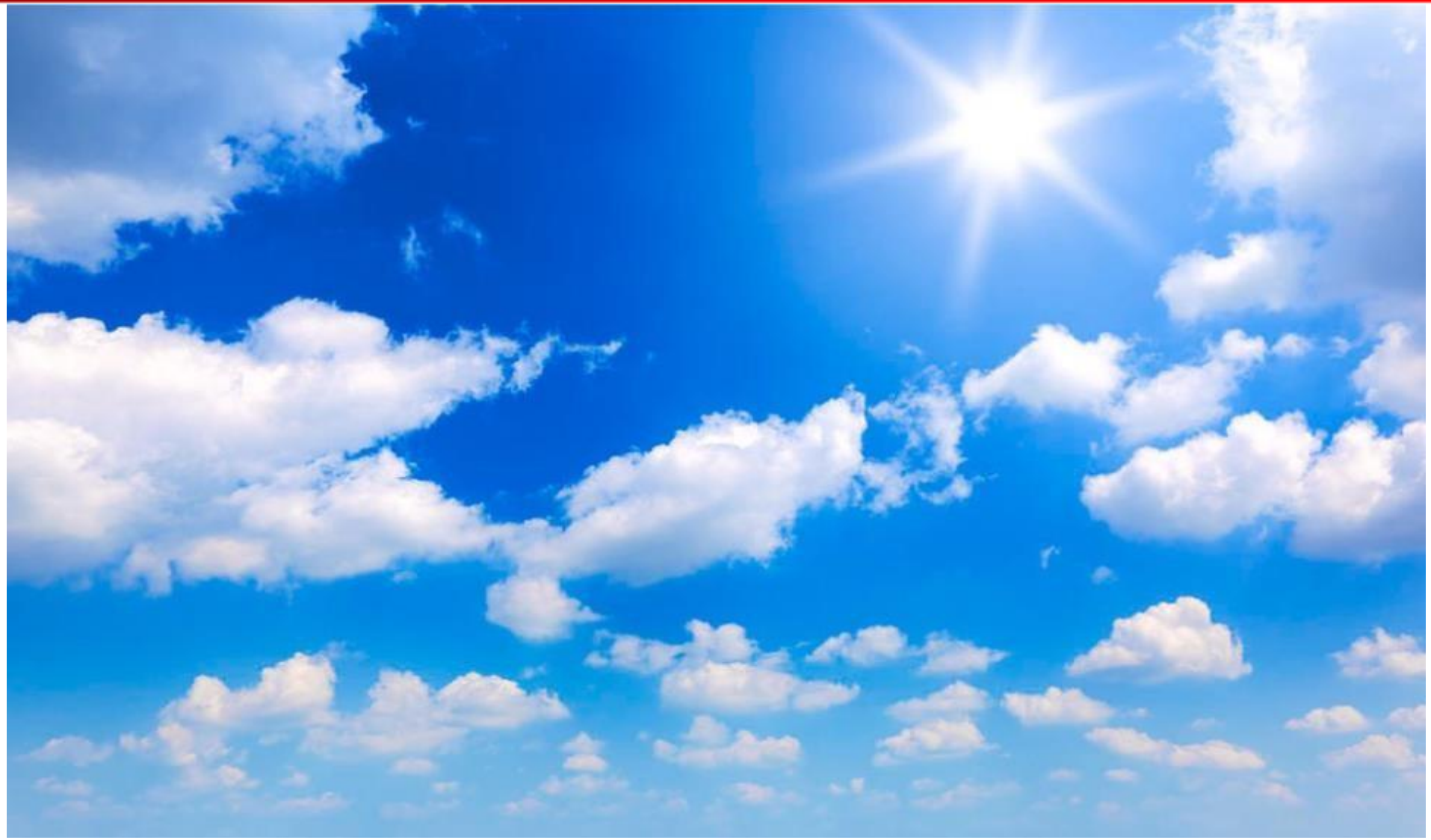
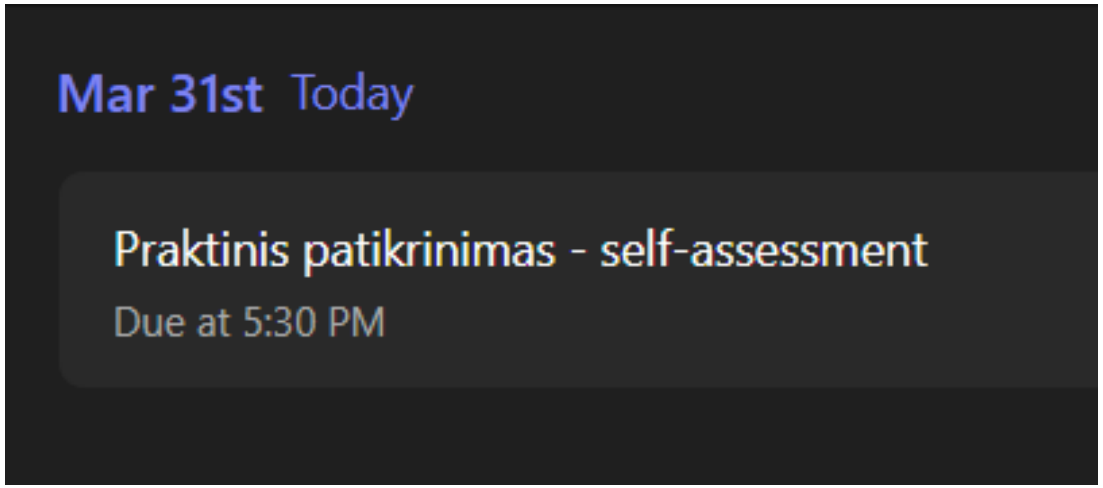
Cyber Security
Lession 2



Labs

Assignments



11 Students – Turned in
0 Students – Viewed
0 Student – Not turned in

LABS

- ✓ Practice exam

13 Questions

LAB 1.1 EXPLANATION

Question 1

A Chief Financial Officer (CFO) has been receiving email messages that have suspicious links embedded from unrecognized senders. The emails ask the recipient for identity verification. The IT department has not received reports of this happening to anyone else. Which of the following is the MOST likely explanation for this behavior?

A. The CFO is the target of a whaling attack.
B. The CFO is the target of identity fraud.
C. The CFO is receiving spam that got past the mail filters.
D. The CFO is experiencing an impersonation attack.

LAB 1.1 EXPLANATION

Question 2

Joe, an employee, knows he is going to be fired in three days. Which of the following characterizations describes the employee?

A. An insider threat

B. A competitor

C. A hacktivist

D. A state actor

LAB 1.1 EXPLANATION

Question 3

The IT department receives a call one morning about users being unable to access files on the network shared drives. An IT technician investigates and determines the files became encrypted at 12:00 a.m. While the files are being recovered from backups, one of the IT supervisors realizes the day is the birthday of a technician who was fired two months prior. Which of the following describes what MOST likely occurred?

A. The fired technician placed a logic bomb.
B. The fired technician installed a rootkit on all the affected users' computers.
C. The fired technician installed ransomware on the file server.
D. The fired technician left a network worm on an old work computer.

LAB 1.1 EXPLANATION

Question 4

An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one implementing the changes. Which of the following describes this policy?

A. Change management
B. Job rotation
C. Separation of duties
D. Least privilege

LAB 1.1 EXPLANATION

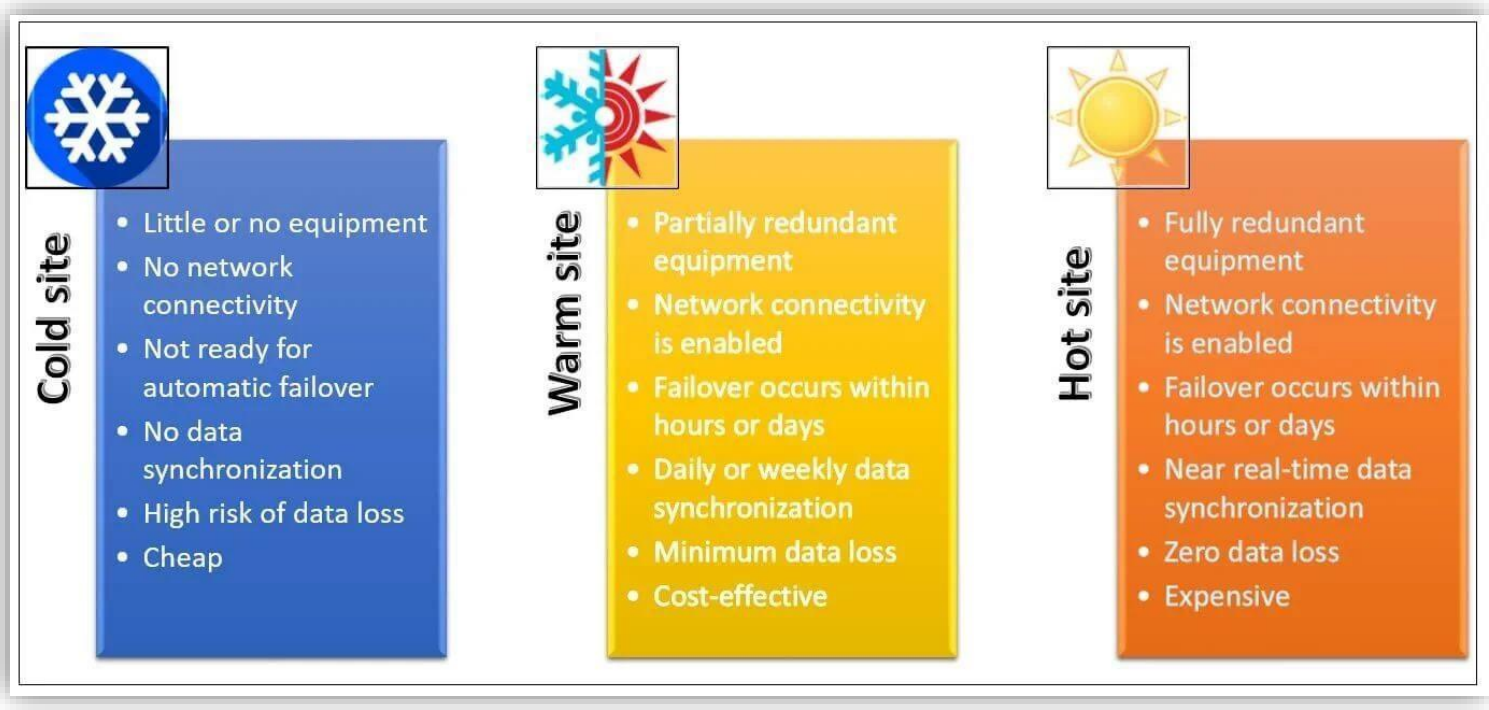
Question 5
Which of the following would be the BEST method to prevent the physical theft of staff laptops at an open-plan bank location with a high volume of customers each day?

A. Guards at the door
B. Cable locks
C. Visitor logs
D. Cameras

LAB 1.1 EXPLANATION

Question 6
Which of the following disaster recovery sites would require the MOST time to get operations back online?

A. Colocation
B. Cold
C. Hot
D. Warm



LAB 1.1 EXPLANATION

Question 7

A security manager needed to protect a high-security datacenter, so the manager installed an access control vestibule that can detect an employee's heartbeat, weight, and badge. Which of the following did the security manager implement?

A. A physical control
B. A corrective control
C. A compensating control
D. A managerial control

LAB 1.1 EXPLANATION

Question 8

Joe, a security analyst, is asked by a co-worker, "What is this AAA thing all about in the security world? Sounds like something I can use for my car." Which of the following terms should Joe discuss in his response to his co-worker? (Select THREE).

A. Accounting
B. Accountability
C. Authorization
D. Authentication
E. Access
F. Agreement

LAB 1.1 EXPLANATION

Question 9

A system administrator is configuring accounts on a newly established server. Which of the following characteristics BEST differentiates service accounts from other types of accounts?

A. They can often be restricted in privilege.
B. They are meant for non-person entities.
C. They require special permissions to OS files and folders.
D. They remain disabled in operations.
E. They do not allow passwords to be set.

LAB 1.1 EXPLANATION

Question 10
Recently, a company has been facing an issue with shoulder surfing. Which of the following safeguards would help with this?

A. Screen filters
B. Biometric authentication
C. Smart cards
D. Video cameras

LAB 1.1 EXPLANATION

Question 11
The process of presenting a user ID to a validating system is known as:

A. authorization.
B. authentication.
C. identification.
D. single sign-on.

LAB 1.1 EXPLANATION

Question 12

An input field that is accepting more data than has been allocated for it in memory is an attribute of:

A. buffer overflow.
B. memory leak.
C. cross-site request forgery.
D. resource exhaustion.

LAB 1.1 EXPLANATION

Question 13
Which of the following if used would BEST reduce the number of successful phishing attacks?

A. Two-factor authentication
B. Application layer firewall
C. Mantraps
D. User training

LAB 1.1 RESULTS

13 Questions

self-assessment
At least 8 correct – passed.

LAB 1.1 RESULTS

Assignment for 11 students

- 1 Students – 13 points
- 1 Student – 11 points
- 2 Students – 10 points
- 2 Students – 9 points
- 3 Students – 7 points
- 1 Students – 6 points
- 1 Students – 4 points
- 0 Student - <not completed>

In the previous lession…

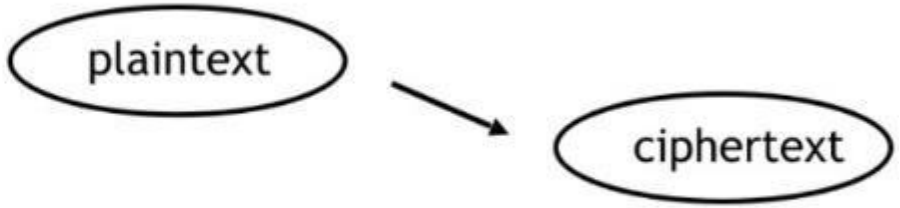
Understanding Core Security Goals

CIA

Understanding Core Security Goals

Confidentiality

- Encryption



- Access controls
  - Identification
  - Authentication
  - Authorization

Understanding Core Security Goals

Availability

- Redundancy & Fault tolerance
- Scalability and Elasticity (scaling up and scaling out)
- Patching
- Resiliency

Understanding Core Security Goals

Integrity

- Protecting data from **unauthorized** :
  - modification
  - deletion
  - addition
- digital signatures
- data hashing

Understanding Core Security Goals

- Authenticity
  - Protecting against impersonation, spoofing and other types of identity fraud :
    - Authentication
    - Digital certificates
    - Biometric identification
- Non-repudiation
  - Party cannot deny having sent or received a message or transaction :
    - Protecting against message tampering and replay attacks
    - Digital signatures
    - Timestamps

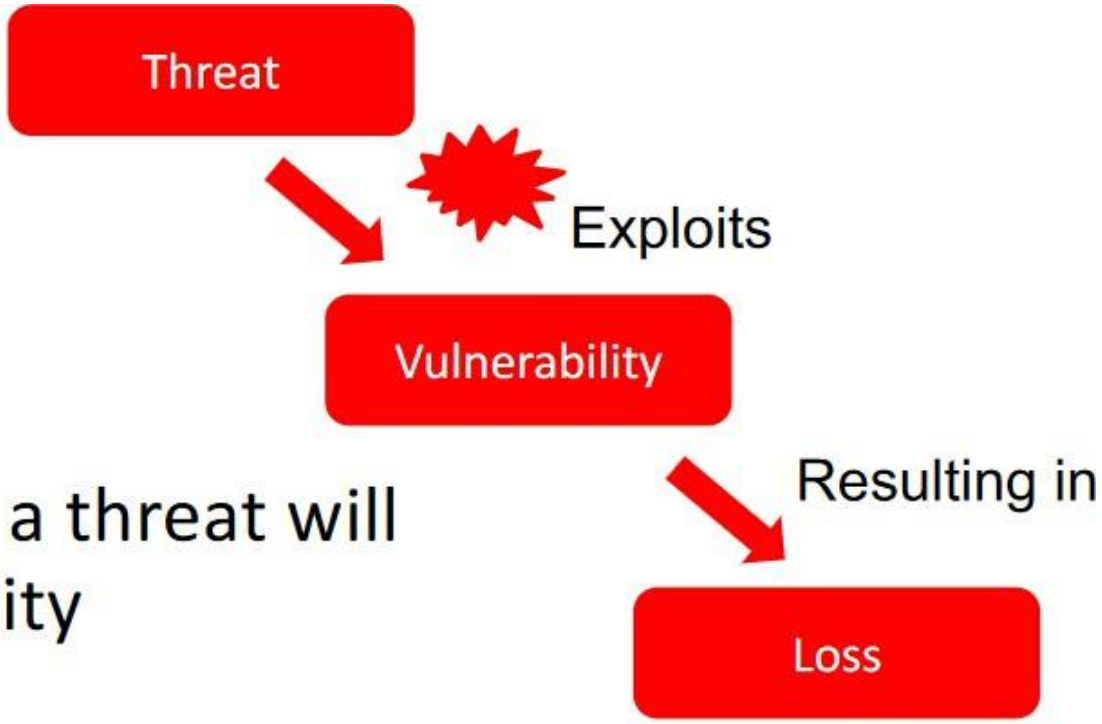
Introduction

- Understanding Core Security Goals DONE
- Introducing Basic Risk Concepts
- Understanding Security Controls
- Using Command-Line Tools
- Understanding Logs

Cyber Security
Risk management

Basic Negative Risk Concepts

- Threats
- Vulnerabilities
  - Any weakness
- Risk is
  - The likelihood that a threat will exploit a vulnerability
- Risk mitigation
  - Reduces the chances that a threat will exploit a vulnerability by implementing controls



Risk - what does it means?

- Risk is an event with some degree of uncertainty;
- Risk management talks about planning, identifying, analyzing, controlling risk and finding best response strategy
- Main objective is to increase impact and likehood of **positive risk (opportunity)** and decrease impact and likehood of **negative risk (threat)**
- Risk management must be proactive process
- Attitude towards risk can be influenced by factors from 3 categories:
  - Risk appetite (anticipation for reward)
  - Risk tolerance (what risk can be withstood)
  - Risk threshold (limit where risk will be unaccepted)

Planning risk

- Planning helps to understand what resources will be needed for risk management
- It is important that stakeholders would accept this plan
- In plan you will find:
  - Risk categories
  - Definitions of both impact and probability and matrix itself
  - Risk breakdown structure
  - Risk tolerance
  - Reporting formats
  - Methodologies
  - Roles/responsibilities
  - Budgeting
  - Timing
- **Tools & Techniques:**
  - Analytical techniques
  - Expert judgment
  - Meetings
- Force majeure should be no more than 10% of all risks

Identification of risks

- Identification is an iterative process
- All risks with their characteristics must be documented in **risk register**
- Everyone can participate in risk identification
- There should be possibility to relatively compare one risk with another
- Risks can be identified using root-cause analysis, brainstorming, interviewing and etc.
- Risks can be written in **cause-event-effect** form
- Preliminary responses are identified
- **Tools & Techniques:**
  - Documentation reviews
  - Information gathering techniques
  - Checklist analysis
  - Assumptions analysis
  - Diagramming techniques
  - SWOT analysis
  - Expert judgment

Qualitative analysis

- First stage of prioritizing risks
- Uncertainty regarding risks at this point is reduced
- Probability and impact are being analyzed
- When analyzing probability and impact refer to their definition established during planning process
- Qualitative analysis is cost effective
- **Quantitative** analysis **can be the next** step;
- Not only negative risk but also positive risk can be assessed
- After the analysis is done risk register must be updated
- **Tools & Techniques:**
  - Risk probability and impact assessment
  - Probability and impact matrix
  - Risk data quality assessment
  - Risk categorization
  - Risk urgency assessment
  - Expert judgment

Risk register with qualitative analysis

Cause	Event (risk)	Effect	Probability (1-8)	Impact (1-10)	Value (probability x impact)
Because there are no team lead	Module will be developed poorly with many security issues	More time for testing and bug fixing, more possibilities and time to use for hacking	2	7	14

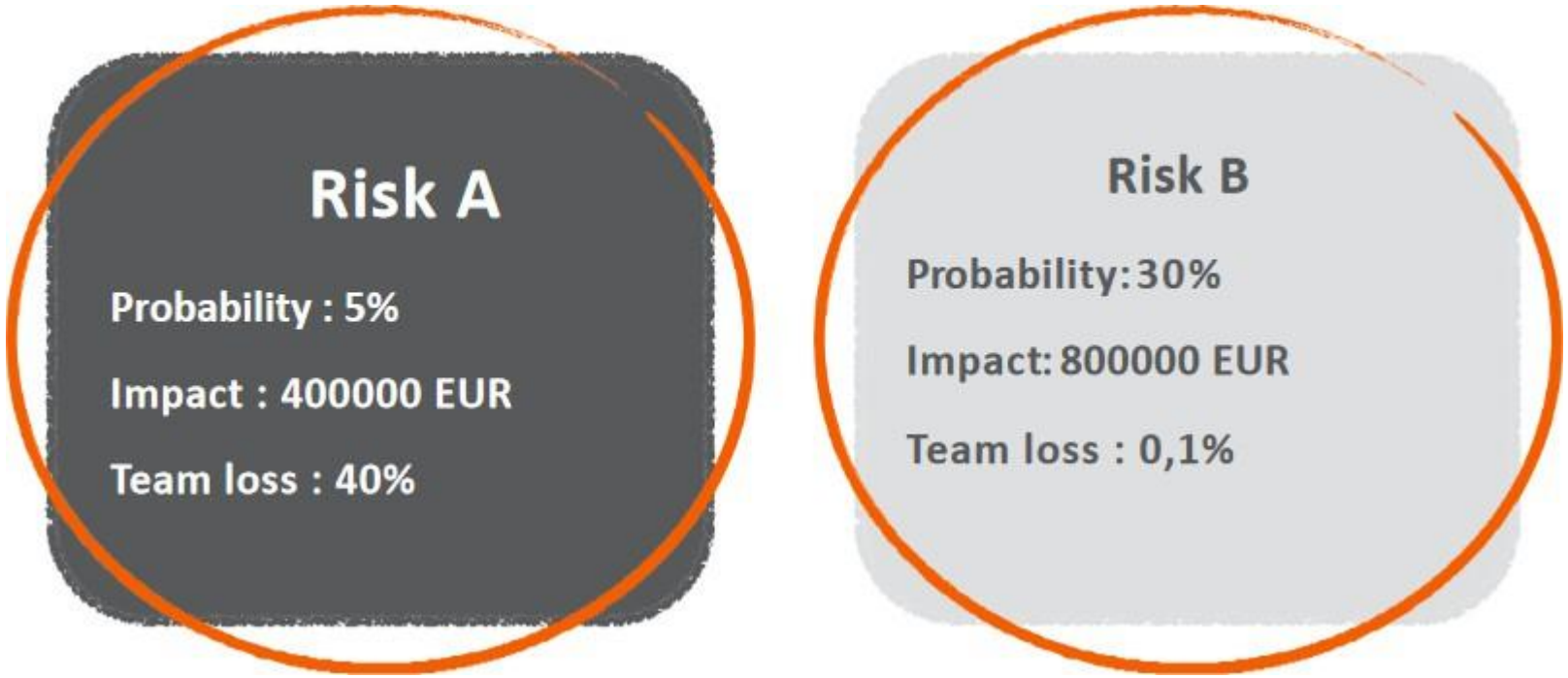
Risk value


Risk A
Probability : 5%
Impact : 4000000 EUR
Risk B
Probability: 70%
Impact: 25000 EUR

Risk matrix

Probability	Threats					Opportunities				
0.90	0.05	0.09	0.18	0.36	0.72	0.72	0.36	0.18	0.09	0.05
0.70	0.04	0.07	0.14	0.28	0.56	0.56	0.28	0.14	0.07	0.04
0.50	0.03	0.05	0.10	0.20	0.40	0.40	0.20	0.10	0.05	0.03
0.30	0.02	0.03	0.06	0.12	0.24	0.24	0.12	0.06	0.03	0.02
0.10	0.01	0.01	0.02	0.04	0.08	0.08	0.04	0.02	0.01	0.01
	0.05/ Very Low	0.10/ Low	0.20/ Moderate	0.40/ High	0.80/ Very High	0.80/ Very High	0.40/ High	0.20/ Moderate	0.10/ Low	0.05/ Very Low

Risk value with additional constraints



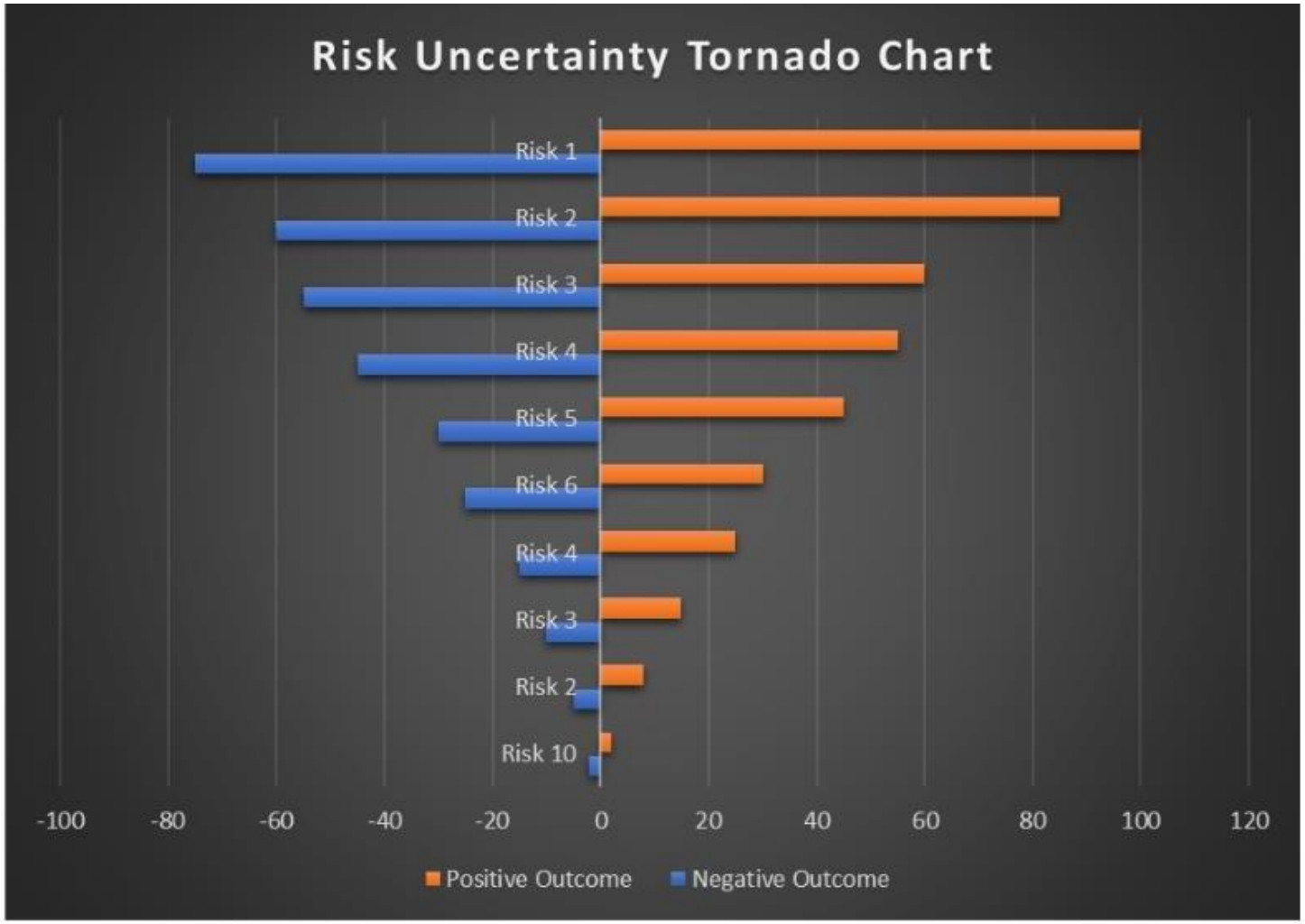
Quantitative analysis

- This process is all about numerical analysis
- This analysis is expensive, requires a lot of data and experience in statistical analysis and modeling
- Analyzed are only those risks, which after qualitative analysis are considered as potential threat to the security
- This process can help to analyze the aggregated effect of all the risks for security
- You must choose how you will gather the data and using which distribution you will represent it
- **Tools & Techniques:**
  - Data gathering and representation techniques
  - Quantitative risk analysis and modelling techniques
  - Expert judgment

Quantitative analysis techniques

- Data Gathering techniques:
  - Interviewing
  - Probability distribution
- Quantitative analysis techniques:
  - Sensitivity analysis (which risks can have the biggest impact on the project):
    - Tornado diagram
  - Expected monetary value – EMV (value of risk):
    - Requires a risk-neutral view;
    - Can be represented as a decision tree
  - Modeling and simulation (uncertainties translated into impact)

Tornado


Risk Uncertainty Tornado Chart
Risk 1
Risk 2
Risk 3
Risk 4
Risk 5
Risk 6
Risk 4
Risk 3
Risk 2
Risk 10
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
Positive Outcome
Negative Outcome

Expected Monetary Value (EMV) analysis

- Formula: **EMV = P * I**, where P – probability and I – impact (monetary value).

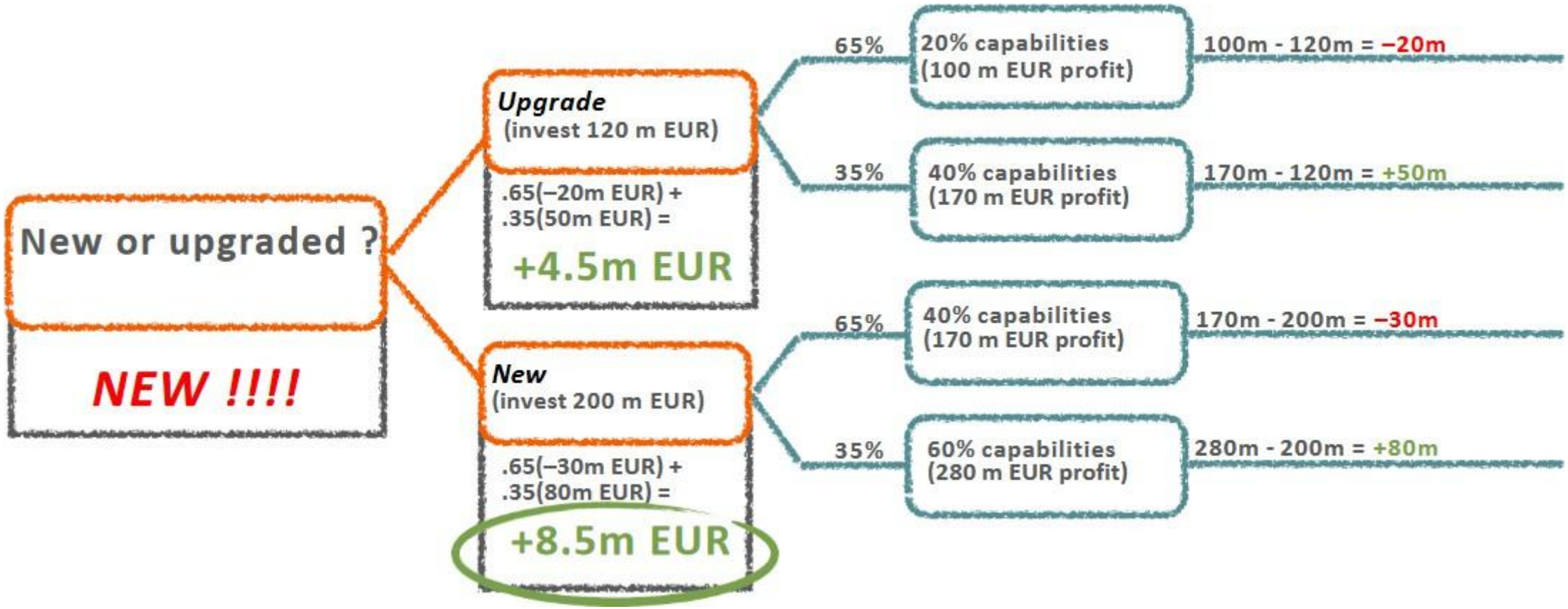
Risk	Probability	Impact	EMV
A	10%	$5,000	$500
B	35%	$20,000	$7,000
C	20%	$100,000	$20,000
D	15%	-$10,000	-$1,500

Complex risk mitigation situation

- A space rocket with better security capabilities is needed for the flight to Mars to reduce the overall security risk, in order to get more money from its passengers.
- If the **existing** model is used with improvements (invest ***120 m EUR***), a **20% - 40% increase in capabilities** is expected.
- If a completely **new** rocket is developed (invest ***200 m EUR***), a **40% - 60% increase in capabilities** is expected.
- **20% - 100 m EUR profit**
- **40% - 170 m EUR profit**
- **60% - 280 m EUR profit**
- Calculating expected profits, **65%** of the respondents were in favour of a more **pessimistic** scenario, **35%** for a more **optimistic** one

What is safer and less risky to invest in ???

EMV solution



Planning responses

- Using response strategies, we must reduce threats and enhance opportunities
- Risks should be addressed by priority
- Each risk response should have its owner
- Risk response should be adequate to the risk
- There are 4 response strategies for threats and 4 strategies for opportunities
- Triggers, symptoms, and warning signs
- Contingency plans, fallback plans (“plan B”)
- Residual risks and secondary risks
- **Tools & Techniques:**
  - Strategies for negative risks or threats
  - Strategies for positive risks or opportunities
  - Contingent response strategies
  - Expert judgment

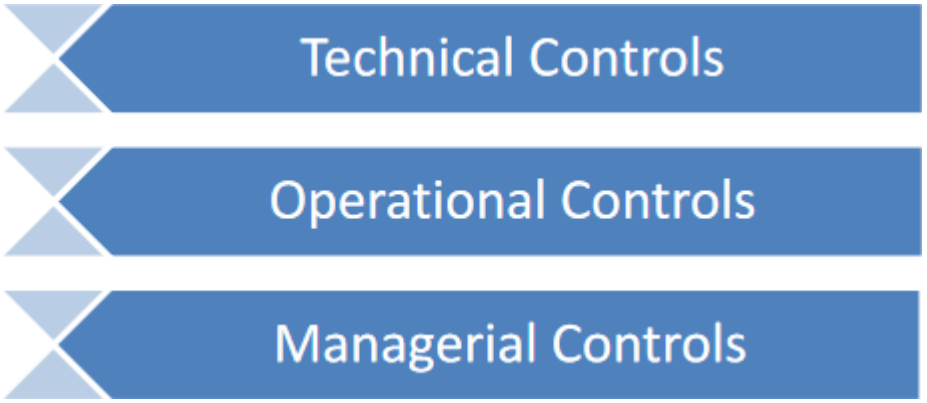
Threats – negative risks

A threat is an event or condition that, if it occurs, has a negative impact on one or more objectives.

- **Avoid.** Threat avoidance is when the team acts to eliminate the threat or protect from its impact.
- **Escalate.** Escalation is appropriate when the team or the manager agrees that a threat is outside the scope of the team or that the proposed response would exceed the manager's authority.
- **Transfer.** Transfer involves shifting ownership of a threat to a third party to manage the risk and to bear the impact if the threat occurs.
- **Mitigate.** In threat mitigation, action is taken to reduce the probability of occurrence and/or impact of a threat. Early mitigation action is often more effective than trying to repair the damage after the threat has occurred.
- **Accept.** Threat acceptance acknowledges the existence of a threat, but no proactive action is planned. Actively accepting a risk can include developing a contingency plan that would be triggered if the event occurred; or it can include passive acceptance, which means doing nothing.

Risk Mitigation

- The key to control selection is the implementation of cost-effective controls that reduce or mitigate risks to levels that are conventional to the organisation
- With the implementation of the controls on the basis of this accept, organisations will reduce risk but not eliminate it
- Controls can be categorised in:



Risk Mitigation

Technical Controls

- These are designed for controlling end-user and system actions
- They can exist within network devices, operating systems, applications, and databases
- Access control lists, password constraints, antivirus software, firewalls, data encryption, and intrusion prevention systems are examples of technical controls
- Technical controls help in the enforcement of requirements specified within administrative controls

Risk Mitigation

Operation Controls

- Monitoring
- Training
- **Preventive** controls are those that attempt to prevent adverse behaviour and actions from occurring
  - Intrusion prevention systems, Firewalls, and segregation of duties are examples of preventive controls
- **Detective** controls are used for the detection of actual or attempted violations of system security
  - Intrusion detection systems and audit logging are examples of detective controls

Risk Mitigation

Managerial Controls

- These controls dictate the performance of activities i.e. how the activities should perform
- Procedures, policies, guidelines, and standards are examples of managerial controls
- Managerial controls provide a framework for the management of personnel and operations
- They can also establish requirements for systems operations
- One such example of managerial control is the requirement that the information security policies should be reviewed annually and updated as required to ensure that they accurately reflect the environment and remain valid

Opportunities

An opportunity is an event or condition that, if it occurs, has a positive impact on one or more objectives.

- **Exploit.** A response strategy whereby the team acts to ensure that an opportunity occurs.
- **Escalate.** As with threats, this opportunity response strategy is used when the team or the manager agrees that an opportunity is outside the scope of the team or that the proposed response would exceed the manager's authority.
- **Share.** Opportunity sharing involves allocating ownership of an opportunity to a third party who is best able to capture the benefit of that opportunity.
- **Enhance.** In opportunity enhancement, the team acts to increase the probability of occurrence or impact of an opportunity. Early enhancement action is often more effective than trying to improve the opportunity after it has occurred.
- **Accept.** As with threats, accepting an opportunity acknowledges its existence but no proactive action is planned.

Response strategies

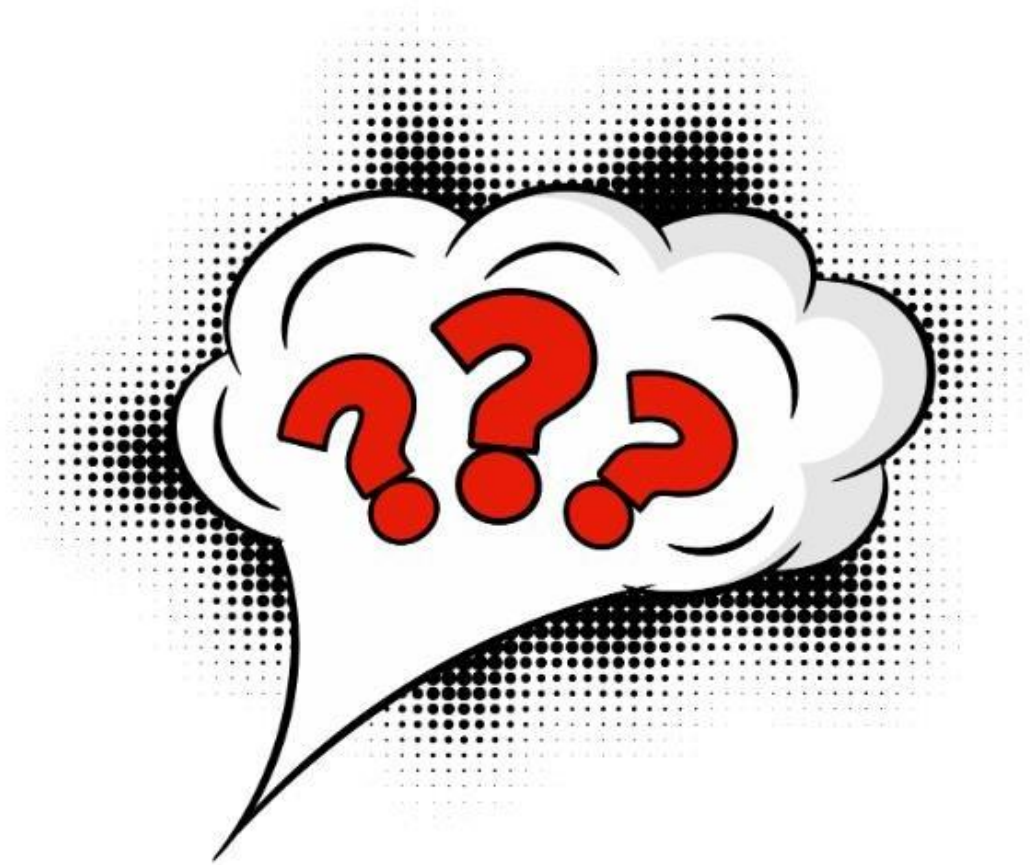
Negative Risks or Threats	Positive Risks or Opportunities
Avoid (eliminate the cause)	Exploit (make sure the opportunity occurs)
Transfer/Deflect/Allocate (make another party responsible)	Share (allocate ownership to a third party)
Mitigate (reduce the probability or the impact)	Enhance (increase the probability or the impact)
Accept ***(do nothing)***	***Accept*** ***(do nothing)***

Controlling risk

- Implement risk response strategies, compare actual situation with the plans and register we have
- Identification and reassessment of risks, closing of outdated risks
- Monitor if risk evaluation is still valid
- Should contingency or fallback plan be implemented
- Auditing risk management processes and the effectiveness of response strategies
- Risks can have either positive or negative impact
- Because of this process change request with corrective and preventive actions can occur
- Workarounds are implemented (when risk happens; no Change Control Board ("CCB") is needed)
- **Tools & Techniques:**
  - Risk reassessment
  - Risk audits
  - Variance and trend analysis
  - Technical performance measurement
  - Reserve analysis
  - Meetings

Things to know about Risk management

- Look not only for threats, but also for an opportunities
- Up to 90% of the identified and investigated threats can be eliminated
- **Uncertainty** is a lack of knowledge about an event that reduces confidence in conclusions drawn from the data
- When looking at risk, one should determine the following:
  - The probability that a risk event will occur (how likely)
  - The range of possible outcomes (impact or amount at stake)
  - Expected timing for it to occur in the project life cycle (when)
  - The anticipated frequency of risk event from that source (how often)
- Someone who does not want to take risk is said to be **risk averse**
- **Risk tolerance** is the degree or level of risk that is acceptable
- **Risk threshold** is the specific point at which risk becomes unacceptable.
- Two main types of risks:
  - **Business risk** (risk of a gain or loss)
  - **Pure (Insurable) risk** (only a risk of loss, e.g., fire, theft, personal injury , etc.)



Labs

- Create risk register with not less than 10 risks (positive and negative)
- Analyse risks :
  - ✓ Perform qualitative analysis
  - ✓ Perform quantitative analysis
  - ✓ Explain tools and methods used