Co-funded by
the European Union

Course: Security Analysis and Risk Management

Project: Cyber Security 4 ALL

Chapter 3

Risk Analysis and Assessment Techniques

Overview

- Quantitative vs. qualitative risk analysis
- Risk matrices and risk assessment frameworks (NIST, ISO 27005)
- Case studies on risk analysis and assessment

Introduction

- As digital transformation accelerates across industries, the reliance on information and communication technology (ICT) and interconnected cyber systems has grown significantly.
- This increased dependence brings substantial benefits but also introduces complex security challenges and vulnerabilities.
- Risk analysis and assessment are essential practices designed to identify, evaluate, and manage these potential risks, ensuring that systems remain resilient and secure against threats.
- Cyber risk analysis involves evaluating potential vulnerabilities and threats to ICT assets, including hardware, software, networks, and data.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

Introduction

- By systematically assessing risks, organizations can prioritize actions that protect critical assets, maintain system integrity, and mitigate potential damage from cyber threats.
- Risk assessment in ICT and cyber systems includes both qualitative and quantitative approaches to evaluating the impact and likelihood of risks.
- Techniques such as threat modeling, failure mode analysis, and continuous monitoring are tailored specifically to address the unique characteristics of digital systems.
- Additionally, industry standards and frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001, provide structured guidance to help organizations build comprehensive risk management strategies.

Co-funded by
the European Union

Risk Analysis and Assessment Techniques

1. **Qualitative Risk Analysis**
2. **Quantitative Risk Analysis**
3. **Failure Mode and Effects Analysis (FMEA)**
4. **Bow-Tie Analysis**
5. **Root Cause Analysis (RCA)**
6. **SWOT Analysis**
7. **Scenario Analysis**
8. **Risk Register**

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Qualitative Risk Analysis

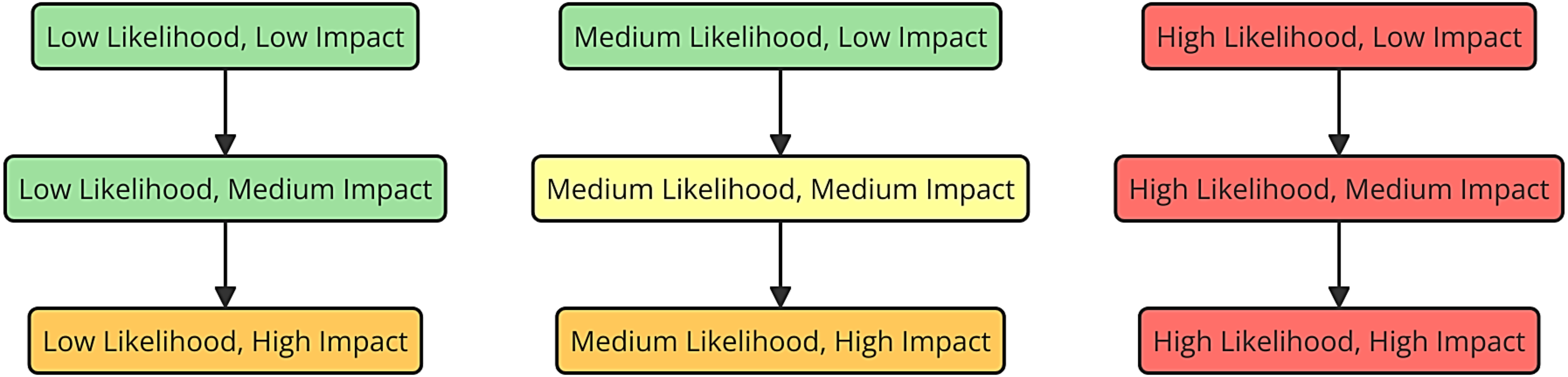
Focuses on subjective assessment of risk by evaluating impact and likelihood using descriptive terms (e.g., high, medium, low).

Techniques:

- **Risk Matrix:** A grid that plots the likelihood and impact of risks to prioritize them.
- **Expert Judgement:** Involves consulting experts to gather qualitative insights about potential risks.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

Custom Risk Matrix



Low Likelihood, Low Impact

Low Likelihood, Medium Impact

Low Likelihood, High Impact

Medium Likelihood, Low Impact

Medium Likelihood, Medium Impact

Medium Likelihood, High Impact

High Likelihood, Low Impact

High Likelihood, Medium Impact

High Likelihood, High Impact

Co-funded by
the European Union

Quantitative Risk Analysis

Uses numerical methods to evaluate risks, offering a more objective, data-driven approach.

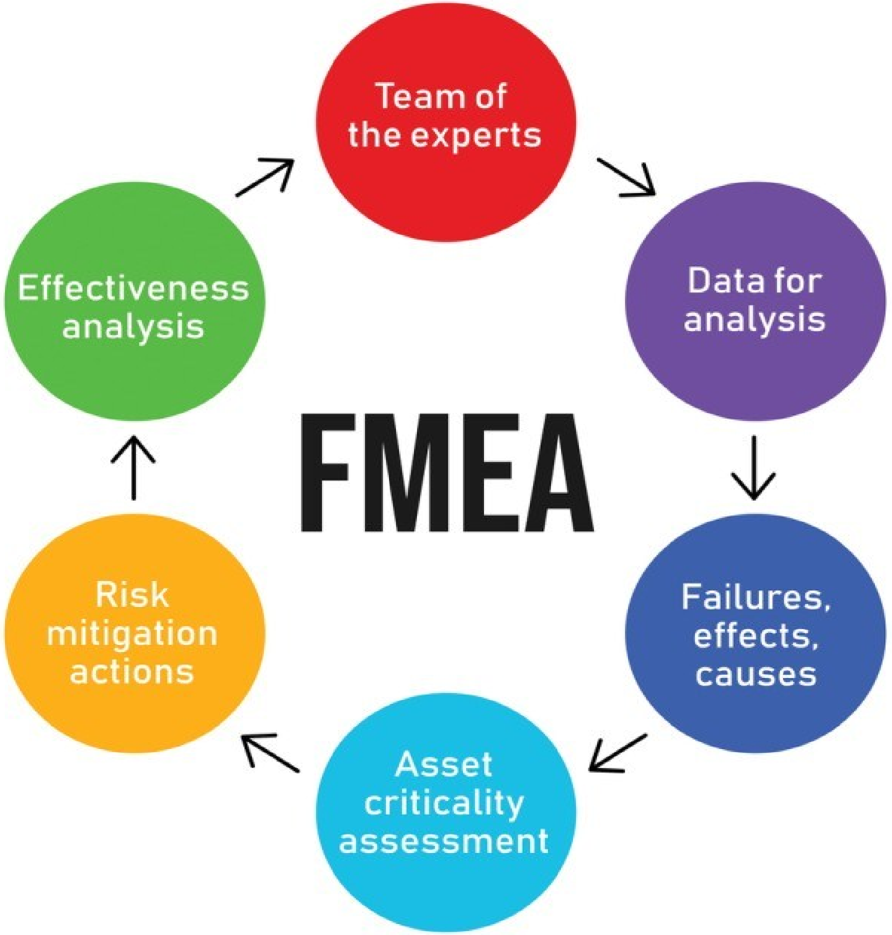
Techniques:

- **Monte Carlo Simulation**: Runs numerous simulations to predict risk outcomes based on variable data.
- **Expected Monetary Value (EMV)**: Calculates the financial impact of risks by multiplying likelihood with impact.
- **Sensitivity Analysis**: Assesses how changes in variables affect overall risk to identify key drivers.

Co-funded by
the European Union

Failure Mode and Effects Analysis (FMEA)

- Identifies points of potential failure in systems, assesses their likelihood and potential impact on ICT operations.
- Often used in IT hardware or software environments to preemptively address system weaknesses, minimize downtime, and ensure continuity.



CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Bow-Tie Analysis

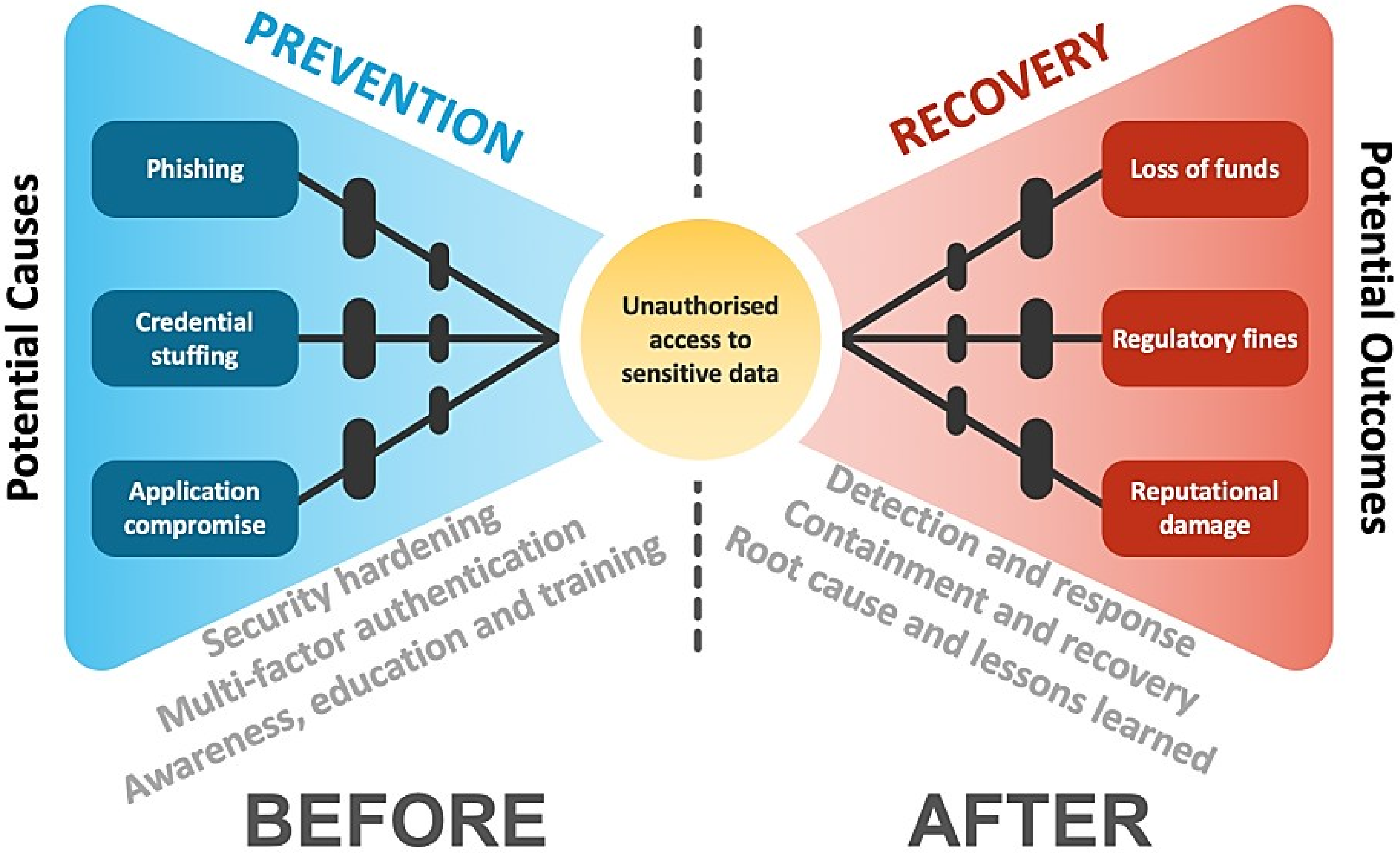
A Bow-Tie Analysis diagram for cyber systems risk analysis is a useful way to visualize threats, preventive controls, potential incidents, and recovery measures.

- Left Side (Threats): Identify and categorize cyber threats (e.g., phishing, malware, insider threat).
- Center (Top Event): Specify the primary event or incident (e.g., security breach or unauthorized access).
- Right Side (Consequences): Lay out possible consequences of the event (e.g., data loss, financial impact).
- Preventive Controls (Left Side): Outline the controls to prevent threats from leading to the top event (e.g., firewall, employee training).
- Recovery Controls (Right Side): List the recovery and response measures to mitigate consequences (e.g., incident response, data backups).

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Bow-Tie Analysis



Co-funded by
the European Union

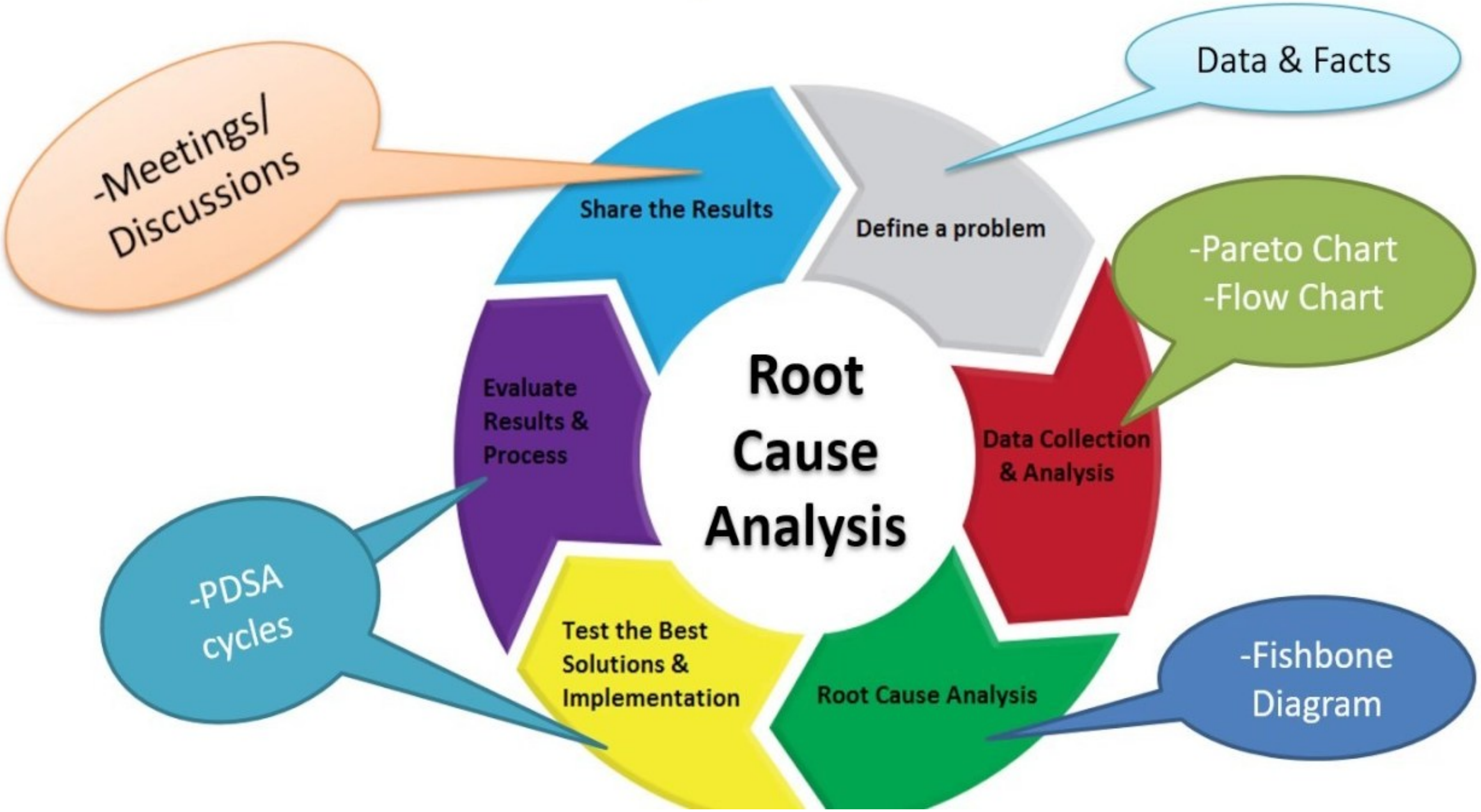
Root Cause Analysis (RCA)

Root Cause Analysis (RCA) focuses on cyber systems risk, the goal is to trace back from a cyber incident to its underlying causes.

- Incident/Event: Start with the primary incident in the center (e.g., data breach or ransomware attack).Direct
- Causes: Identify immediate reasons for the incident (e.g., unauthorized access, malware execution).
- Root Causes: Trace each direct cause back to underlying causes such as weak access controls, inadequate patching, or lack of employee training.
- Contributing Factors: Consider external or systemic factors that increase vulnerability, like outdated software or insufficient monitoring.

Co-funded by
the European Union

Root Cause Analysis (RCA)



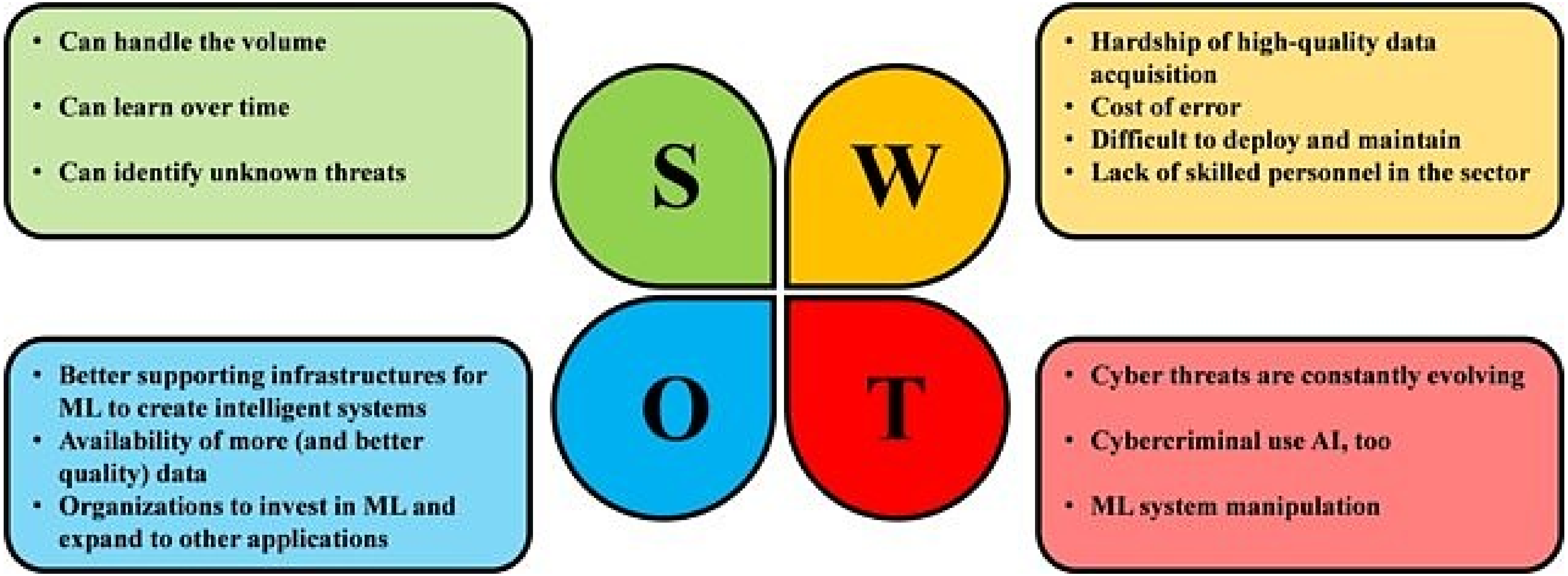
Co-funded by the European Union

Co-funded by the European Union

SWOT Analysis (Cyber Systems)

- **Strengths: Identify internal strengths (e.g., strong firewall systems, comprehensive employee training).**
- **Weaknesses: Highlight internal weaknesses (e.g., outdated software, lack of incident response planning).**
- **Opportunities: List potential opportunities to improve (e.g., new cybersecurity technology, regulatory incentives).**
- **Threats: Note external threats (e.g., increasing sophistication of cyber-attacks, regulatory fines).**

SWOT Analysis (Cyber Systems)



- Can handle the volume
- Can learn over time
- Can identify unknown threats

- Hardship of high-quality data acquisition
- Cost of error
- Difficult to deploy and maintain
- Lack of skilled personnel in the sector

- Better supporting infrastructures for ML to create intelligent systems
- Availability of more (and better quality) data
- Organizations to invest in ML and expand to other applications

- Cyber threats are constantly evolving
- Cybercriminal use AI, too
- ML system manipulation

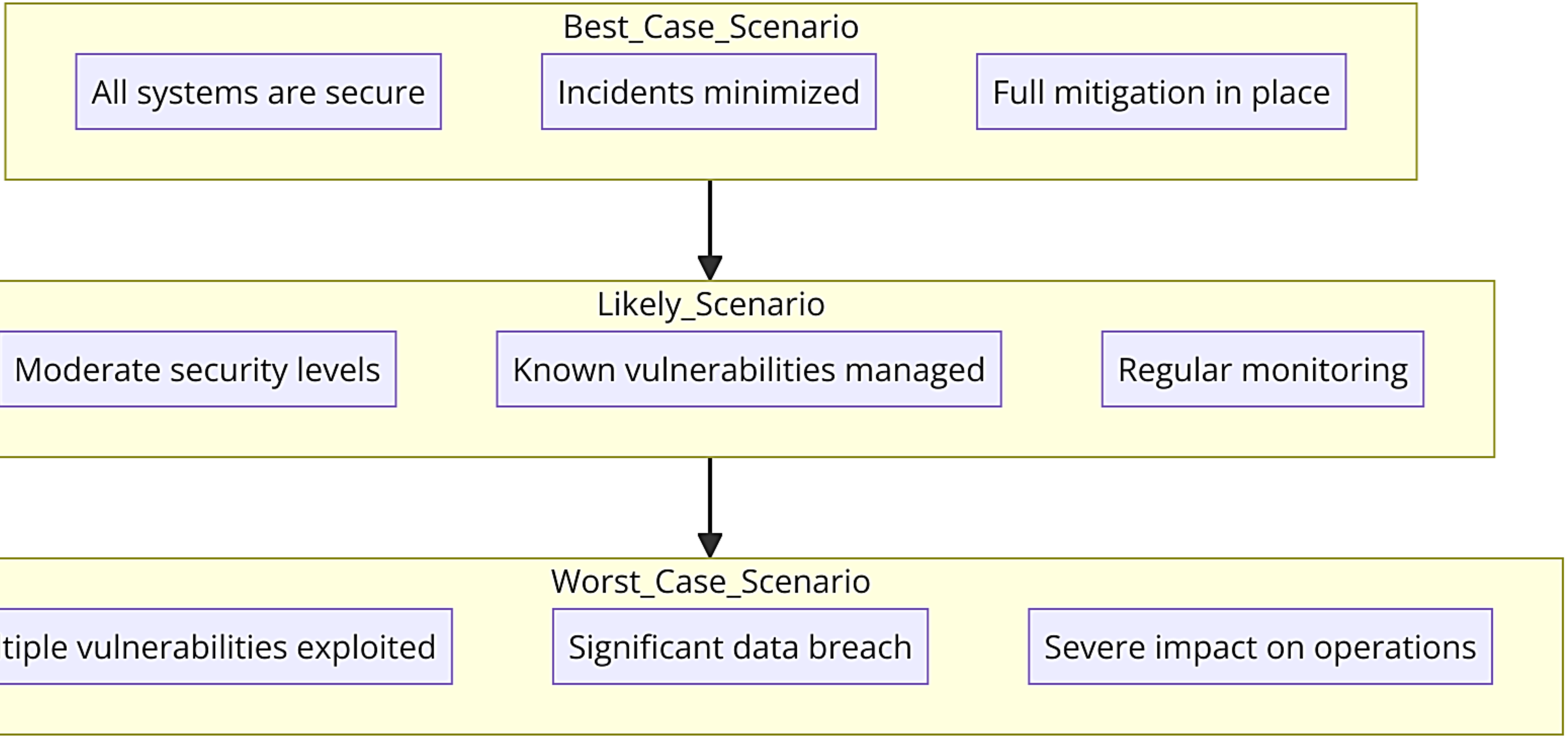
Co-funded by
the European Union

Co-funded by
the European Union

Scenario Analysis (Cyber Systems)

- **Best-Case Scenario:** Describe the ideal scenario, where all systems are secure, and incidents are minimized or fully mitigated.
- **Likely Scenario:** Outline the expected situation, considering current controls and known vulnerabilities.
- **Worst-Case Scenario:** Detail the highest-risk scenario, where an attack exploits multiple vulnerabilities, leading to severe impact.

Scenario Analysis (Cyber Systems)



Best_Case_Scenario

All systems are secure

Incidents minimized

Full mitigation in place

Likely_Scenario

Moderate security levels

Known vulnerabilities managed

Regular monitoring

Worst_Case_Scenario

Multiple vulnerabilities exploited

Significant data breach

Severe impact on operations

Co-funded by
the European Union

Co-funded by the European Union

Risk Register (Cyber Systems)

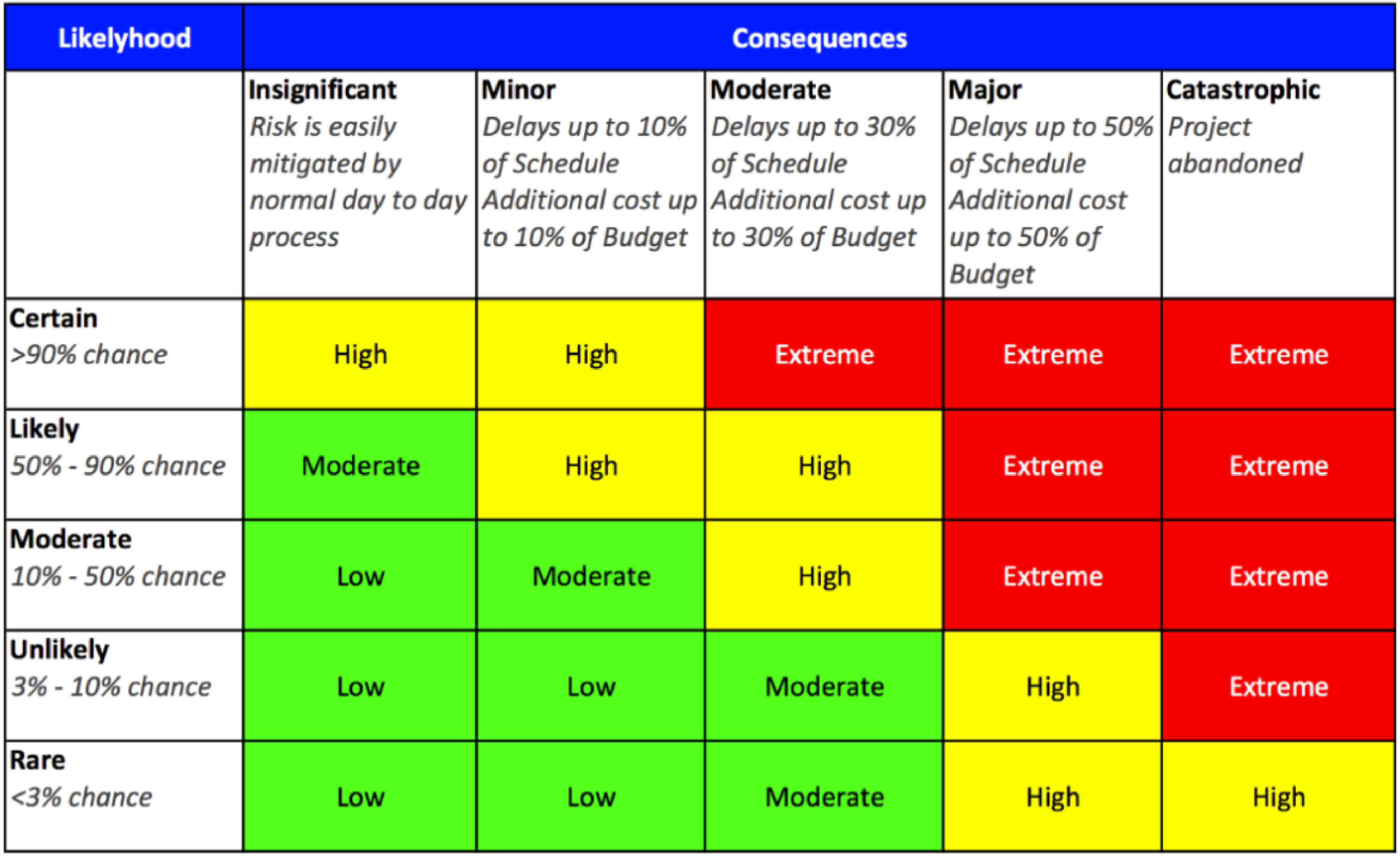
Risk Identification: List known risks, such as phishing attacks, insider threats, or software vulnerabilities.

Impact: Assess the potential impact of each risk (e.g., high, medium, low).

Likelihood: Assign a likelihood rating for each risk.

Mitigation Measures: Document current controls and proposed additional measures to reduce each risk.

Risk Register (Cyber Systems)



Likelyhood	Consequences				
	Insignificant *Risk is easily mitigated by normal day to day process*	**Minor** *Delays up to 10% of Schedule Additional cost up to 10% of Budget*	**Moderate** *Delays up to 30% of Schedule Additional cost up to 30% of Budget*	**Major** *Delays up to 50% of Schedule Additional cost up to 50% of Budget*	**Catastrophic** *Project abandoned*
Certain *>90% chance*	High	High	Extreme	Extreme	Extreme
Likely *50% - 90% chance*	Moderate	High	High	Extreme	Extreme
Moderate *10% - 50% chance*	Low	Moderate	High	Extreme	Extreme
Unlikely *3% - 10% chance*	Low	Low	Moderate	High	Extreme
Rare *<3% chance*	Low	Low	Moderate	High	High

Co-funded by
the European Union

Co-funded by the European Union

Advantage vs Dis-advantage

Quantitative Analysis:

- Advantages: Precision, ability to model complex scenarios.
- **Disadvantages:** Requires extensive data, complex modeling.

Qualitative Analysis:

- **Advantages:** Simpler to conduct, faster.
- **Disadvantages:** Subjective, less precise.

Co-funded by the European Union

Risk Assessment Frameworks

NIST Framework:

- Developed by the National Institute of Standards and Technology.
- Focus on identifying, protecting, detecting, responding to, and recovering from cyber threats.

ISO 27005:

- Part of the ISO/IEC 27000 family, focusing on information security risk management.
- Steps include establishing context, risk assessment, risk treatment, and monitoring.

Co-funded by the European Union

Comparison of NIST and ISO 27005

NIST:

- Pros: Detailed guidance, strong emphasis on cybersecurity.
- Cons: More prescriptive, complex for some organizations.

ISO 27005:

- Pros: Flexible, integrates with broader ISO 27000 family.
- Cons: Less prescriptive, may require additional interpretation for cybersecurity.

Case Studies on Risk Analysis & Assessment

Case Study 1: Quantitative Analysis in the Financial Sector

- Focus: Banking institution assessing risk in loan portfolios.
- Method: Monte Carlo simulations for financial impact.

Case Study 2: Qualitative Analysis in Healthcare

- Focus: Operational risks in patient data handling.
- Method: Expert interviews, risk matrix for prioritization.

Case Study 3: NIST Framework in a Tech Company

- Focus: Cybersecurity incident response.
- Method: Threat analysis, integration with response protocols.

Co-funded by
the European Union

Conclusion

Risk Analysis Techniques

- Quantitative and qualitative risk analysis methods offer unique insights.
- Each approach serves specific purposes, with quantitative methods providing precision and qualitative methods offering simplicity.

Frameworks for Risk Management

- NIST and ISO 27005 frameworks provide structured approaches for risk assessment and are adaptable across industries.
- Each framework has its strengths, with NIST focusing on detailed cybersecurity measures and ISO 27005 offering flexibility.

Questions & answers

Co-funded by
the European Union

Resources

List the resources :

- https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
- https://cybermap.kaspersky.com/
- https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

Co-funded by
the European Union