequency can be directly estimated**, then the process is broken down into two tasks: **estimating threat event frequency** and **estimating vulnerability.**



FAIR: Estimating Threat Event Frequency

The assessment of threat event frequency **involves two aspects**:

(1) Determining the **frequency** with which a threat agent will come in **contact with an asset**

(2) The **probability** that, once in contact, the threat agent will **act against the asset**

1

Contact can be physical or logical

- **Physical** access is possible for employees, contract workers such as cleaning and maintenance crews, and outside actors, such as clients, customers, salespeople, and inspectors
- **Logical** access is via a network

Contact can be unplanned, or random, or it can be regular, such as with a cleaning crew or it can be intentional as when a hacker tries to gain logical access

The task for a security analyst is to come up with a reasonable estimate, such as using **five levels of frequency: VH, H, M, VL.**

2

The next task is to determine the **probability that the threat agent will take action**, given that contact has been made.

- This, of course, depends on the nature of the threat and the type of action available to the threat agent.

FAIR: Estimating Vulnerability

The two dimensions of vulnerability are the **threat capability** and the **control strength**

(1) FAIR defines threat **capability** as the capability of the threat community to act against an asset using a specific threat

(2) The technique used in FAIR is to define **five levels of threat capability that describe the strength** of a specific threat

1

Estimating **threat capability** involves looking at two factors:

- **Skill:**
  - The knowledge and experience of the threat agent are critical factors in the severity of the threat action
  - Skill is reflected in the manner in which a threat agent is able to act, such as performing social engineering or bypassing logon or other access barriers
- **Resources:**
  - The other important factor is the resources, such as the time, financial resources, and materials that a threat agent can use

2

The other dimension is the **control strength** (or **resistance strength**).

- The FAIR approach is to define **five levels of resistance strength**, based on the percentage of a threat population that an asset can successfully contrast: **VL, L, M, H, VH**

Impact Assessment

PROCESS

- The process of developing some sort of agreed-upon **impact score or cost value that estimates the magnitude or the adverse consequence of a successful threat action.**
- **The essence of impact assessment** is that, for a given threat to a given asset, you determine the **impact (cost or relative magnitude of impact)** on the asset if the threat were to **become an actual security incident**.
- FAIR provides detailed guidance on how to systematically characterize impact.
- FAIR impact analysis depends on **two categories of loss**: **primary** and **secondary**

This analysis needs to be repeated for every threat to every asset.

Impact Assessment: Estimating the Primary Loss

LOSS CATEGORIES

Primary Loss: Occurs **directly as a result of the threat agent's action upon the asset**. The owner of the affected assets is considered the primary stakeholder in an analysis. **This event affects the primary stakeholder in terms of productivity loss, response costs, and so on.**

Estimating:

1. There are two aspects to this assessment:
   - **Asset factors:** The value of the asset under threat
   - **Threat factors:** Threat factors that contribute to the loss

2. The next step is to **determine what threat action might apply to this asset**. Possible actions include:
   - **Access**: simple unauthorized access
   - **Misuse**: unauthorized use of assets
   - **Disclosure**: the threat agent illicitly disclosing sensitive information
   - **Modification**: unauthorized changes to an asset
   - **Deny access**: destruction or theft of a non-data asset

Impact Assessment: Estimating the Secondary Loss

LOSS CATEGORIES

Secondary loss factors: Occurs as **a result of secondary stakeholders** (for example, customers, stockholders, regulators) **reacting negatively to the primary event**. The reactions of the secondary stakeholders may, in turn, act as new threat agents against the organization's assets (such as **reputation**, legal fees, and so on), which, of course, affects the primary stakeholder.

Estimating two components:

1. Secondary loss **magnitude**:
   - **Losses that are expected to materialize** from dealing with secondary stakeholder reactions (for example, fines and judgments, loss of market share)
   - Two sets of factors need to be considered in determining the nature of the threat: organizational and external factors.

2. Secondary **loss event frequency**:
   - To derive the secondary loss frequency, the analyst first needs to estimate the probability that a secondary stakeholder would be engaged, generating some form of secondary loss

Risk Determination

COMBINE PRIMARY AND SECONDARY RISK

- **Once the loss magnitude is estimated and the loss event frequency derived, it is a straightforward process to derive an estimate of risk!**
- This is done **separately for primary and secondary risks**, and then the two are combined.
- The two risks are then **combined to determine an overall risk** using the matrix

Example of FAIR Risk Assessment Matrices

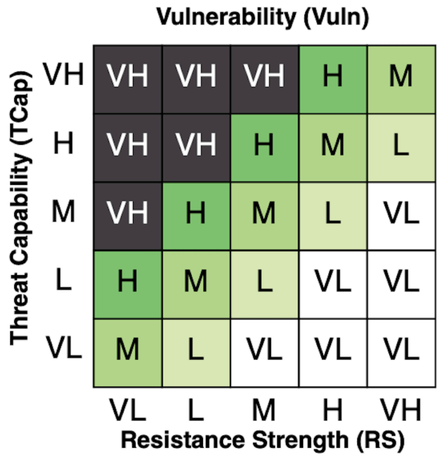
FAIR MATRICES TO DETERMINE RISK

As shown, the higher the resistance strength, the lower the vulnerability, and the higher the threat capability, the higher the vulnerability.

The vulnerability values shown in the matrix are based on the experience of those involved in developing the FAIR model.

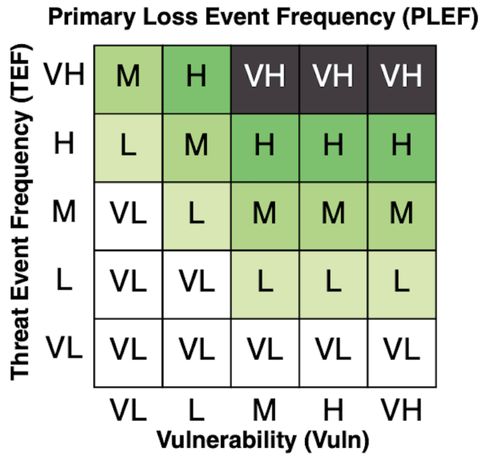
Once the loss magnitude is estimated and the loss event frequency derived it is a straightforward process to derive an estimate of risk

This is done separately for primary and secondary losses



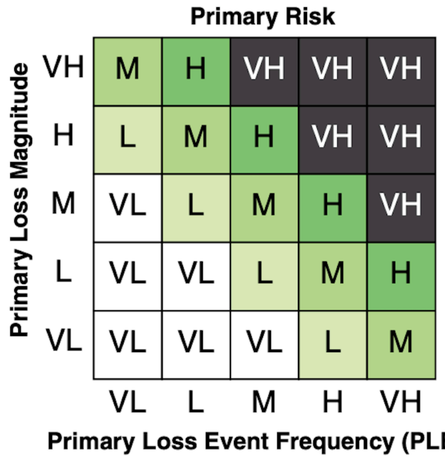
Vuln = f_1(RS, TCap)

(a)



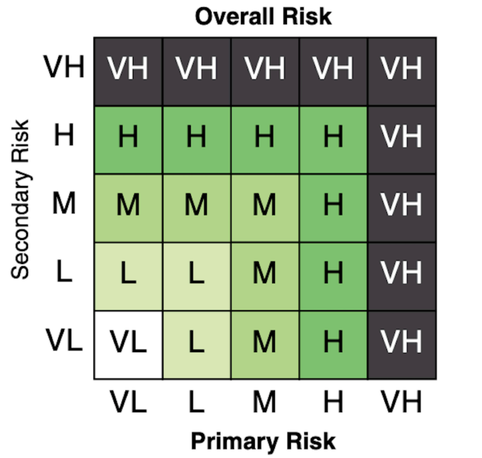
PLEF = f_2(Vuln, TEF)
SLEF = f_2(SLP, PLEF)

(b)



Primary Risk = f_3(PLEF, Primary Loss Magnitude)
Secondary Risk = f_3(SLEF, Secondary Loss Magnitude)

(c)



Risk = f_4(Primary Risk, Secondary Risk)

(d)

Primary and secondary Loss Event Frequency are calculated separately and then used to calculate primary and secondary Risk

The two risks are then combined to determine an overall risk

Risk Evaluation

WHICH FIRST?

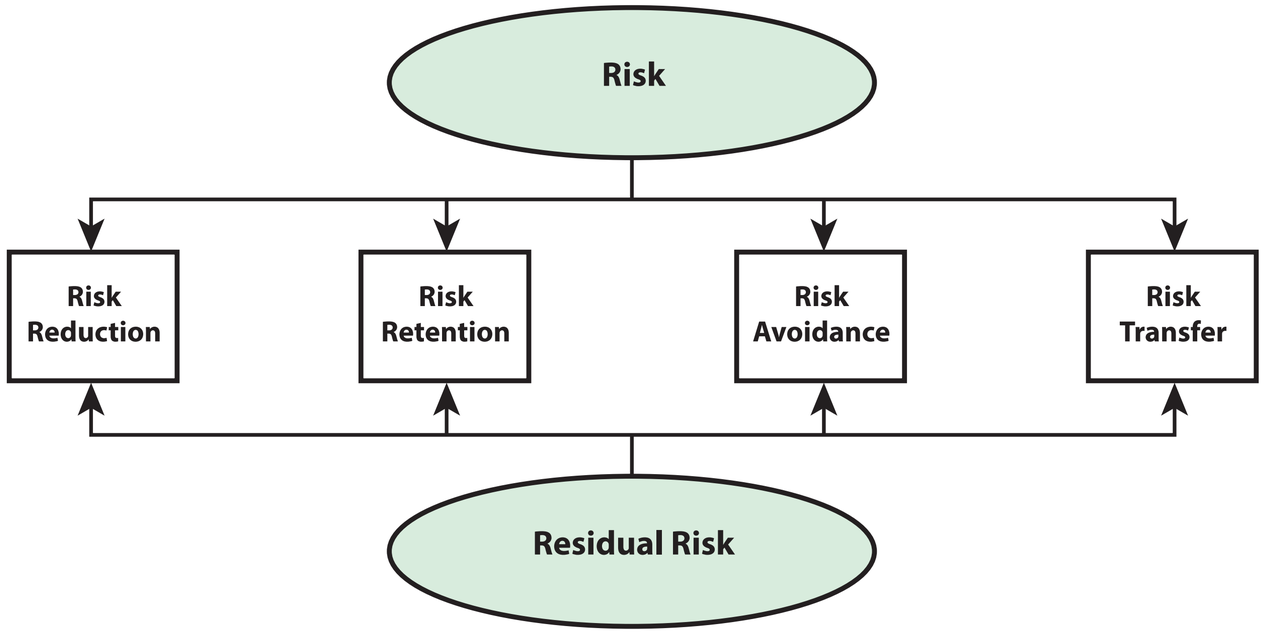
- **Evaluation process:** Once a risk analysis is done, **senior security management and executives can determine whether to accept a particular risk and if not determine the priority in assigning resources to mitigate the risk**.

- This process, known as risk evaluation, involves **comparing the results of risk analysis with risk evaluation criteria**.

- **SP 800-100 provides some general guidance for evaluating risk** and prioritizing action based on a three-level model:
  - **High**
    - If an observation or a finding is evaluated as high risk, there is a strong need for corrective measures
    - An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible
  - **Moderate**
    - If an observation is rated as moderate risk, corrective actions are needed
    - A plan must be developed to incorporate these actions within a reasonable period of time
  - **Low**
    - If an observation is described as low risk the system's authorizing official must either determine whether corrective actions are still required or decide to accept the risk

Risk Treatment

ISO 27005



ISO 27005 lists these options for treating risk:

- **Risk reduction or mitigation**: Actions taken to lessen the probability and/or negative consequences associated with a risk
- **Risk retention:** Acceptance of the cost from a risk
- **Risk avoidance:** Decision not to become involved in, or action to withdraw from, a risk situation
- **Risk transfer or sharing:** Sharing with another party the burden of loss from a risk

Risk Treatment: Reduction

ISO 27005

Risk reduction is achieved by **implementing security controls**.

Security controls can result in the following:

- **Removing the threat source**
- **Changing the likelihood** that the threat can exploit a vulnerability
- **Changing the consequences** of a security event

Risk Treatment: Retention

ISO 27005

Risk Retention

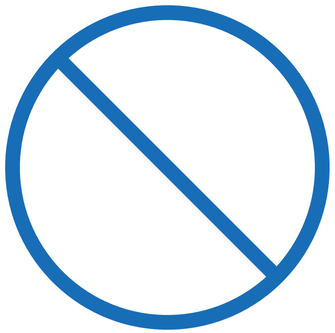
- Also called risk **acceptance**, is a conscious management decision to pursue an activity despite the risk presented or to abstain from adding to the existing controls, if any, in place to protect an asset from a given threat
- This form of **treatment is acceptable if the defined risk magnitude is within the risk tolerance level** of the organization

Risk Treatment: Avoidance

ISO 27005

Risk Avoidance

- If the risk in a certain situation **is considered too high** and the costs of mitigating the risk down to an acceptable level exceed the benefits, the organization may choose to avoid the circumstance leading to the risk exposure
- Some examples include forgoing a business opportunity, relocating to avoid an environmental threat or legal liability, or banning the use of certain hardware or software



Risk Treatment: Transfer

ISO 27005

Risk Transfer

- Sharing or transferring risk is accomplished **by allocating all or some of the risk mitigation responsibility or risk consequence to some other organization**
- This can take the form of obtaining insurance or subcontracting or partnering with another entity

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

simone.soderi@unipd.it

M2.1 - Planning for Cybersecurity

Thanks for your attention!