2023 | 2024

Network and Information Systems Security

Information Security Risk Management

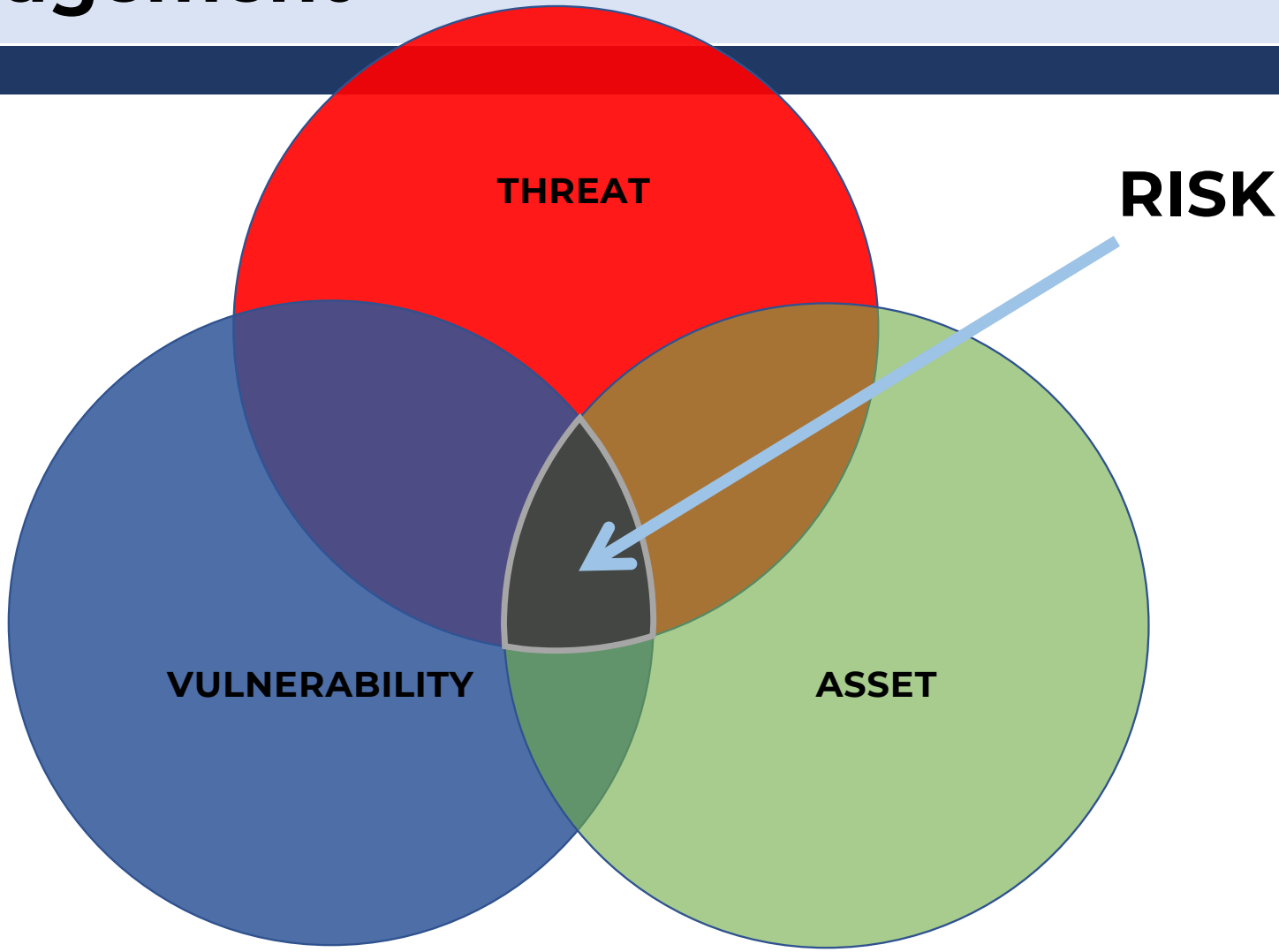
Carlos Serrão
carlos.serrao@iscte-iul.pt

iscte INSTITUTO UNIVERSITÁRIO DE LISBOA

Risk Management

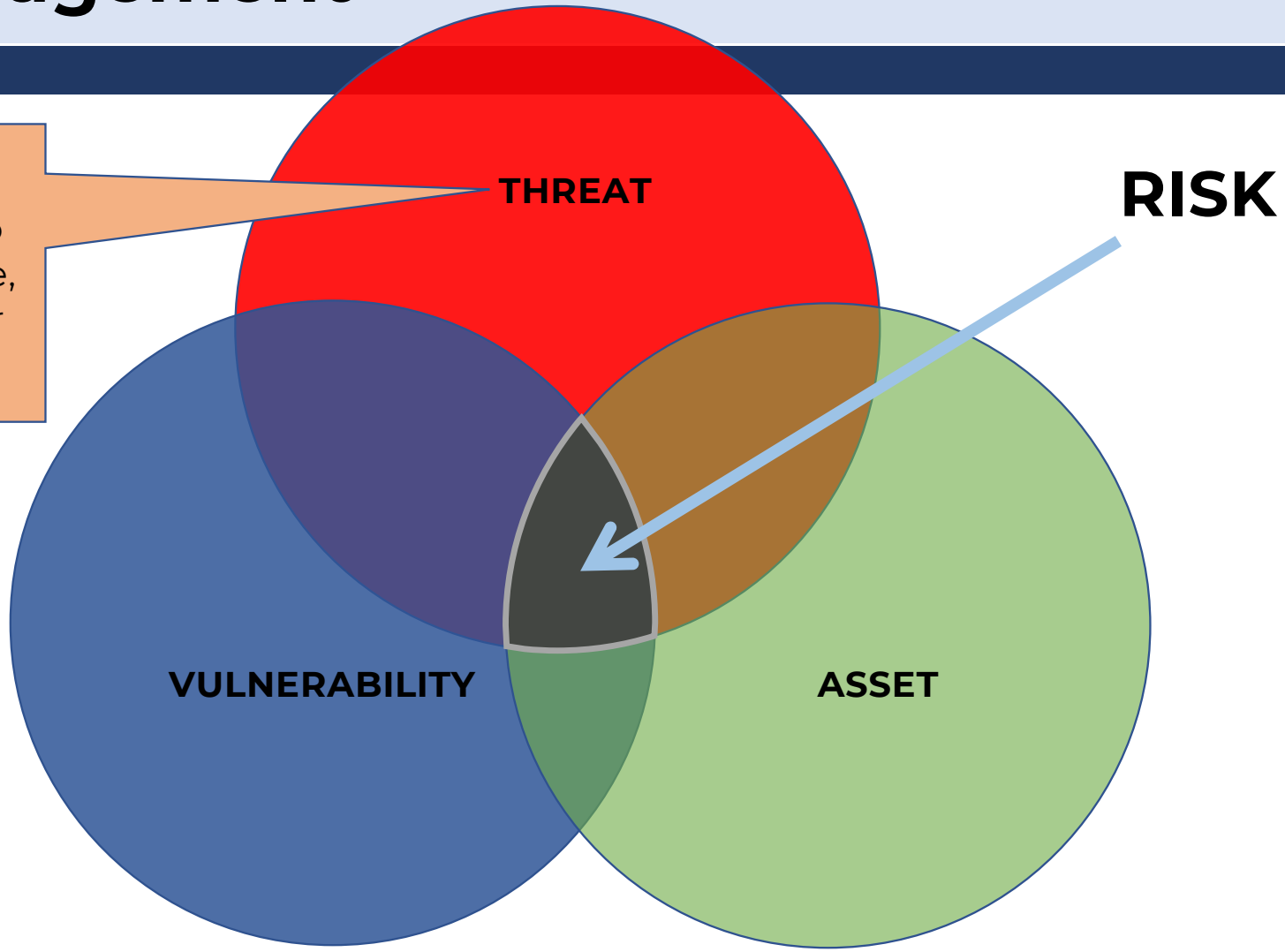
- A **central component** of the **Organization's Security Program**
- It should be included/defined **as a project** under development in the **governance policies/framework**
- **Indicates** the **vision** of the **real posture** of the **organization's information security**
- Helps **meet** due diligence and **due care obligations**
- The organisation is **negligent** if **risk management is not well carried out**
- It should be carried out annually or if there are substantial changes in the environment

Risk Management

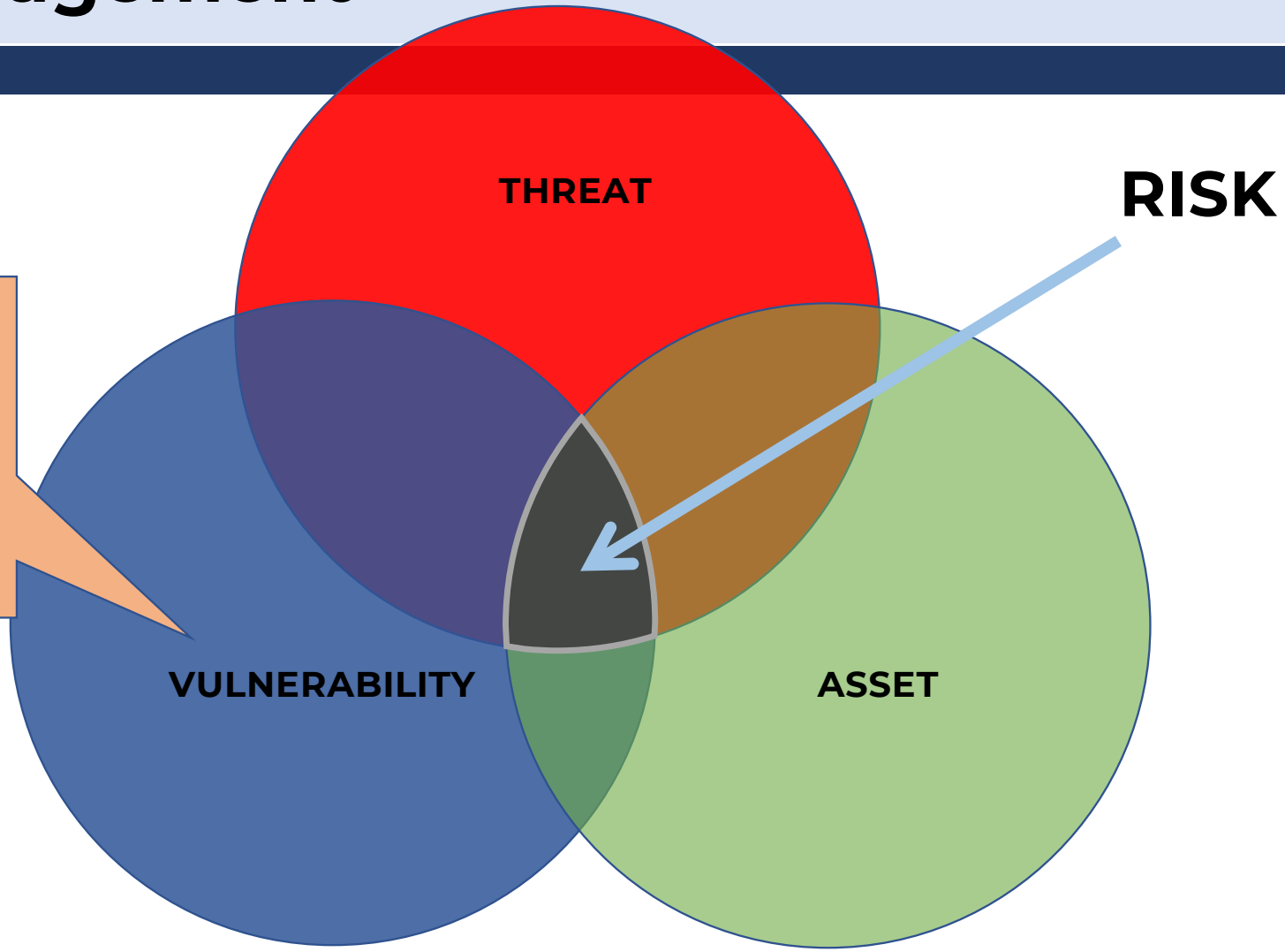


Risk Management

A threat is a negative event that can lead to an undesired outcome, such as damage to, or loss of, an asset.

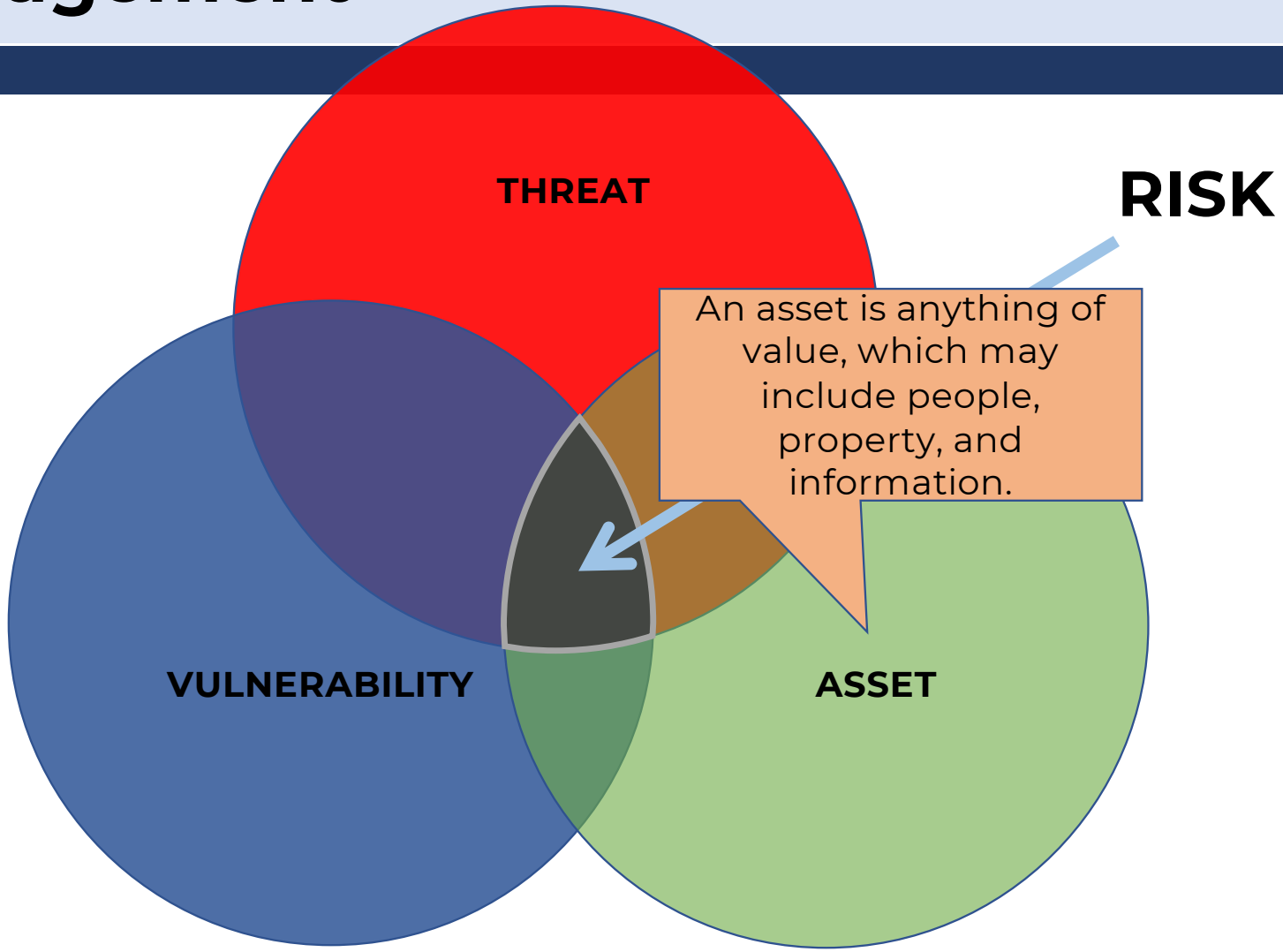


Risk Management



A vulnerability is a weakness or gap that exists within a system that may be exploited (by a threat actor) to compromise an asset's security or trigger a risk event.

Risk Management



Risk Management Project

Risk Management

⇢Starts with **Risk Identification** and **Assessment**:

⇢The development of **knowledge** and **awareness** of the **risks facing the organization**

⇢**Risk Assessment** is essentially **conversation** and **documentation**

⇢**Risk Assessment** is a **subset** of **Risk Management**

Risk Assessment

Risk assessment is the set of **activities** that involve **identifying the threats** and **vulnerabilities** that exist and **determining the impact and likelihood** of those threats exploiting the identified vulnerabilities

Risk Assessment

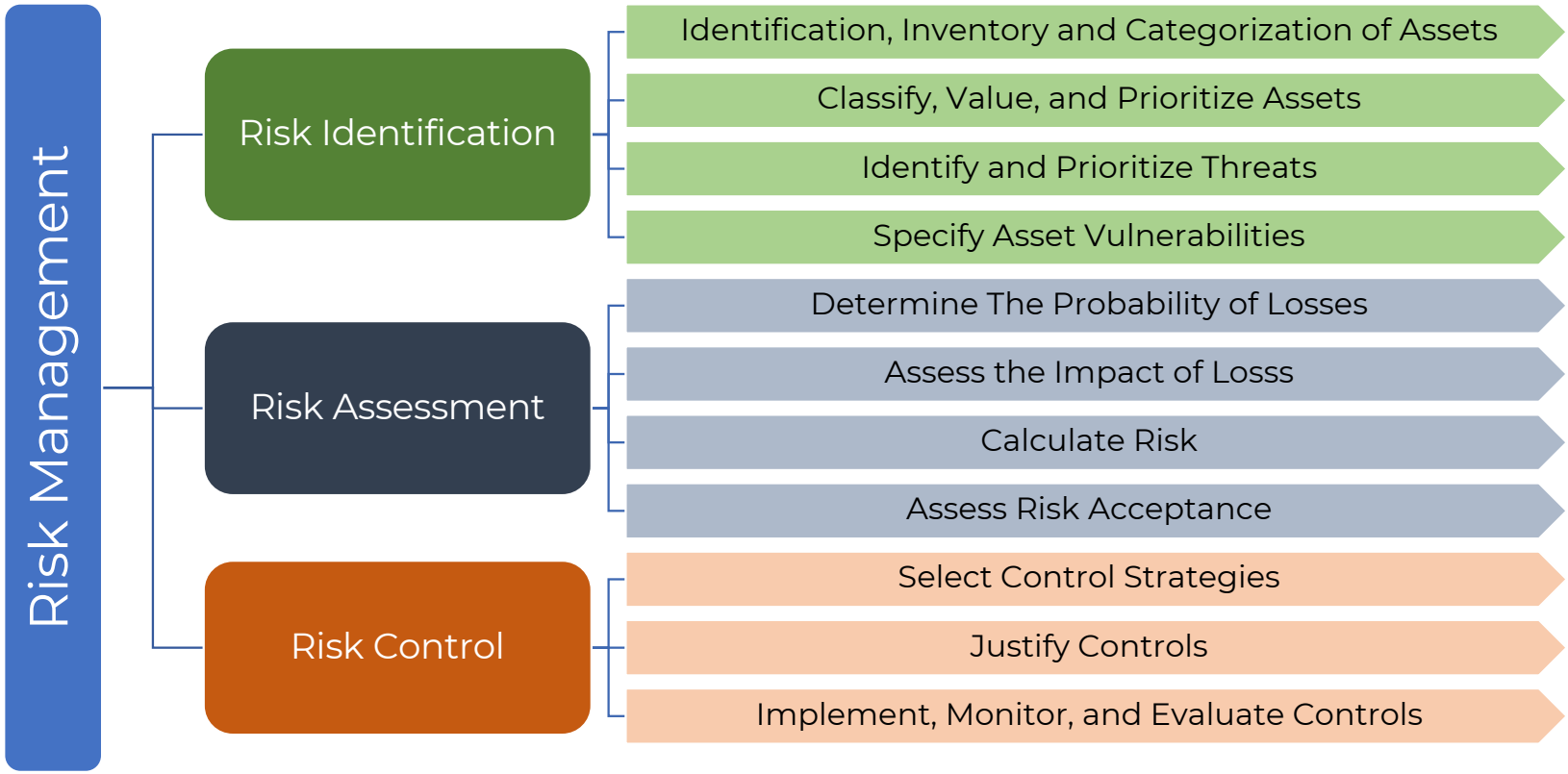
Identify your **assets** and **determine the value of those assets** (systems, applications and information); **Identify** and **describe** the **vulnerabilities** and **threats** that **pose a risk to** each of those assets.

Risk Assessment

Always begin with a **vulnerability assessment** and a **threat analysis**; Focused on evaluating the **likelihood** of identified threats exploiting weaknesses and determining the **impact** to your assets if that happens.

Risk Assessment

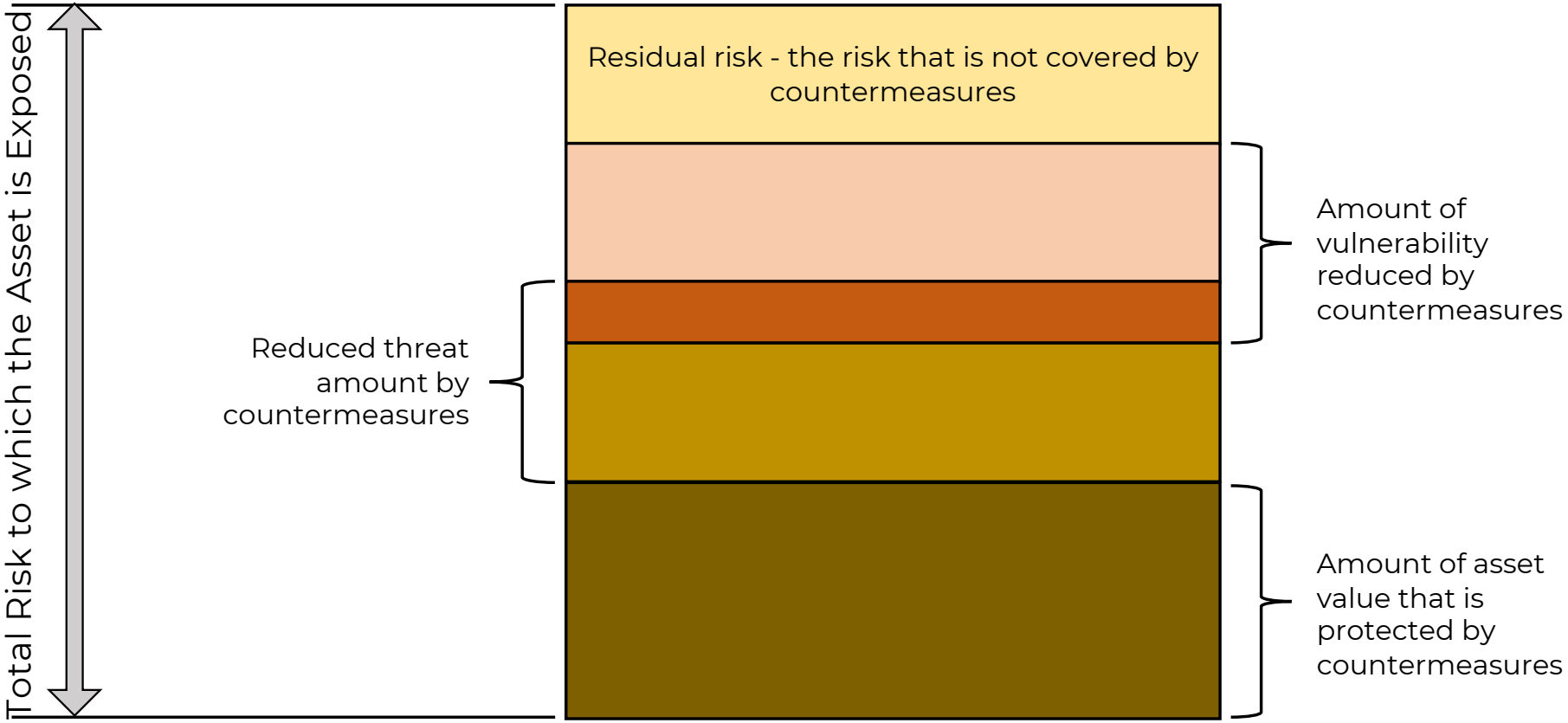
Risk Management Process



Risk Appetite and Residual Risk

- **Risk Appetite**: Defines the **amount** and **nature** of the **risk** that organizations are **willing to accept as a "trade-of" between perfect security and unlimited accessibility**
  - Reasonable approach: ensures the balance between the expense of controlling vulnerabilities against potential losses if a vulnerability is exploited.
- **Residual Risk**: Risk that has **not been completely removed**, **transferred** or **planned**
  - The purpose of information security is to align the residual risk with the risk appetite of the.

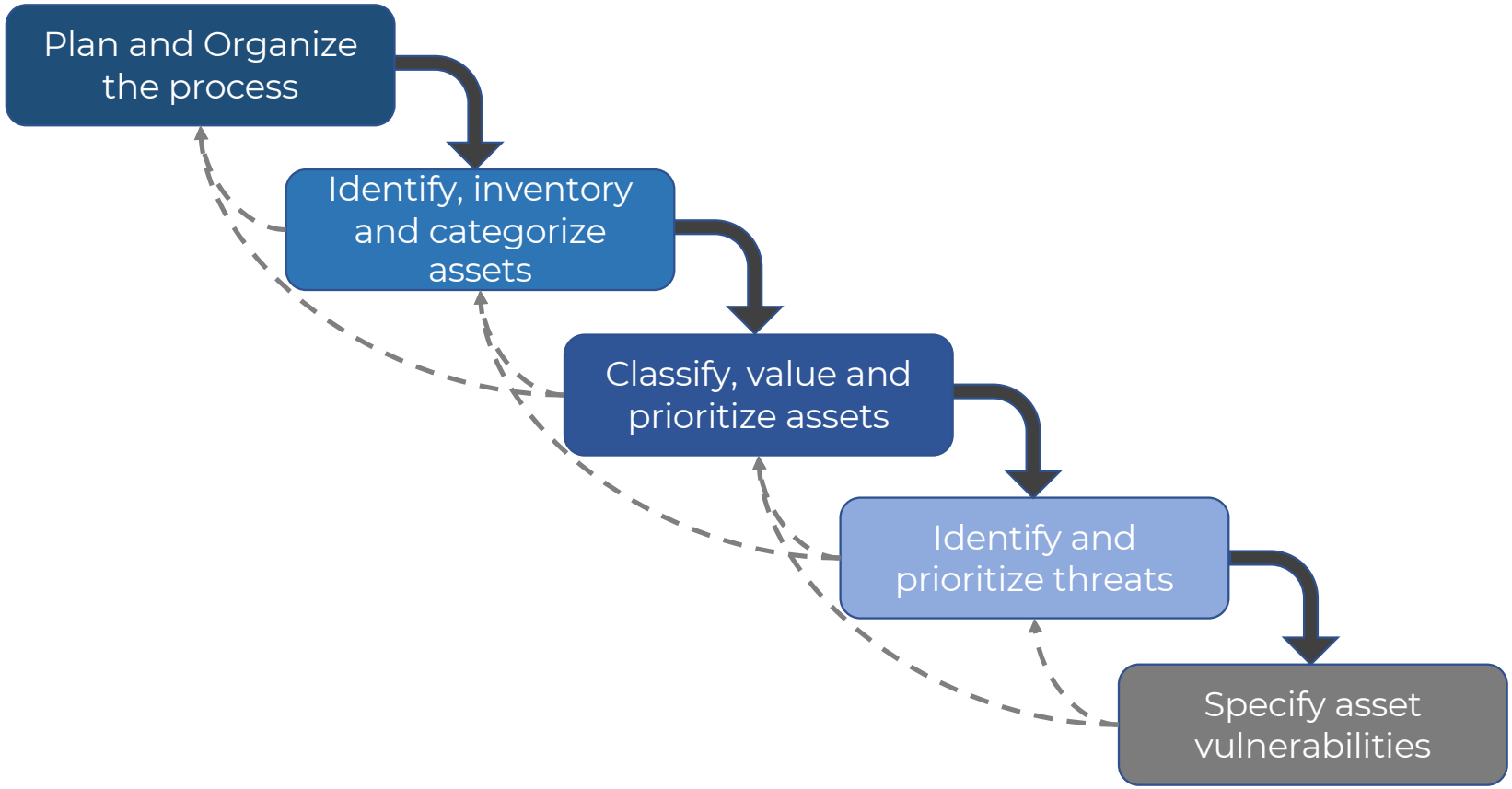
Residual Risk



Risk Identification

- Risk Management involves the **identification**, **classification** and **prioritization** of the organization's assets
- The **threat assessment** process **identifies** and **quantifies** the **risks** that **affect each asset**.

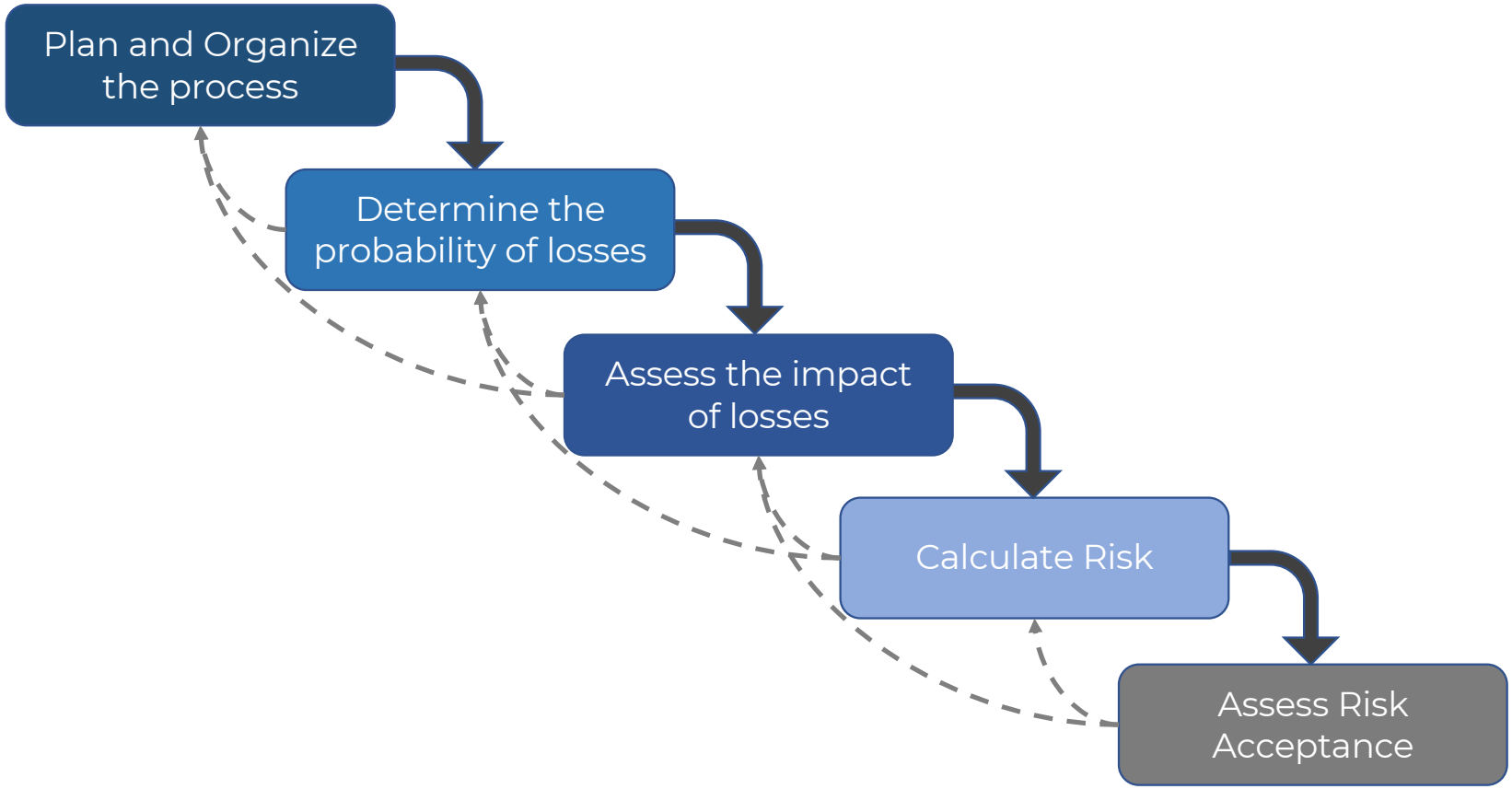
Risk Identification



Risk Assessment

- The risk assessment **assesses** the **relative risk** for **each vulnerability/threat**
- Assigns a **risk rating** or **score** to each information asset
- Plan and organise risk assessment
  - The objective at this point is to create a method to assess the relative risk of each identified vulnerability.

Risk Assessment



Risk Management Project | Beginning

- Project **Initiation**
  - Top management assigns responsibility, authority, budget, planning, and also…
    - Defines the scope - What part of the organisation are we assessing? Department, floor, building, campus, entire organisation, other?
      - Avoids possible confusion
      - Document interfaces and assumptions
  - Define the **Risk Management team**
    - There should be a representation of the main parts of the organisation within the scope of the RM project
    - Should also include people from the legal department, HR, network operations, security and others that are required.
  - Define/acquire **tools** and **methods to collect information**
    - Automated tools to support a project of this size!
    - Questionnaires, interviews, audits, intrusion testing, vulnerability assessments, etc.
  - Specific **training** and **task definition** for team members

Risk Frameworks

- **Risk framework** is a structured process for **identifying**, **assessing**, and **managing** an organization's **risks**.
- It should create a control environment with the following characteristics:
  - **Consistent**: A governance program must be consistent in how information security and privacy are approached and applied.
  - **Measurable**: The governance program must provide a way to determine progress and set goals.
  - **Standardized**: As with measurable, a controls framework should rely on standardization so results from one organization or part of an organization can be com- pared in a meaningful way to results from another organization.
  - **Comprehensive**: The selected framework should cover the minimum legal and regulatory requirements of an organization and be extensible to accommodate additional organization-specific requirements.
  - **Modular**: A modular framework is more likely to withstand the changes of an organization, as only the controls or requirements needing modification are reviewed and updated.

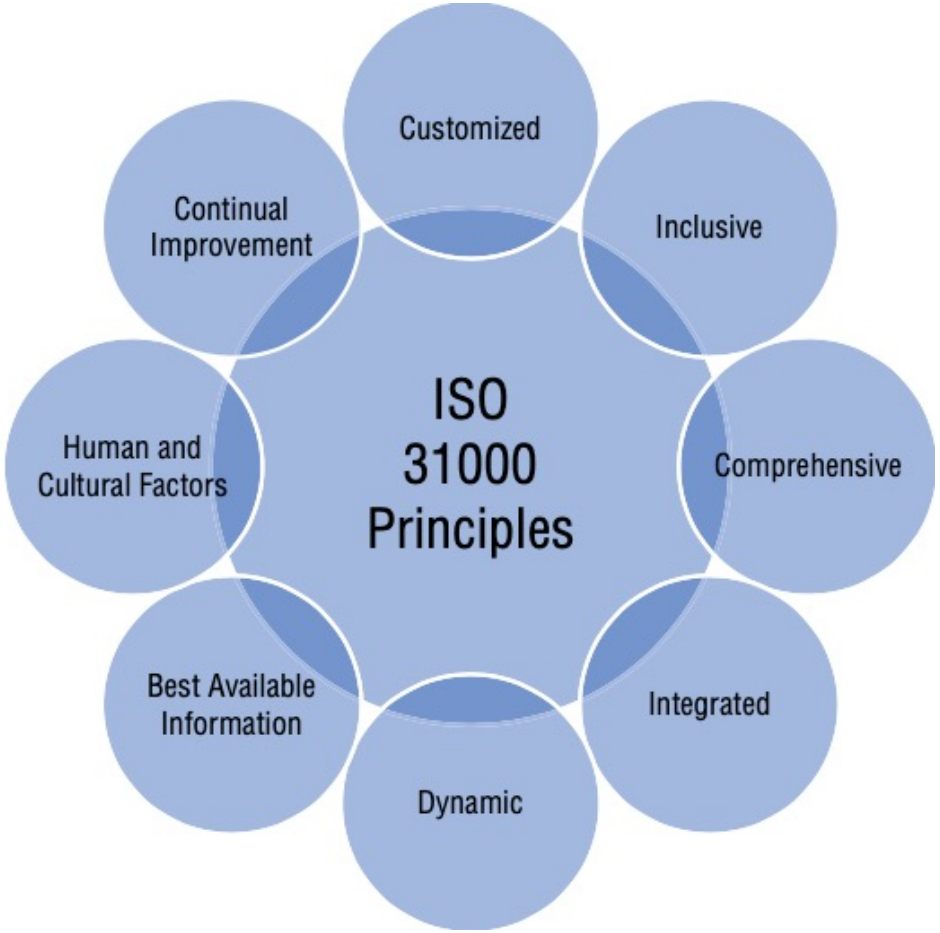
Risk Frameworks

- ISO/IEC 31000:2018 series (handling risk in general in every organization; common language)
- **ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”**
- **NIST Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems”**
- COBIT (Control Objectives for Information and Related Technologies)
- Factor Analysis of Information Risk (FAIR): is a taxonomy of the factors that contribute to risk and how they affect each other.
- RiskIT
- (...)

ISO/IEC 31000:2018 series

Risk Frameworks

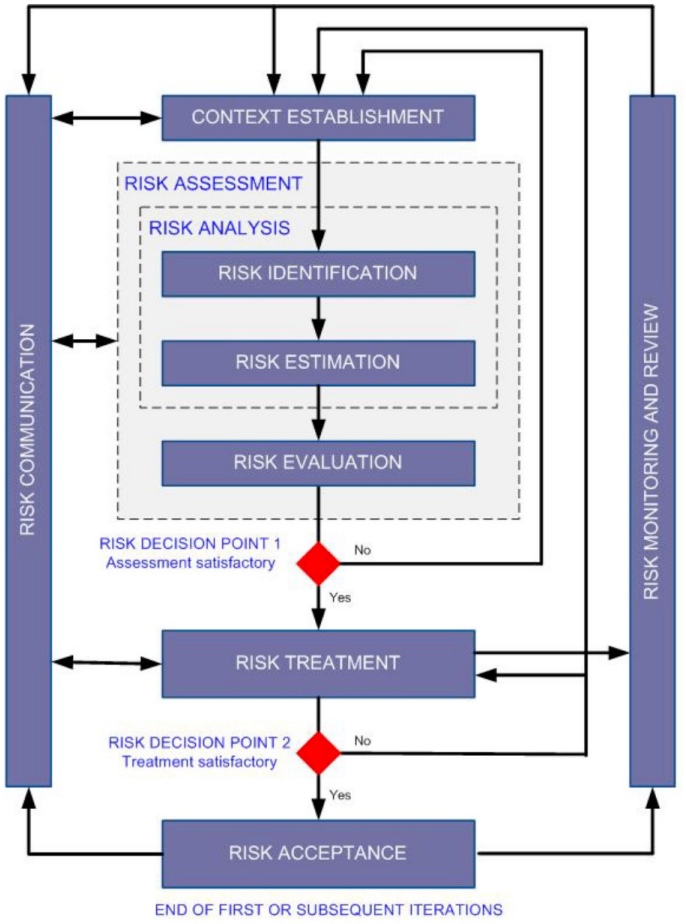
- Is intended to be **applicable** to **any organization**, regardless of the **governance structure** or **industry**.
- The **standard encourages** the **integration** of **risk management activities** across **organizational lines and levels** to provide the organization with a consistent approach to management of operational and strategic risks.
- Based on **eight principles**



ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”

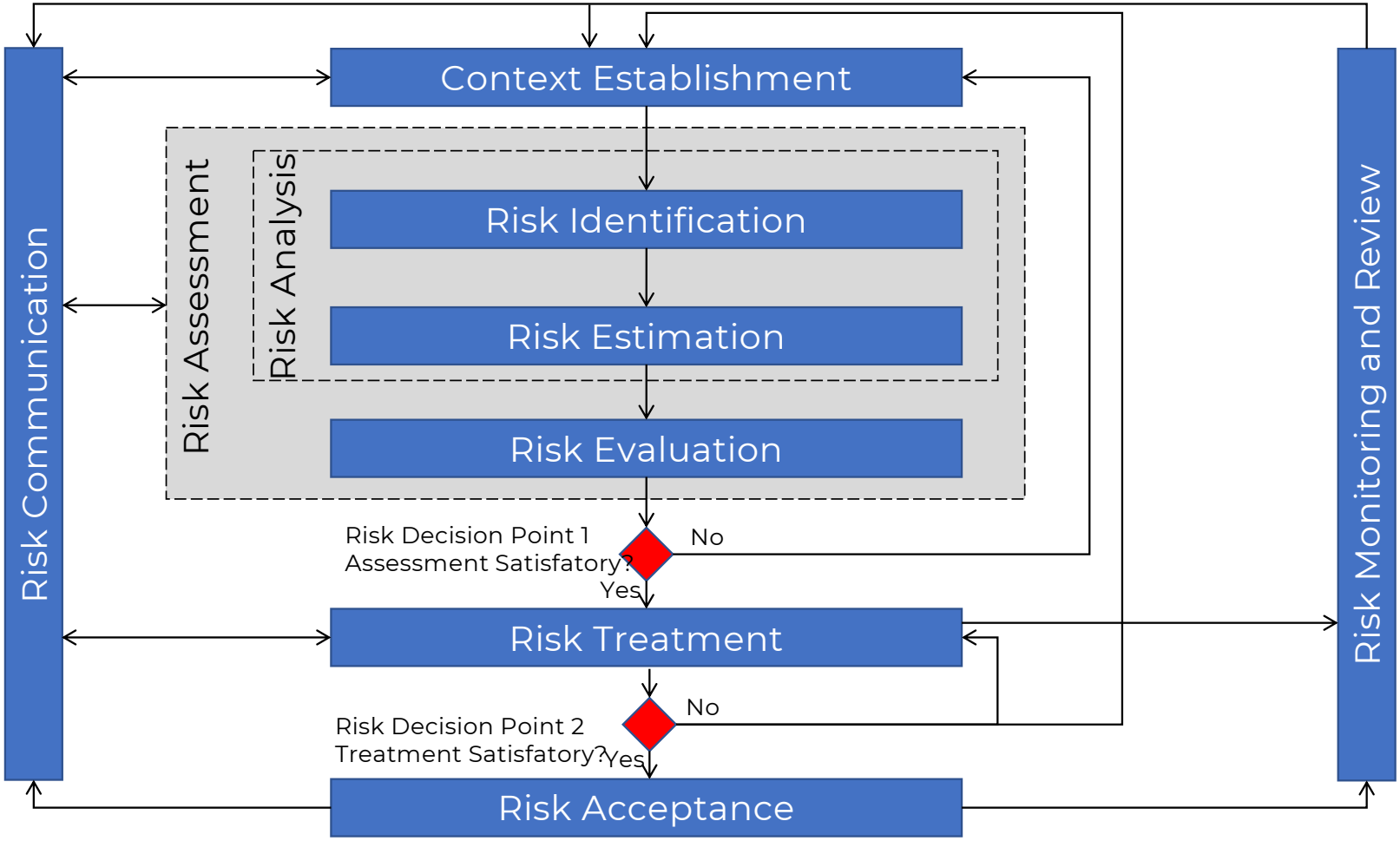
Risk Frameworks

- Gives **detail** and **structure** to the **information security risks** by defining the **context for information security risk decision-making**.
- Includes definition of the **organization’s risk tolerance**, **compliance expectations**, and the **preferred approaches for assessment** and **treatment** of risk.



ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”

Risk Frameworks



ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”

Risk Frameworks

Table 1 — Alignment of ISMS and Information Security Risk Management Process

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”

Examples of typical threats

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D

Type	Threats	Origin
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

D (deliberate)
A (accidental)
E (environmental)

ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”

Risk Frameworks

Origins of threats

Origin of threat	Motivation	Possible consequences
Hacker, cracker	Challenge Ego Rebellion Status Money	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge Political Gain Media Coverage	• Bomb/Terrorism • Information warfare • System attack (e.g. distributed denial of service) • System penetration • System tampering
Industrial espionage (Intelligence, companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Defence advantage • Political advantage • Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

ISO/IEC 27005:2011, “Information technology— Security techniques — Information security risk management”

Risk Frameworks

Vulnerabilities

Types	Examples of vulnerabilities	Examples of threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Susceptibility to temperature variations	Meteorological phenomenon
	Unprotected storage	Theft of media or documents
	Lack of care at disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
	Well-known flaws in the software	Abuse of rights
	No 'logout' when leaving the workstation	Abuse of rights
	Disposal or reuse of storage media without proper erasure	Abuse of rights
	Lack of audit trail	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
	Widely-distributed software	Corruption of data
	Applying application programs to the wrong data in terms of time	Corruption of data
	Complicated user interface	Error in use
	Lack of documentation	Error in use
	Incorrect parameter set up	Error in use
	Incorrect dates	Error in use

NIST Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems”

Risk Frameworks

I. **Categorise** - Systems & Data

II. **Select controls** - management approval

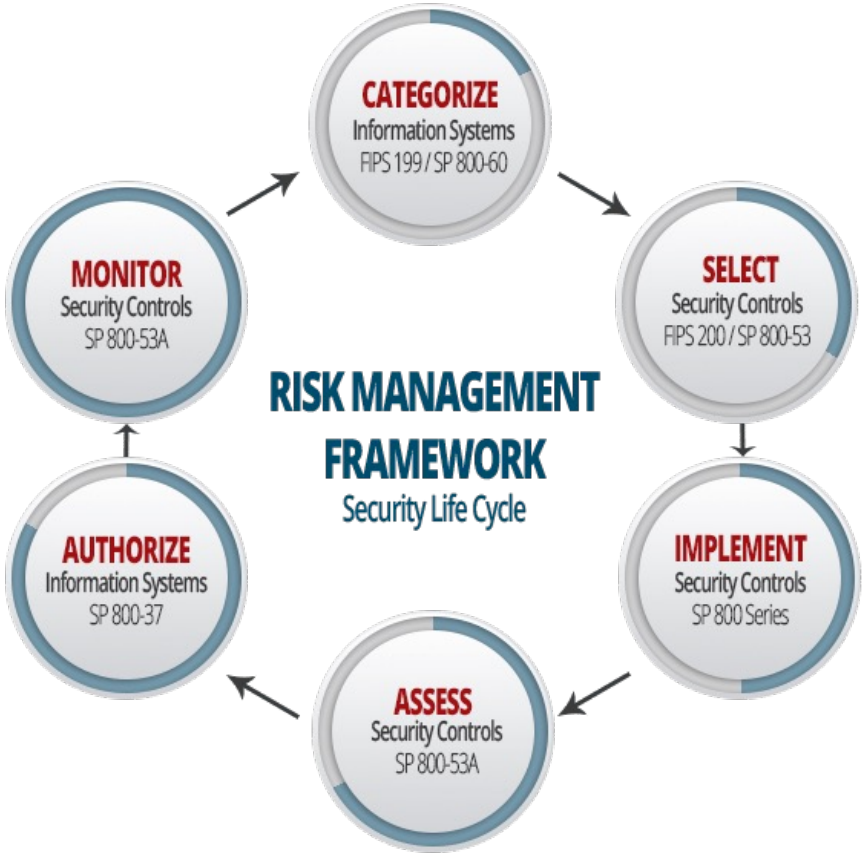
III. **Implement** controls

IV. **Evaluate** controls - assess their effectiveness

V. **Authorise** systems - in terms of data use, risk acceptance

VI. **Monitor** - continuous evaluation of effectiveness, metrics, reporting, breaches, breaches of data confidentiality

VII. **Repeat** - adjustments, improvements, new risks, new controls



NIST SP 800-37 | (I) Categorisation

1. Identify the inventory of all information assets with value (tangible and intangible)
2. Assign a value to each asset
3. Classify the asset based on its value
4. Perform a vulnerability and threat analysis/threat modeling for each asset
5. Identify and justify the cost of countermeasures for each threat
6. Prepare the evaluation report and the proposal of the selected countermeasures
7. Submit to management for approval

NIST SP 800-37 | (1) Asset Inventory

- Include **data elements** and **anything that supports** the data elements themselves
  - **Tangible** assets - physical
  - **Intangible** assets - digital content, reputation, IP

- Files
- Databases
- Documents
- HDD
- File servers
- Web servers
- Server racks
- Data center
- Air conditioning
- Electricity
- Workstations
- Building
- Workers
- Applications
- Routers
- Firewalls
- Security systems
- Audit systems
- Backup systems
- Clustered servers
- Application servers
- Laptops
- Switches
- Directory services
- VPN Servers
- Authentication devices
- Wireless APs
- others...

NIST SP 800-37 | (2) Assign value to each asset

NIST SP 800-37 | (2) Assign value to each asset

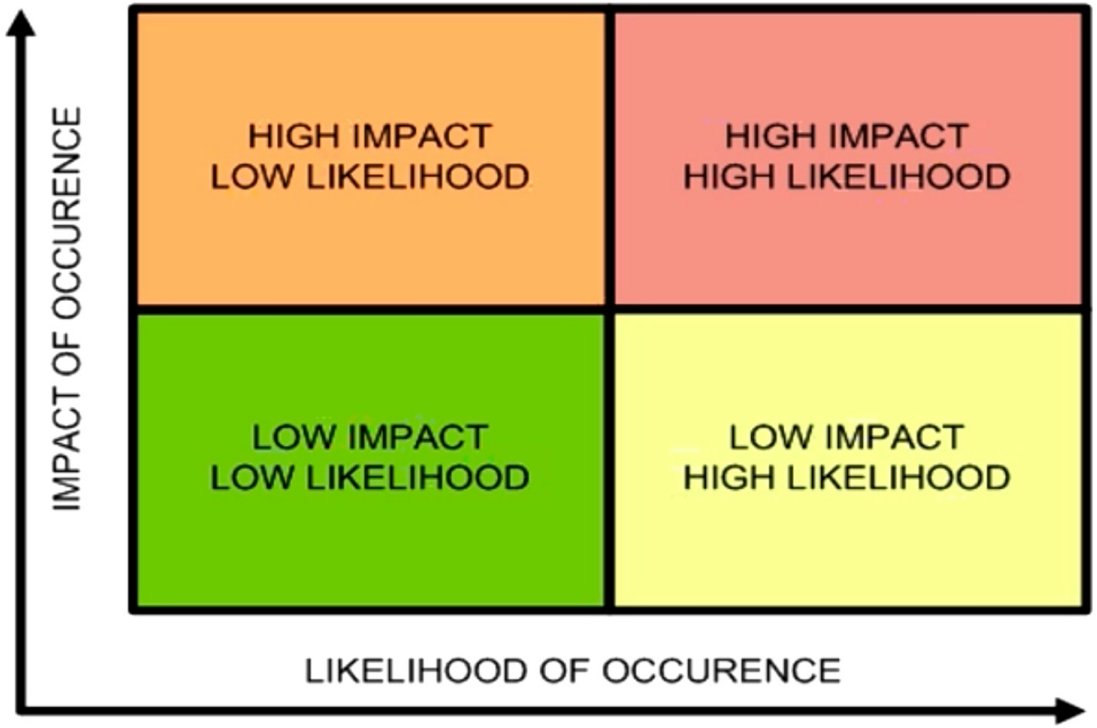
- **Quantitative** value
  - Value directly identified by numbers through invoices, receipts, quotations, etc.
- **Qualitative** value
  - Linked to the reputation of the company that identifies the customer's desire and preference to do business with it.

NIST SP 800-37 | (2) Assign value to each asset

- Most security breaches lead to **some form of damage** affecting the organisation's **reputation**
- This **damage** has an **impact on turnover and profit**
- Lower **turnover** and **profit**, corresponds to a **loss by the incident**
- It is important to **assess the qualitative** value through **questionnaires and scenarios**
- It is important to **quantify** the **qualitative value** to **justify the cost** of **protections/countermeasures**

NIST SP 800-37 | (2) Assign value to each asset

- **Qualitative** assessment
  - Based on the **survey results**, show the **likelihood** and **impact** of **reputational damage** in a graph



NIST SP 800-37 | (2) Assign value to each asset

- **Quantitative** assessments and **qualitative** assessments
  - **Quantitative** risk analysis is **far more precise** and **objective**, because it **uses verifiable data to analyze** the **impact** and **likelihood** of each risk.
  - A **purely quantitative** assessment **is not possible**
    - It does not consider the negative impact on an organisation's reputation
    - The impact introduces losses that must be accounted for and made good
  - **Qualitative** risk analysis **avoids** the use of **numbers** and **tends to be more subjective**.
  - A **purely qualitative** assessment **is possible**, but **not recommended**
    - Since turnover/profit is the norm, base the analysis only on events that negatively influence it

NIST SP 800-37 | (3) Classify the asset based on its value

- Group assets into 4 or 5 categories to simplify protection measures
- Identify the **most valuable assets** (**Red**)
  - These will hurt the organisation the most if they are compromised
  - The budget to protect them will be the highest
  - The controls to protect these will be the most extensive

Red = $1M +

Orange = $500K até $1M

Green = $100K até $500K

Blue = < $100K

NIST SP 800-37 | (4) Vulnerability and threat analysis

- Start the **analysis/modelling** of the most **valuable assets first**
- What **negative occurrences** can happen to each asset?
- Consider the **full spectrum** of **threats** for **each asset**
  - Natural
  - Human
  - Technological
  - Supply
- Proceed with the **analysis down to the least valuable assets on the list**

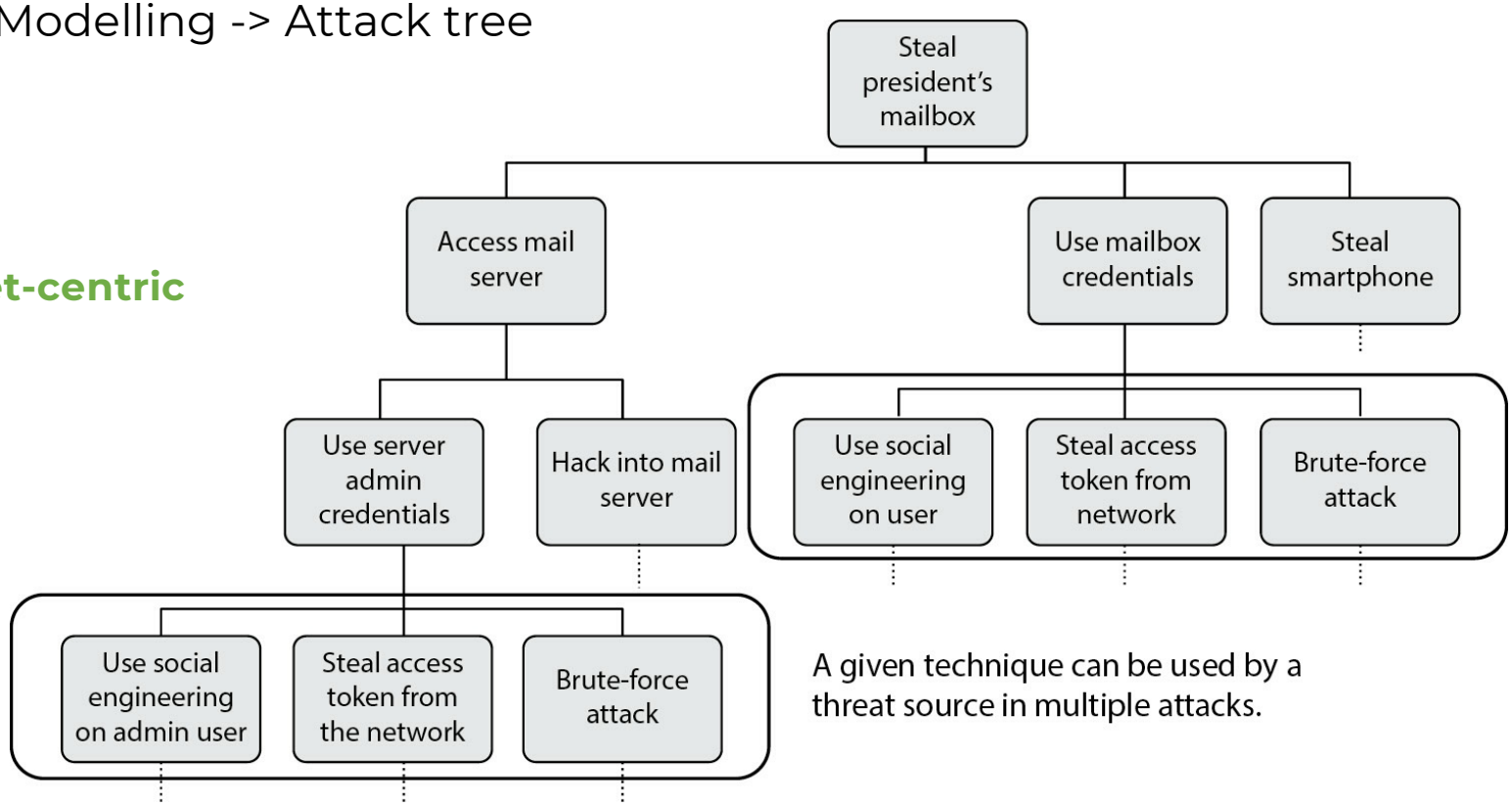
NIST SP 800-37 | (4) Threat Modeling

- **Three** general approaches
  - **Attacker-centric**
    - Starts by identifying the various actors who could potentially cause harm to a system
    - Start by profiling a potential attacker's characteristics, skillset, and motivation, and then use that profile to identify attackers who would be most likely to execute specific types of attacks
  - **Asset-centric**
    - Identifies the assets of value first.
    - Assets should be characterized by their value to the organization as well as their value to potential attackers.
  - **Software-centric (or System-centric)**
    - The system is represented as a set of interconnected processes, using architecture diagrams such as dataflow diagrams (DFDs) or component diagrams.
    - Diagrams are then evaluated by threat analysts to identify potential attacks against each component.

NIST SP 800-37 | (4) Threat Modeling

⇢Threat Modelling -> Attack tree

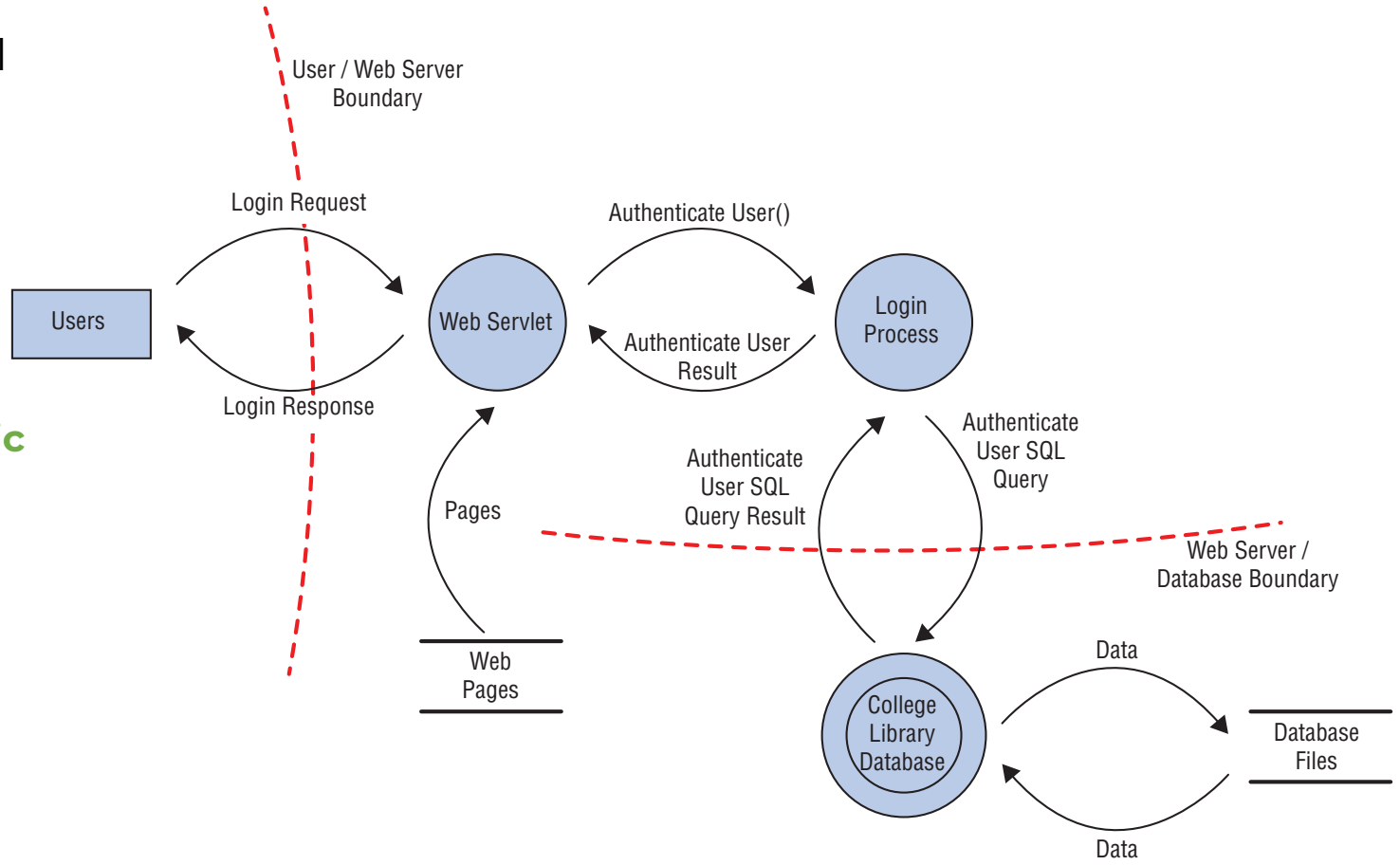
Asset-centric



A given technique can be used by a threat source in multiple attacks.

NIST SP 800-37 | (4) Threat Modeling

⇢Threat Model



System-centric

NIST SP 800-37 | (4) Threat Modeling

- Relationship between threats and vulnerabilities

Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data-processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

Threat Modeling

Risk Management

- **STRIDE** (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Previlege): late 1990, Microsoft
- **PASTA** (Process for Attack Simulation and Threat Analysis): 2012, dynamic threat analysis, more easily understood by upper management
- **NIST SP 800-154 - Guide to Data-Centric System Threat Modeling**: 2016
- **DREAD** (Damage, Reproducibility, Exploitability, Affected users, Discoverability): older, Microsoft, abandoned
- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Software Engineering Institute
- **TRIKE**: open-source
- **CORAS** (Construct a platform for Risk Analysis of Security Critical Systems): opens-source. European Project, based on UML
- **VAST** (Visual, Agile, and Simple Threat Modeling): proprietary, leverages Agile concepts

NIST SP 800-37 | (4) Calculating Losses

- Organisations operate on **annual financial calendars**
  - Convert **expected losses to annual loss levels**
  - For each **threat to each asset calculate** the **annualized loss expectancy (ALE):**

Asset Value (AV) x Exposure Factor (EF) = Single Loss Expectancy (SLE)

SLE x Annual Rate of Occurrence (ARO) = Annualized Loss Expectancy (ALE)

NIST SP 800-37 | (4) Calculating Losses

- Example :
  - Imagine a facility that is worth $1M. Your insurance agent tells you that this area floods every 15 years, and historically causes about 45% damage.

AV x EF = SLE	AV = $1M, EF = 45%	$1,000,000 x 0.45 = $450,000
SLE x ARO = ALE	ARO = 1/15	$450,000 x 1/15 = $30,000

  - The company **should plan to lose about $30,000 per year to address flooding**, in **its current security posture**.

NIST SP 800-37 | (4) Calculating Losses - ALE

- **ALE identifies** how much the company **should expect to lose per year due to threats**, according to its current security posture
- **ALE** is **used** to **identify the level of risk**, and to **justify the costs of countermeasures** during the proposal phase in Risk Management.

NIST SP 800-37 | (5) Countermeasures

⇢Countermeasures **selection criteria**:

- ⇢ **Personnel-related**
- ⇢ **Process-related**
- ⇢ **Technology-related**

⇢**Three** types of countermeasures: **administrative**, **technical** and **physical**

⇢Consider using security services offered by third parties - Security as a Service (SECaaS)

Administrative

- Policies, rules, laws, customs
- They work through user awareness, an expectation of compliance
- Policies, rules, laws, customs
- They work through user awareness, an expectation of compliance

Technical

- Software controls such as permissions, encryption, firewall rules, AV software, IDS/IPS, etc..

Physical

- Walls, doors, locks, guards, dogs, cameras, lights, barriers, IDS/IPS sensors

NIST SP 800-37 | (5) Types of Countermeasures

Deterrence
- convince the attacker not to attack -- psychology -- before

Delay
- delay the attackers - make dessuasion and detection more effective - during

Preventive
- prevents the loss from occurring - during

Detection
- identifies the attack as soon as possible - during and after

Evaluation
- determines the severity of the loss to adjust the response - during and after

Correction (answer)
- initial response to mitigate losses - during

Recovery (answer)
- after confinement, return to normal - during and after

Compensation
- alternates controls if primary controls are not available

Management
- information albeits, usually related to safety, efficiency, traffic flow

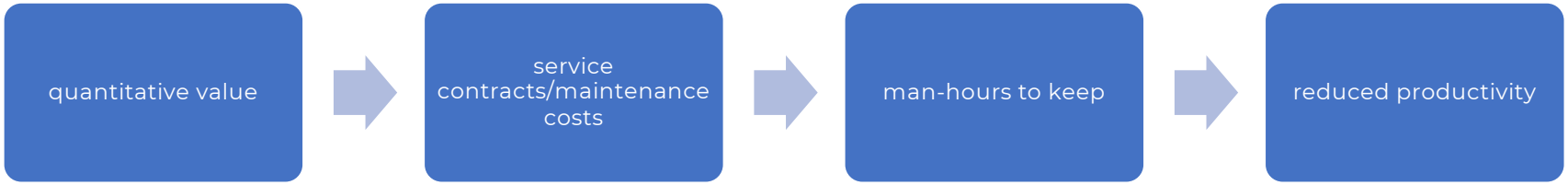
NIST SP 800-37 | (5) Assessment of countermeasures

- Goal: **reduce exposure** and **attack surface**
  - For each of the threats, identify one or more cost-justified countermeasures that eliminate or mitigate the vulnerability, likelihood and/or impact of the incident
  - For the countermeasure it is important to understand:

NIST SP 800-37 | (5) Assessment of countermeasures

⇢**Determine** the **annual cost of countermeasures** and the **amount of additional protection offered** (reduction in ALE) by **the countermeasure**

⇢It **should consider all aspects** of the **cost** of the proposed countermeasure:



NIST SP 800-37 | (5) Justification of the cost of countermeasures

⇢The **share of the asset that collective countermeasures do not protect** is called a "**Control Gap**" (difference in controls)

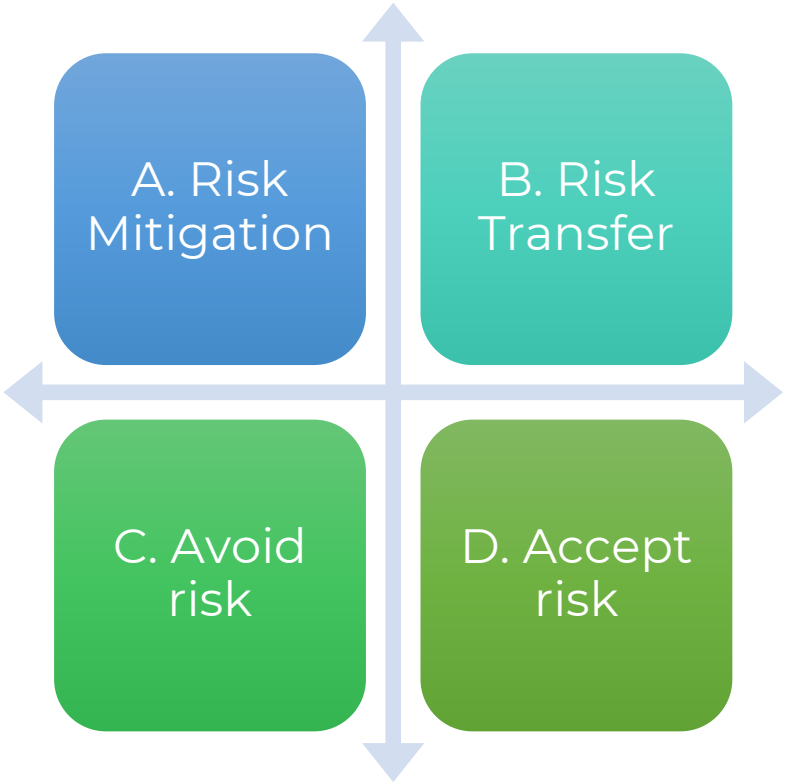
⇢Usually expressed as a percentage

⇢"Control Gap" is **directly related to the residual risk value**

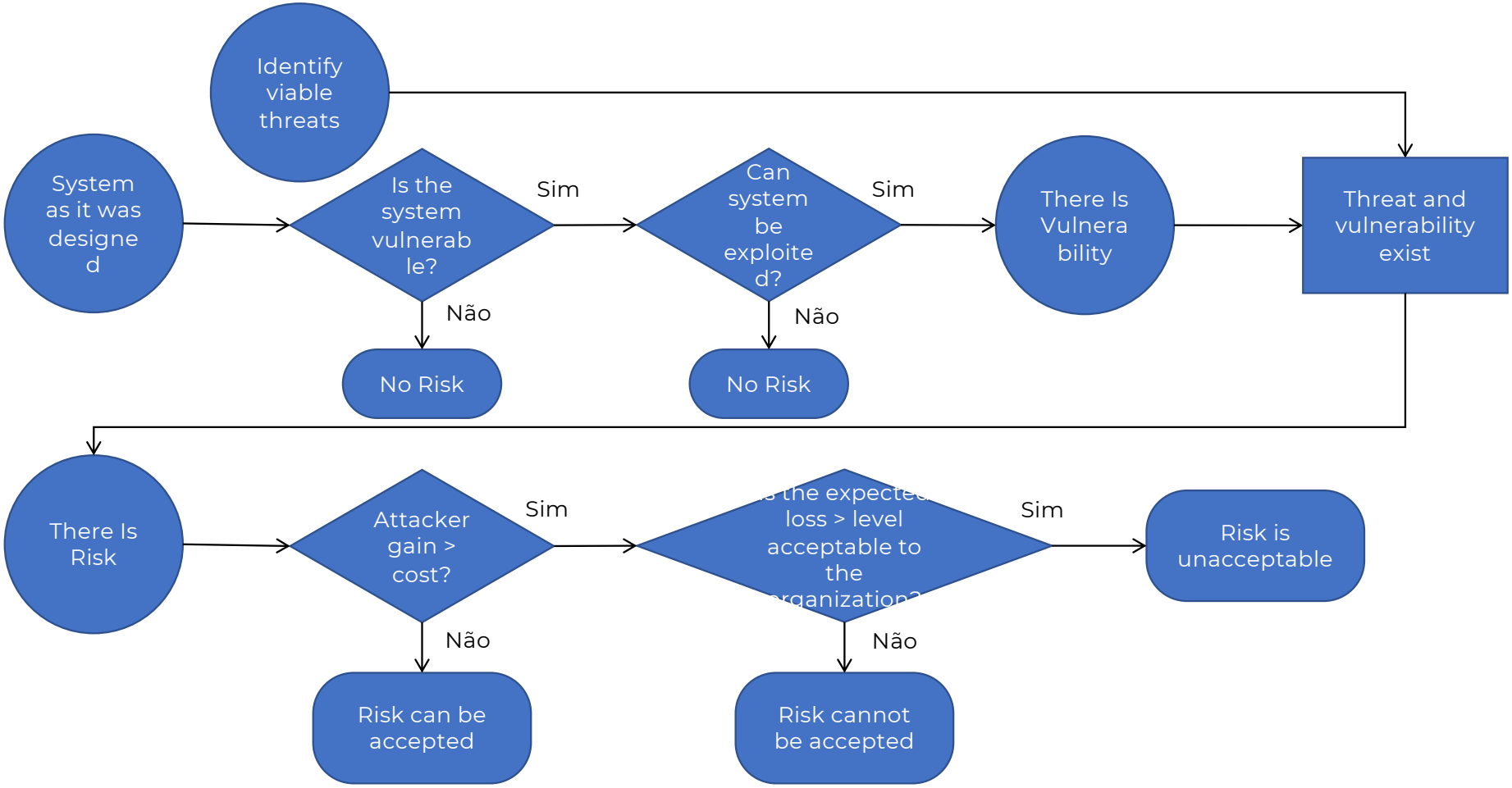
Example:
Asset Value x Control Gap = Residual Risk
$1,000,000 x 6% = $60,000

NIST SP 800-37 | (5) Dealing with risk

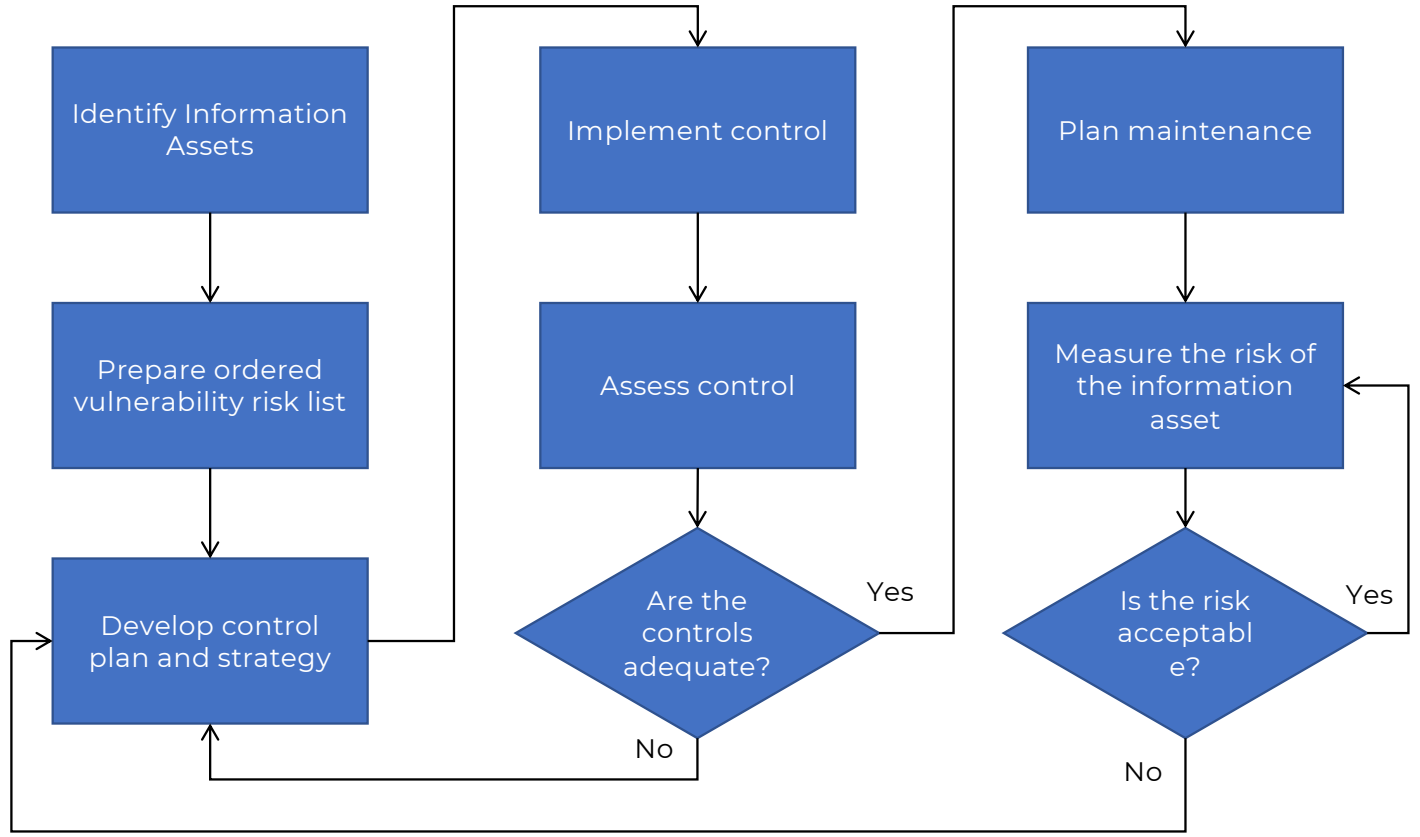
- Management will approve combinations of items A, B and C … until the D is acceptable (or the budget runs out)



Select Risk Control Strategy



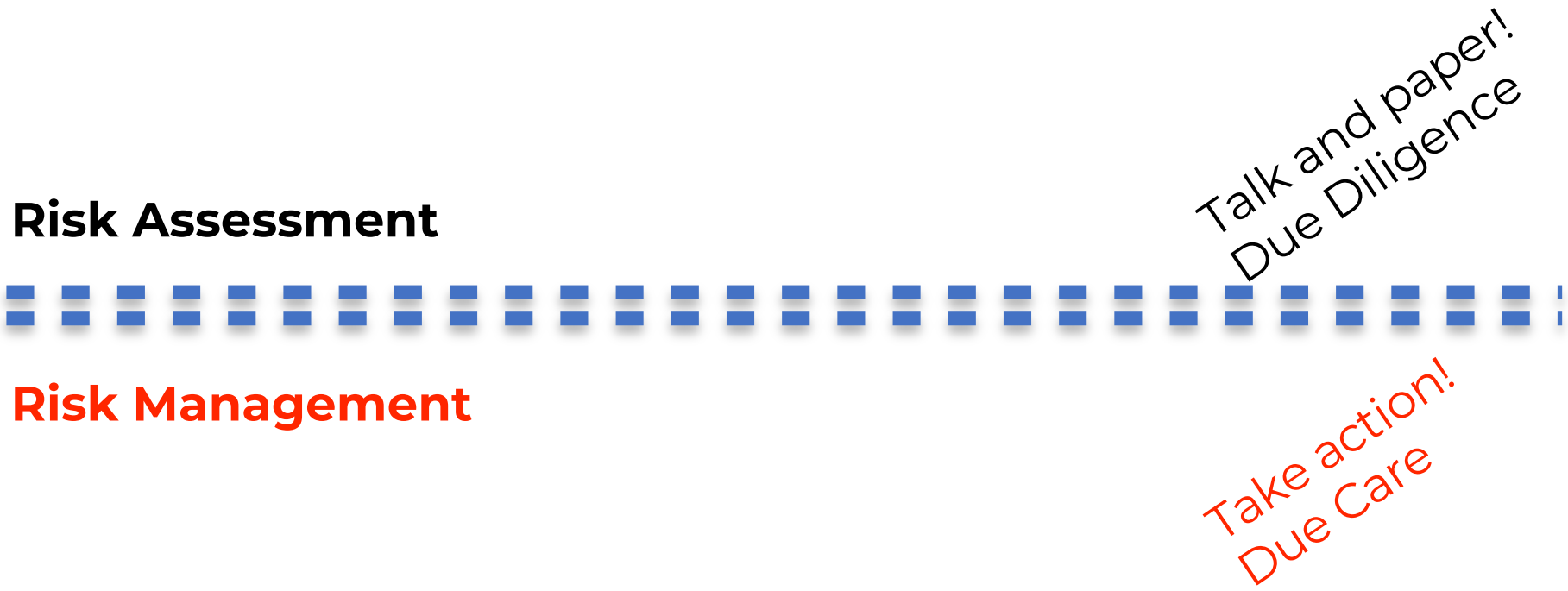
Risk Control Cycle



NIST SP 800-37 | (6) and (7) Final parts

- (6) **Prepare** the **report** - a summary of the inventory of assets, value of assets, threats, and expected losses (ALE), together with the list of proposed cost-justified countermeasures
- (7) **Presentation to management** for **selection** and **approval** of **countermeasures**

Risk Management Project - (6) and (7) Final Parts



Risk Management

- **Countermeasure approvals** serve to **identify** the **real risk tolerance**
  - When management no longer approves countermeasures, the residual risk that is left is the definition of the tolerance of risk management
- **Prudently implement controls**
- Following the approval of countermeasures by the management
  - it serves to define the security program, budget, and plan for next year

Risk Management

- **Approved** and selected **countermeasures identify**:
  - the hardware and software to purchase
  - new people to hire or train
  - the policy documents to be produced or updated
  - the new processes and procedures to be implemented
  - training programs to be offered to employees, administrators, managers, etc.

Risk Management Framework - NIST SP 800-37

I. Categorize - Risk Assessment

II. Select controls - Management approval

III. Implement controls

IV. Assess controls

V. Authorize systems

VI. Monitor, Detect, Report, Remedy

VII. Repeat

All talk and paper!

Take action.
It becomes part of a continued and routine security posture of the organization.

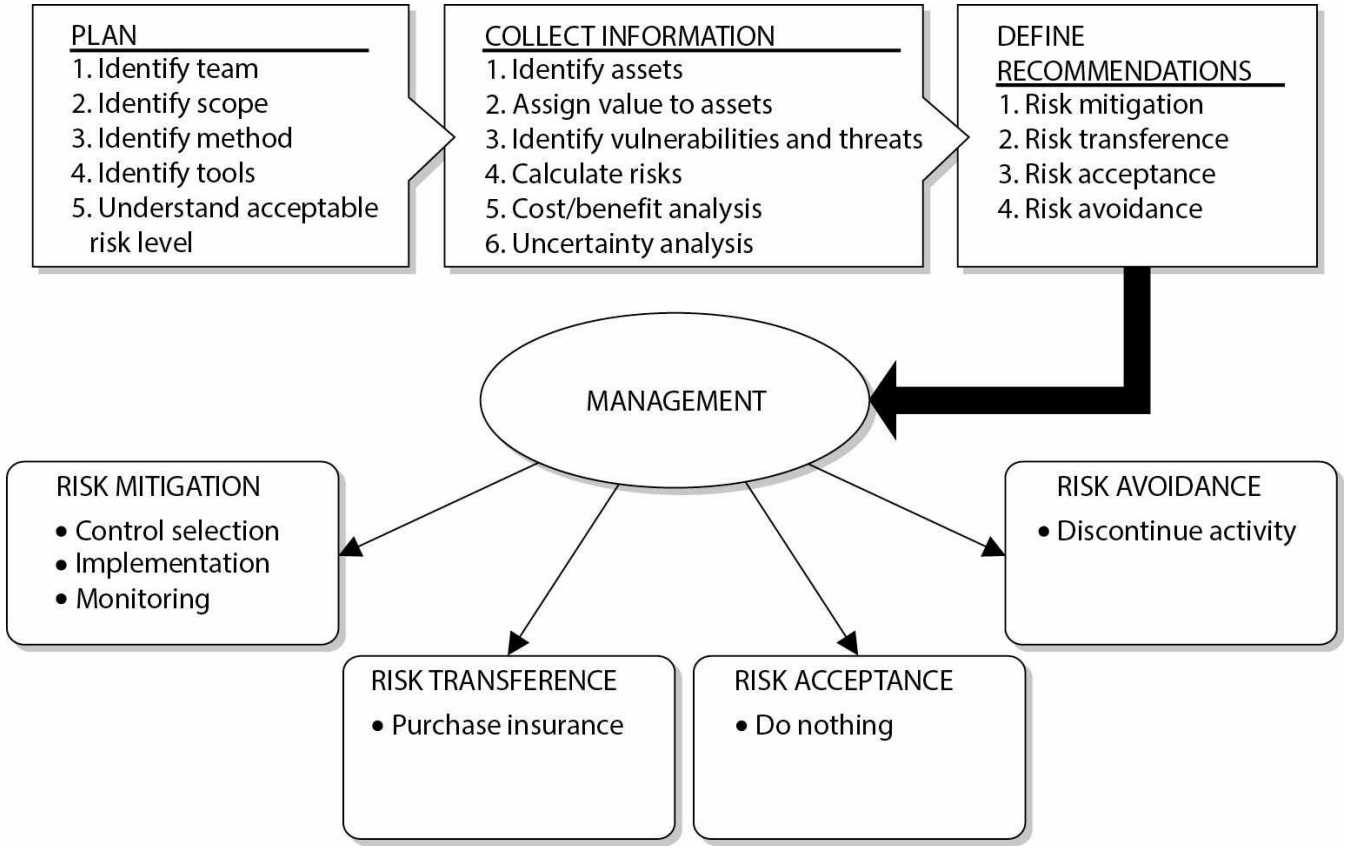
Risk Management Framework - NIST SP 800-37

Gestão do Risco

- III. Implement controls
  - Acquire HW, SW, hire new staff, update policies, train employees, etc., for each of the management approvals
  - Do not go into production with these controls - yet...
- IV. Assess controls
  - QA – set up controls and assess their effectiveness
    - Are they working the way they were supposed to, and offering the expected level of protection?
    - They introduce new vulnerabilities/threats/risks that must be prevented, mitigated?
- V. Authorize systems
  - Once you have set up security controls properly, check their effectiveness, and perform risk analysis and management of those controls, management will be prepared to use the controls in the information systems?
  - Management must accept this new collection of risks.
- VI. Monitor, Detect, Report, Remedy
  - Controls are now in production and dealing with data. They are now part of the organization's routine security posture.
  - Ensure their effectiveness and correct problems that may arise.
- VII. Repeat

Risk Assessment and Management

Summary



Risk Analysis - Threats

https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600
https://www.iso.org/standard/75281.html

- Threat identification:
- A total of 45 threats based on best practices and international standards, including:
  - 27 Threats with a greater focus on business continuity, taken from NFPA 1600; and
  - 18 More technology-oriented threats taken from ISO/IEC 27005.

Inherent Risk	Threats
High	Cybercrime Information Manipulation Emerging diseases that affect humans (e.g. Influenza A, Ebola) Public service power failure .... Eavesdropping - Information Listening Information leak Information from untrusted sources .... Viruses, Malware, Trojans
Reduced	Extreme temperatures (heat, cold) Tsunami Volcano Landslide Flood, flood Drought Fire (natural causes) .... Lightning Transport accident
Medium	Strike, labor dispute Violation of physical security Information theft Theft of equipment .... Hardware Handling Software Manipulation Abuse of access Improper access Concealment of actions

Risk Analysis - Threats

- Criteria for risk measurement

-

Vulnerability	Very High	High exposure and there is no response strategy.	4
	High	High exposure and there is only one partial response strategy.	3
	Average	High/moderate exposure, but a response strategy is in place.	2
	Low	Low exposure with or without response strategy.	1

Duration	Long	More than 1 week	3
	Intermediate	Up to 1 week	2
	Short	Up to 1 day	1

Notice	No	It is not possible to predict the threat and be informed in advance of the event of the same	2
	Yes	It is possible to predict the threat and be informed in advance of the event of the same	1

Risk Analysis - Threats

Criteria for risk measurement

Impact Score (V+D+AP)	High	The occurrence of this threat may represent a serious anomaly in the organization's overall operation significantly compromising its operation.	8 – 9
	Medium	The occurrence of this threat may represent an anomaly located in the organization, and the impact is restricted to a critical process/resource group.	6 – 7
	Low	The occurrence of this threat represents specific anomalies in the organization	3 – 5

Probability of occurrence	High	There is knowledge or registration of more than 1 annual event with these characteristics	3
	Average	There is knowledge or registration of at least 1 event with these characteristics	2
	Low	There is no knowledge or record of an event occurring with these characteristics	1

Mitigation Controls	Efficient	All or almost all control strategies are implemented. Few opportunities for improvement.	3
	Acceptable	Some mitigation strategies are implemented. Some opportunities for improvement.	2
	To improve	Lack/ few mitigation strategies implemented. Substantial improvement opportunities.	1

Risk Analysis - Threats

Nº	Risco	Risco Residual	Recomendação	Nível de controlo (após implementação)	Novo Risco Residual
1	Falha de energia do serviço público	Elevado	De forma a assegurar o funcionamento contínuo dos sistemas que suportam o [redacted] deve considerar: • Proceder às alterações necessárias para que o gerador existente passe a fornecer energia ao *Datacenter* de forma automatizada, i.e. sem intervenção humana para a comutação.	3	Baixo
2	Interrupções nos sistemas de comunicação com o exterior	Elevado	De forma a assegurar o funcionamento contínuo dos sistemas que suportam o [redacted] deve considerar: • A contratualização de um serviço de internet alternativo com comutação totalmente automática em caso de falha de uma ligação.	3	Baixo
3	Fuga de informação	Elevado	• Revisão periódica de acessos a todos os sistemas e rede [redacted]; • Sensibilização dos colaboradores do IT para a detecção de situações anómalas; • Formação dos colaboradores [redacted] e utilizadores finais do [redacted] relativamente a temáticas relacionadas com a Segurança da Informação; e • Restrição na utilização de meios de armazenamento amovíveis.	2	Médio

Risk Analysis - Threats

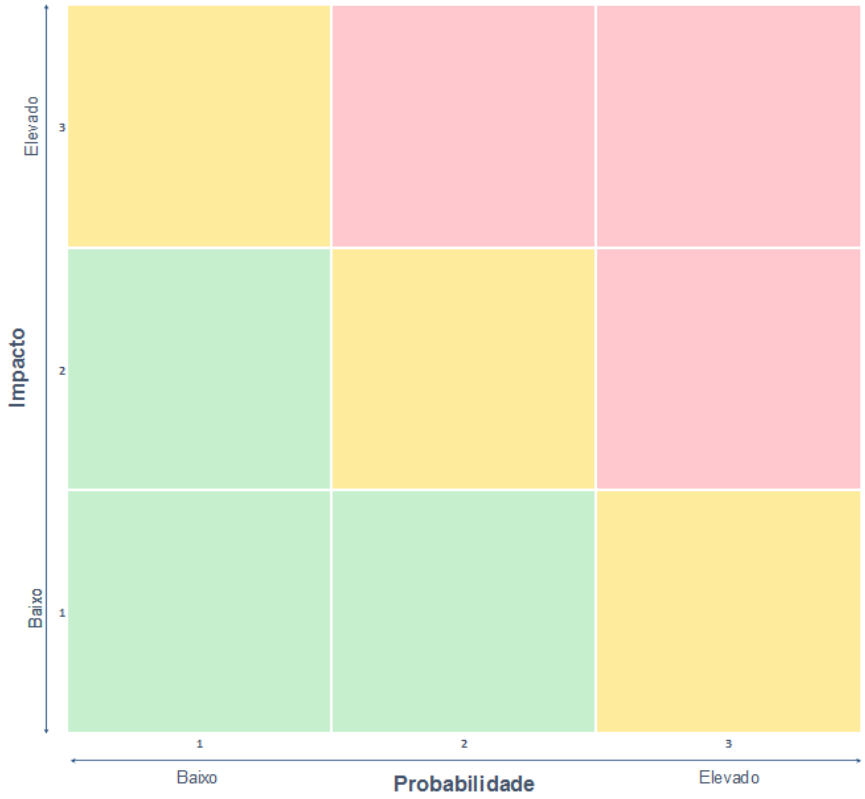
Risk Management

AMEACA.17	**Falha de energia do serviço público**		
Avaliação do Impacto	- Todos os sistemas de TI [redacted] dependem de energia eléctrica. Esta situação tem impacto directo em todos os processos, internos e externos; e - A ocorrência deste tipo de ameaças não é previsível e a sua duração não deverá ser longa	**Vulnerabilidade**	**4**
		Aviso prévio	**2**
		Duração	**1**
		Valor do impacto	**7**
Probabilidade	- Embora não seja provável, o abastecimento de energia pode ser cortado por factores alheios [redacted]. Adicionalmente, foi reportado que esta situação já aconteceu, pelo que a probabilidade é média.	**Valor da Probabilidade**	**2**
Risco Inerente			**Elevado**
Avaliação dos controlos	- [redacted] possui alguns controlos implementados de forma a suprimir as suas necessidades energéticas no caso de falha da rede energética contratada. Existe 1 UPS com capacidade de suportar os sistemas durante aproximadamente 4horas. Mas no caso de a duração ser superior a 4 horas: - Não existe um sistema que suporte o DC [redacted]; - O gerador existente não alimenta o UPS que suporta o DC; e - Em caso de falha energética os AC não funcionam.	**Valor dos controlos**	**1**
Risco residual			**Elevado**

Risk ID	Asset Identification	Threat to the Asset	Threat Likelihood Estimate	Consequence, if the threat is realised	Resultant Risk Level	Required Threat Likelihood	Required Consequence, if threat is realised	Required Risk	Countermeasure(s) Priority	Countermeasure(s) Recommendation based on AS/NZS 7799.2
1	XYZ Association's Internet services -- Availability	Critical network device (e.g. router, firewall, etc.) failure	Low	Significant	Medium	Very Low	Significant	Low	1	A.7.2.1 Equipment siting and protection A.7.2.2 Power supplies A.7.2.4 Equipment maintenance A.8.1.3 Incident management procedures A.8.2.1 Capacity planning A.8.2.2 System acceptance A.8.5.1 Network controls A.11.1.1 Business continuity management process A.11.1.2 Business continuity and impact analysis A.11.1.3 Writing and implementing continuity plans A.11.1.4 Business continuity planning framework A.11.1.5 Testing, maintaining and re-assessing business continuity plans
2	XYZ Association's Internet services -- Availability	Denial of Service attack from Internet	Very High	Significant	High	Very Low	Minor	Low	2	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use A.9.7.3 Clock synchronization A.11.1.1 Business continuity management process A.11.1.2 Business continuity and impact analysis A.11.1.3 Writing and implementing continuity plans A.11.1.4 Business continuity planning framework A.11.1.5 Testing, maintaining and re-assessing business continuity plans
3	XYZ Association's Data - Integrity	Compromised network security by hackers from the Internet	Low	Serious	High	Negligible	Damaging	Nil	3	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use

Risk Analysis - Threats

Risk Management



2023 | 2024

Network and Information Systems Security

Information Security Risk Management

Carlos Serrão
carlos.serrao@iscte-iul.pt

iscte INSTITUTO UNIVERSITÁRIO DE LISBOA