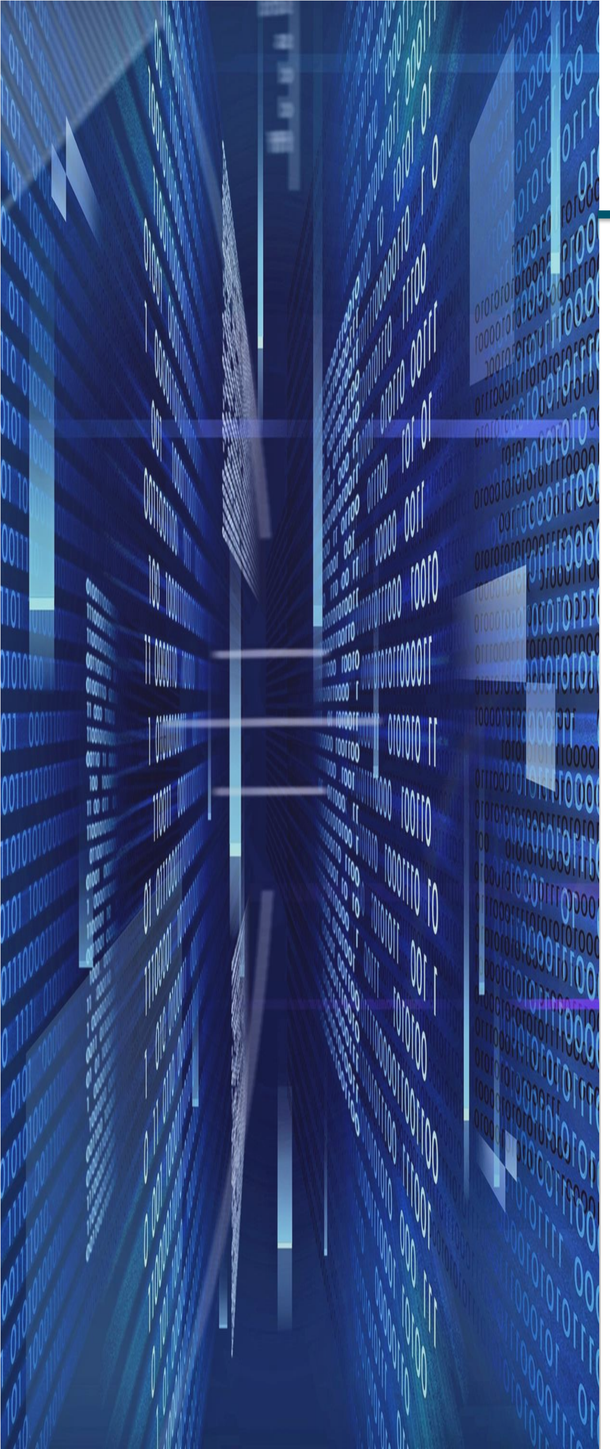


Cyber Risk Management

Prof. Federica Paci

Today’s lecture

- Why Risk Management?
- What is Risk Management?
- How to conduct Risk Assessment?
- NIST 800-30 standard

Learning Outcomes

At the end of this lecture you should be able to:

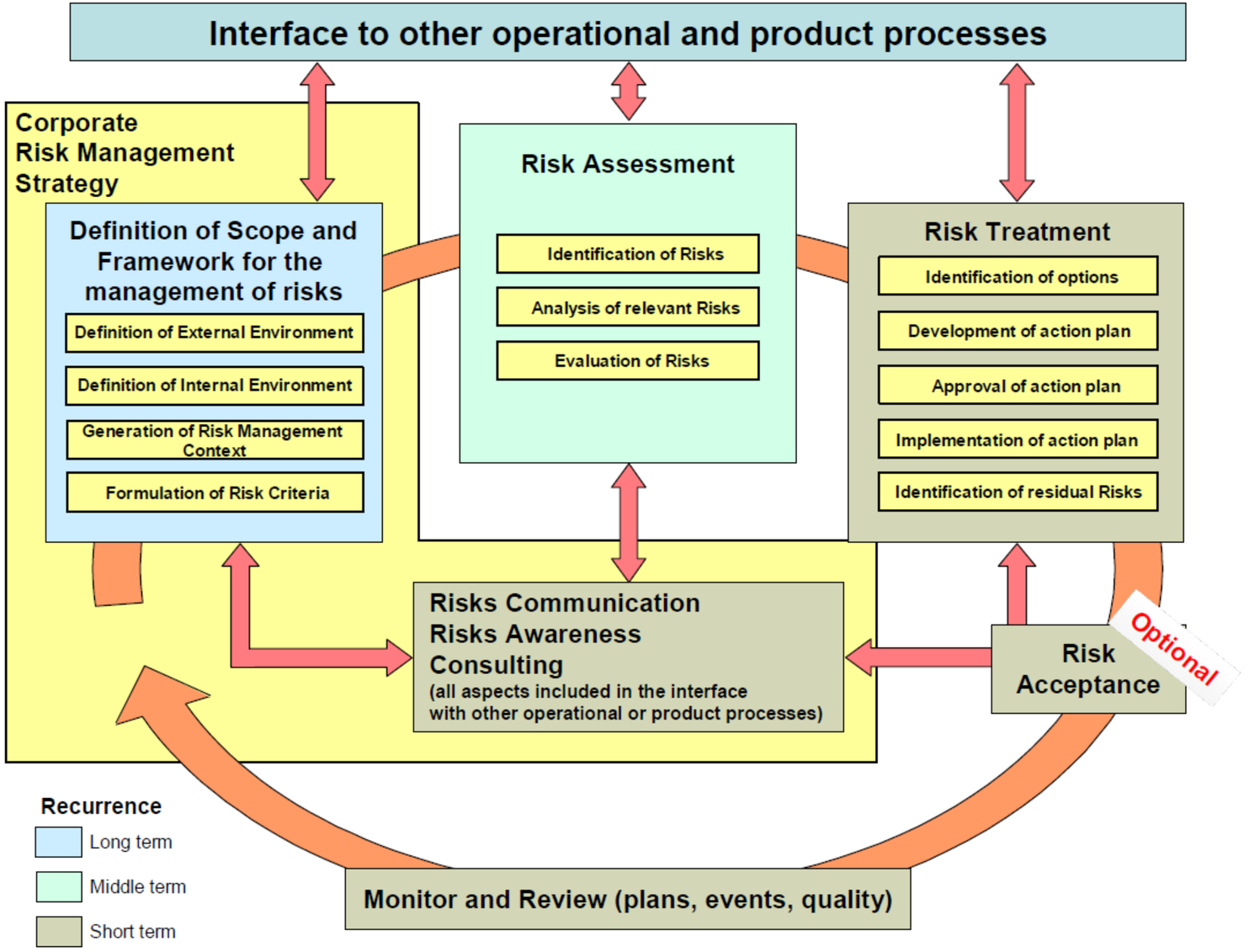
- Define what cyber risk is
- Explain how cyber risks are identified and assessed
- Explain how to reduce cyber risks

Why Risk Management?

- Organizations have to decide around how much time and money to spend protecting their technology and services
- One of the main goals of risk management is to *inform* and *improve* these decisions
- It is an explicit requirement of the most important standards and regulations:
  - ISO 27001 (ISMS)
  - GDPR
  - PCI DSS
  - DORA
  - 10 Steps to Cyber Security

un piano di gestione del rischio mi permette di capire dove andare ad investire e quanto farlo

What is Risk Management?



Risk Management - Step 1: Frame Risk

- Establish the context in which the organization operates
  - organization's mission, purpose, goals, and priorities
  - the key and critical areas of the organization's business
  - Identify who is responsible and accountable for making cyber security risk management decisions
  - legal, statutory, regulatory, compliance or contractual requirements that the organization has to meet
  - Identify the acceptable risks

Risk Management - Step 2: Assess Risk

The purpose is to identify:

- **threats** to organizations (i.e., operations, assets, or individuals)
- **vulnerabilities** internal and external to organizations;15
- the **adverse impact** that may occur given the potential threats exploiting vulnerabilities
- the **likelihood** that harm will occur

Risk Maangement – Step 3 – Responde to Risk

- This step involves the analysis and prioritisation of risks and making decisions about how you are going manage them
- Four possible strategies are available:
  - Accept the risk
  - Avoid the risk
  - Transfer the risk
  - Treat the risk

Decidere come gestire il rischio

evitare

trasferire

trattare

Risk Maangement – Step 3 – Responde to Risk

- **Procedural security:** security controls that seek to mitigate or treat identified risks by way of policies, procedures, processes, or guidelines.
- **Physical security:** controls that seek to mitigate or treat identified risks through the physical protection of assets such as buildings, facilities, IT equipment, personnel etc.
- **Personnel security:** measures put in place to mitigate or treat risks from authorised users of cyber systems e.g vetting, training and threat awareness campaigns
- **Technical security:** measures built into the cyber system to mitigate or treat identified risks e.g firewalls, secure configuration, access controls, anti-malware software, and software updates and patching

Risk Management – Step 4 – Communicate the Risk

- Communicate the findings and recommendations to the appropriate decision maker or group of decision makers within the organization.
- The communications need to be meaningful, and be appropriate to the audience in terms of the level of detail and format used

Risk Management – Step 5- Implement and assure risk

- Implement the recommended security controls maintain confidence that the controls and measures that are applied work, and continue to work, effectively and as expected
- Train people that use, manage and maintain the systems and services by requiring that they have the training and skills they need to do their jobs securely
- Make sure that the technology and processes the organization uses have been designed with security in mind.
- Carry out security testing on services and devices prior to their deployment and whilst in operation, and by monitoring and auditing how they are used

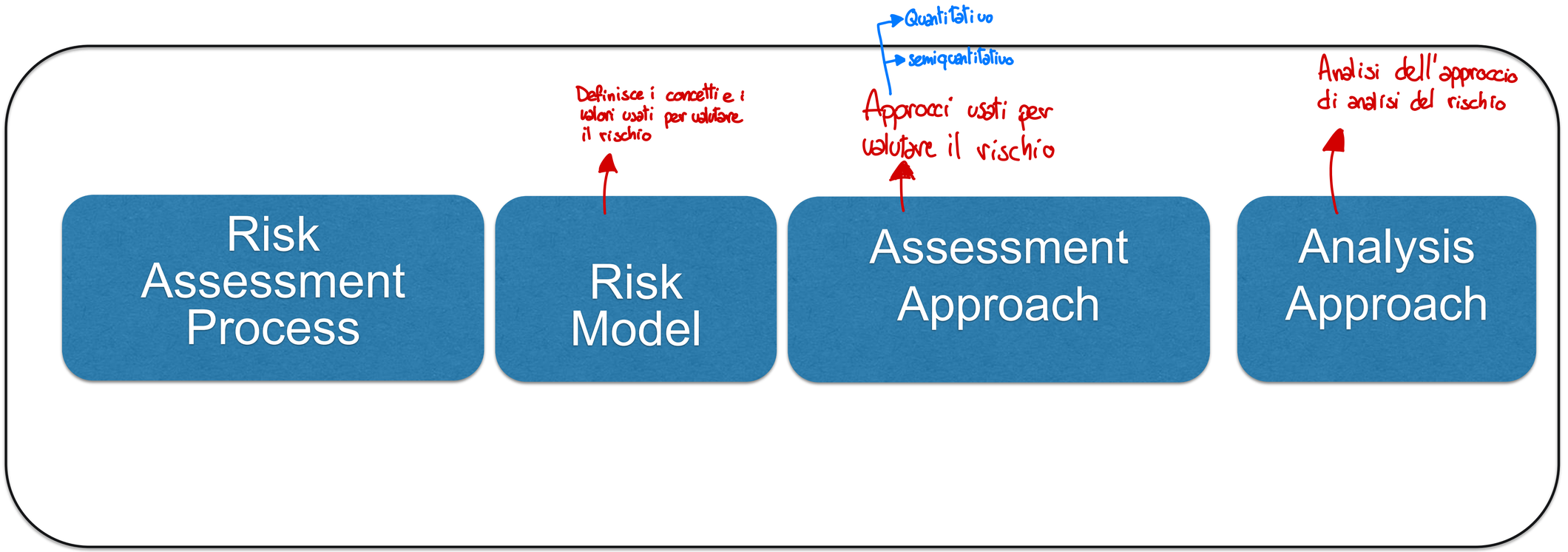
Risk Management – Step 4 – Monitor Risk

- Continually confirm that the controls in place are appropriate and proportionate in terms of managing cyber security risk
- Develop metrics and performance indicators to measure the effectiveness of controls
- Revisit risk assessments and analysis when something significant changes
  - New vulnerabilities
  - New technologies

Other risk standards and frameworks

- Risk Management
  - ISO/IEC IS 27005
  - ISO 31000
  - NIST 800-37
- Risk Assessment
  - EBIOS
  - CRAMM
  - MAGERIT
  - IT-Grundschutz
  - OCTAVE
  - CORAS
  - NIST 800-30

Risk Assessment Methodology Components



Risk Model

Non c'è una definizione effettiva, si intende per rischio un qualcosa che può avere un impatto negativo sul sistema

Assets

Vulnerabilities

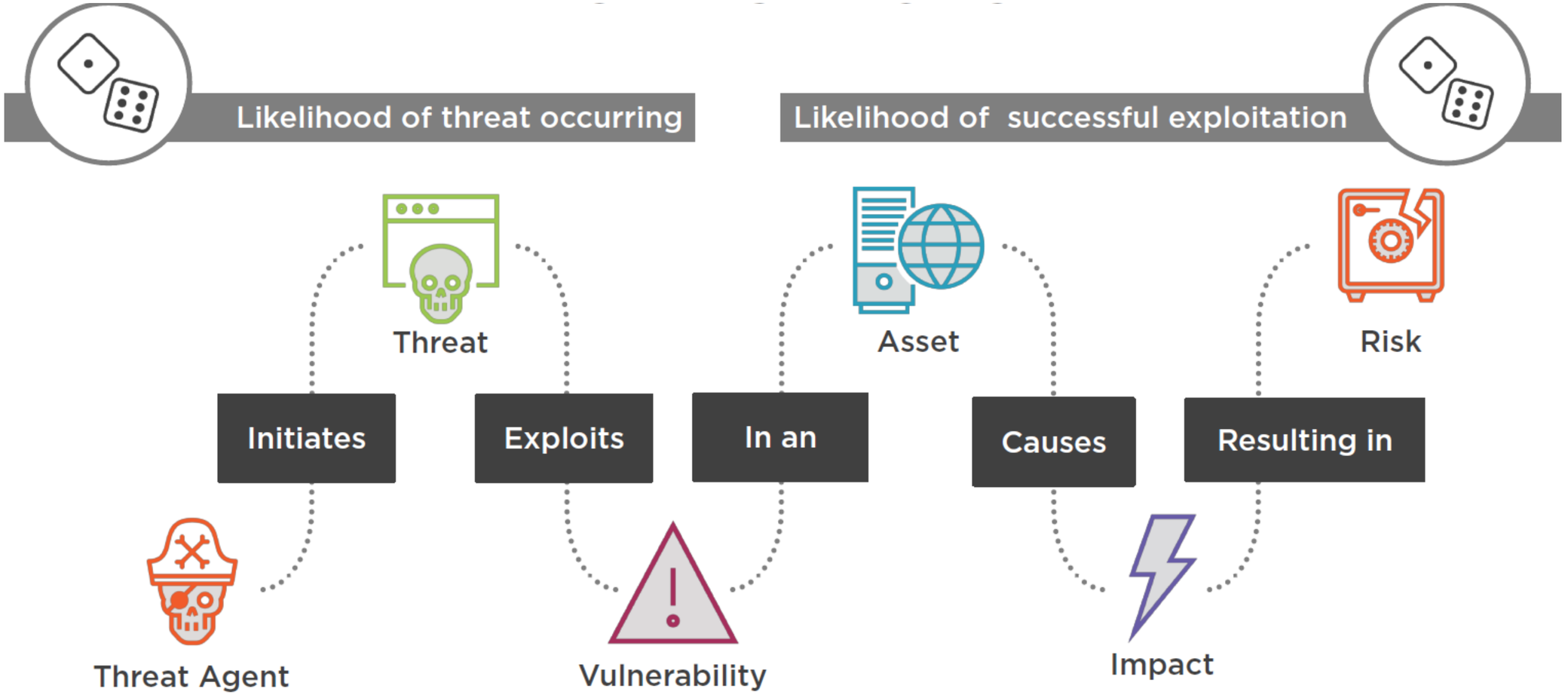
Threat Actors

Threats

Likelihood

Impact

Risk Model


Likelihood of threat occurring
Likelihood of successful exploitation
Threat
Asset
Risk
Initiates
Exploits
In an
Causes
Resulting in
Threat Agent
Vulnerability
Impact

OWASP Risk Rating Methodology

- Provides a set of factors to estimate the likelihood and impact
- The likelihood is estimated based on two sets of factors
  - Threat Agent factors
  - Vulnerability factors
- The impact is estimated based on
  - Technical impact factors
  - Business impact factors

Threat Agent factors

- **Skill Level** - How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)

- **Motive** - How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

- **Opportunity** - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

- **Size** - How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Vulnerability Factors

- **Ease of Discovery** - How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

- **Ease of Exploit** - How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

- **Awareness** - How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

- **Intrusion Detection** - How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

Technical impact factors

- **Loss of Confidentiality** - How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

- Loss of Integrity - How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

- Loss of Availability - How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)

- **Loss of Accountability** - Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

Business impact factors

- **Financial damage** - How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)

- **Reputation damage** - Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)

- **Non-compliance** - How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)

- **Privacy violation** - How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

Determining the severity of risk

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Assessing likelihood

Valutazione della probabilità

'"Threat agent factors"'					'"Vulnerability factors"'			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Assessing impact

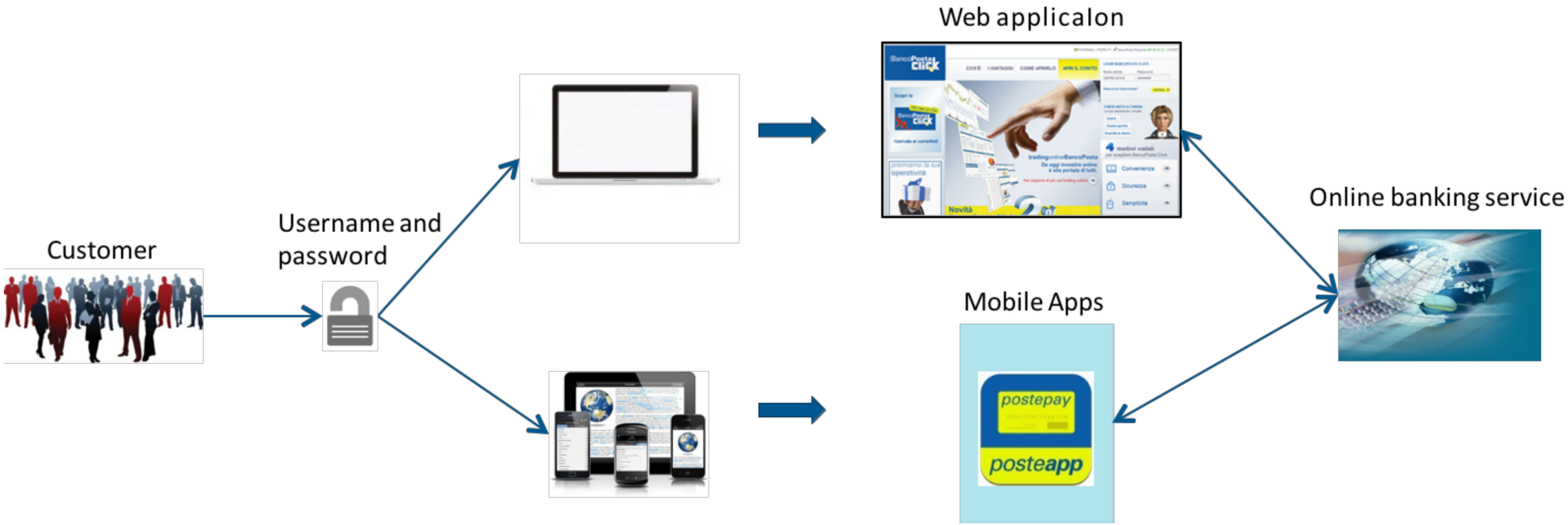
Valutazione dell'impatto

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8		1	2	1	5
Overall technical impact=7.25 (HIGH)					Overall business impact=2.25 (LOW)			

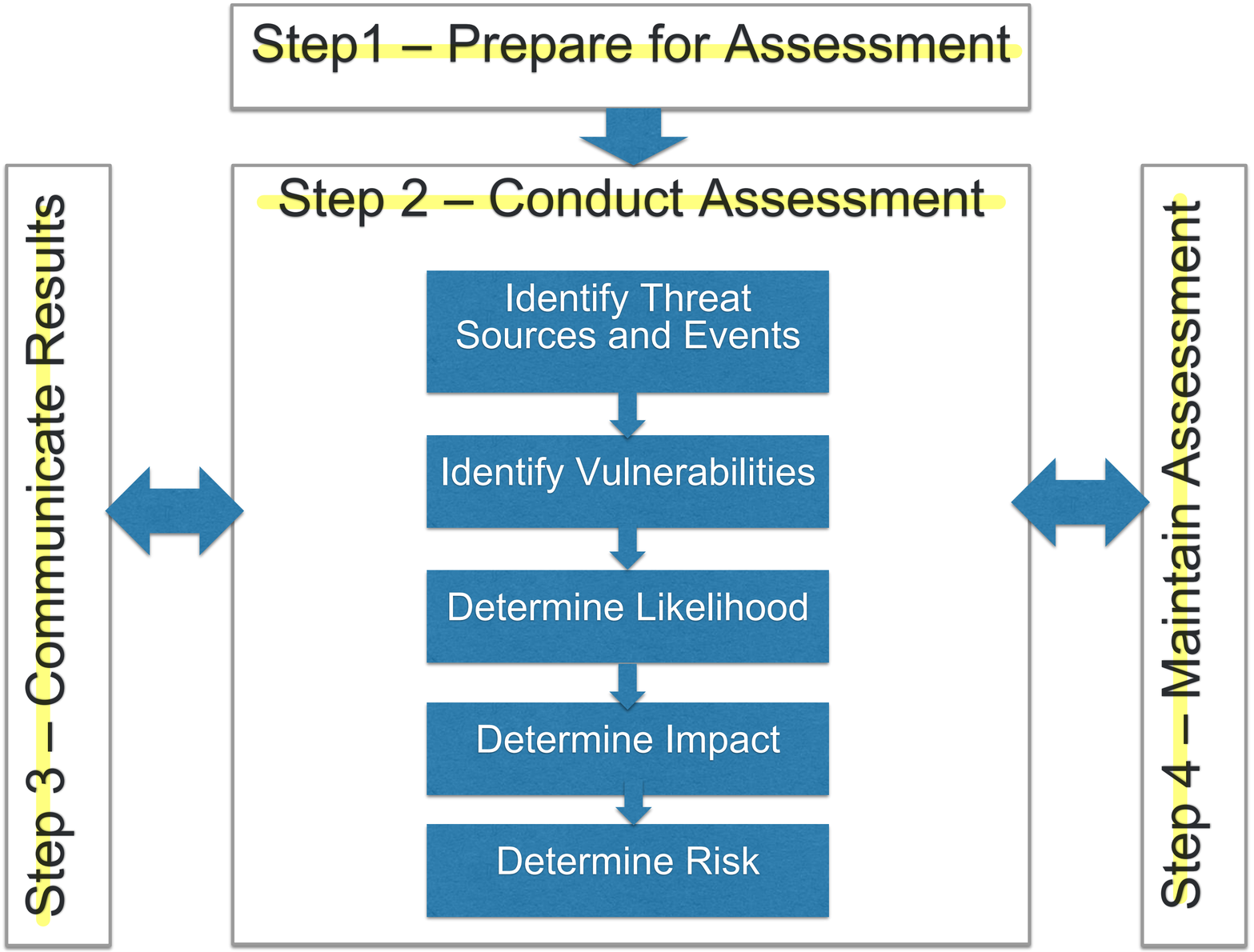
Estimating severity

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood probabilità che avvenga			

Online Banking Scenario



Risk Assessment with NIST 800-30



Step 1 – Prepare for the Risk Assessment

Definite le parti dell'azienda coinvolte ed interessate

- **Objective**: Establish a context for the risk assessment
- Includes the following tasks:
  - Identify the **purpose** (scopo) of the assessment
  - Identify the **scope** (ambito) of the assessment
  - Identify the **assumptions** (assunzioni) and **constraints** (vincoli) associated with the assessment
  - Identify the **risk model, assessment approach,** and **analysis approach** to be used in the risk assessment

Step 2 – Conduct Risk Assessment

- **Objective:** Produce a list of cyber security risks
- It consists of the following tasks:
  - Identify **threat sources**
  - Identify **threat events**
  - Identify **vulnerabilities**
  - Determine **likelihood**
  - Determine **impact**
  - Determine **risks**

Step 2-1 Identify Threat Sources

Objective: Identify threat sources of concern

Type of threat source	Descriptions	Characteristics
ADVERSARIAL Outsider Insider Competitor Supplier Nation State	Individuals, groups, organizations, or states that seek to exploit the organization' dependence on cyber resources	Capability, Intent, Targeting
ACCIDENTAL User Privileged User	Erroneous actions taken by individuals	Range of effects
STRUCTURAL IT Equipment Environmental Controls Software	Failure of equipment, environmental controls, or software	Range of effects
ENVIRONMENTAL Natural or Man-Made Disaster Infrastructure Failure	Natural disasters and failures of critical infrastructures on which the organization depends	Range of effects

Step 2-1 Identify Threat Sources

Objective: Identify threat sources of concern

Attaccanti	capability	motivazione	Attacchi	vulnerabilità
Cybercriminali	elevate tecnical skills	profitto economico	ransomware	remote code execution
Attivisti	elevate tecnical skills	messaggio politico	DDOS	no load balancing

For adversarial threat sources ask yourself

- *How technically skilled is the threat source?*
- *How motivated is the threat source to find and exploit a vulnerability?*
- *What organizational resources the threat source is targeting?*

- For non adversarial threats
  - *What is the effect of the threat source?*

	L1	LM	Probabilità L	Impatto	RISK
RAMSOMWARE	HIGH	HIGH	HIGH	HIGH	→ HIGH
DDOS	MODERATE	LOW	MODERATE	LOW	→ LOW

Step 2-1 Identify Threat Sources

What are possible adversarial threat sources for the Poste Italiane use case?

What are possible non adversarial threat sources for the Poste Italiane use case?

Time: 5 min

Step 2-2 Identify Threat Events

Objective: Identify threat event

Rce → remote code execution
DDOS → chiedendo riscatto
↳ meitre attack matrix

How what may happen? What does it harm?

What kind of threat events can be initiate by the threat sources identified at step 2-1?

Time: 5 minute

Step 2-3 Identify Vulnerabilities

Objective: assess the vulnerabilities that a threat event can exploit and their severity

What can make the threat events possible?

What can make the threat events identified at step 2-2 possible?

In presenza di un attacco DDOS
le vulnerabilità possono essere:

mancanza di un sistema di
loadbalancing

Time: 5 minutes

Step 2-4 Determine The Likelihood

Objective: Determine the likelihood of threat event

- To estimate the likelihood of threat event consider the capability, intent and targeting and how difficult it is to exploit the vulnerability

capacità intento

obbiettivo

- probabilità avvenimento attacco
- Capability
- Motivation
- Obbiettivo
- probabilità efficacia attacco
- probabilità di mancanza di sistemi in grado di rilevare e contrastare l'attacco

Step 2-4 Determine The Likelihood (Adversarial)

attaccanti

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Step 2-4 Determine The Likelihood (Non-adversarial)

senza attaccanti, perciò ci riferiamo ad incidenti

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Step 2-4 – Determine the Likelihood of resulting in adverse impact

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

effetto avverso

Step 2-4 – Determine the Overall Likelihood

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Step 2-4 Determine Likelihood

What is the likelihood of the following threat event identified at Step 2-2?

Time: 5 minutes

Step 2-5 Determine Impact

danno

Objective: Identify the potential harm caused to organizational assets

Type of Impact	Impact
Harm to Operations	• Inability to perform current business functions • Non compliance • Direct Financial Costs • Damage to image of reputation
Harm to Assets	• Damage to or loss of physical facilities • Damage to or loss of information systems or networks • Damage to or loss of equipment • Damage to or loss of information assets • Loss of intellectual properties
Harm to Individuals	• Loss of life • Identity Theft • Loss of PII • Damage to the reputation
Harm to Other Organizations	• Non compliance • Direct Financial Costs • Damage to image of reputation
Harm to the Nation	• Damage to a critical infrastructure

Step 2-5 Determine Impact

Impact	*Description*
Very High	Threat event could have **multiple severe or catastrophic** adverse effects on organizational operations, assets, individuals, other organizations or the Nation
High	Threat event could have **severe or catastrophic adverse effects** on organizational operations, assets, individuals, other organizations or the Nation
Moderate	Threat event could have **serious effects** on organizational operations, assets, individuals, other organizations or the Nation
Low	Threat event could have **limited effects** on organizational operations, assets, individuals, other organizations or the Nation
Very Low	Threat event could have **negligible** on organizational operations, assets, individuals, other organizations or the Nation

What is the impact of the threat events identified at Step 2-2?

Time: 5 minutes

Step 2-5 Determine Risk

Objective: Determine the level of risk as a combination of likelihood and impact

Adverse Impact	Likelihood of Threat Event				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Step 2-5 Determine Risk

What is the risk level of the threat events identified at Step 2-2?

Time: 5 minutes

Step 3 – Communicate Results

Objective: Communicate the assessment results and share risk related information

- Communicate the results to organization decision makers to support risk responses
- Share risk-related information produced during the risk assessment with appropriate organizational personal

Step 4 – Maintain the Risk Assessment

Objective: Maintain the knowledge of the risk organization incurs

Help organizations to:

- Determine the effectiveness of risk responses
- Identify risk-impacting changes to organizational assets
- Verify compliance

Summary

Risk Management is the process of prioritizing the identified risks in terms of likelihood of occurrence, then making coordinated efforts to minimize, monitor and control the impact of those risks.

Risk Assessment is the process of Identifying and assessing the level of risk faced by an organization

Resources

- NCSC Guidance on cyber risk management
  - https://www.ncsc.gov.uk/collection/risk-management/
- ENISA, Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools
- NIST 800-30 Guide for conducting risk assessment
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- OWASP Risk Rating Methodology
  - https://owasp.org/www-community/OWASP_Risk_Rating_Methodology