Course: IT RISK MANAGEMENT AND CONTROL

Week 5

Topic: Risk Evaluation and Prioritization

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 4 Material
2. Risk Evaluation Criteria
3. Risk Prioritization Techniques
4. Risk Appetite and Tolerance

Week 4 Review

Before we start looking at week 5 material, let’s first do a quick review of our previous lecture material (week 4)

In week 4, we discussed the following;

Week 4 Summary

1. Risk Assessment and Analysis

- Risk assessment can be defined as the activities done with an aim of understanding and documenting the risk picture for specific parts of a system or an organization.

2. The Risk Assessment process

Step 1. *Context Establishment*

✓ It involves the documentation of both the external and the internal co ntext relevant to the assessment in question.

Step 2. *Risk identification*

✓ Risk identification are the activities aimed at identifying, describing, a nd documenting risks and their possible causes.

Week 4 Summary

1. Risk Assessment and Analysis

Step 3. *Risk Analysis*

- ✓ Risk analysis involves the activities that are aimed at estimating and determining the level of the identified risks.

Step 4. *Risk Evaluation*

- ✓ Risk evaluation involves the activities that deal with the comparison of the risk analysis results with the risk evaluation criteria to determine which risks should be considered for treatment.

Step 5. *Risk Treatment*

- ✓ Risk treatment means the activities aimed at identifying and selecting means for risk mitigation and reduction.

Week 4 Summary

2. Risk assessment methodologies

Risk assessment methodologies are processes used to identify, analyze, and evaluate risks in order to manage or reduce them.

They work by:

- **Identifying risks** – They spot potential hazards or threats.
- **Analyzing risks** – They determine the likelihood and impact of each risk.
- **Evaluating risks** – Then they rank the risks to prioritize action.
- **Controlling risks** –Finally they implement measures to reduce or eliminate risks.

Week 4 Summary

Risk assessment methodologies cont….

Qualitative Vs Quantitative Risk Assessments

Qualitative Risk Assessment.

- Qualitative risk assessment involves evaluating risks based on expert judgment, ex perience, opinions, and descriptions rather than relying on numeric data.

Quantitative Risk Assessment.

- Quantitative risk assessment describes risks with numbers and data.

Week 4 Summary

3. Conducting an IT Risk Assessment

Conducting an IT Risk Assessment is a structured process to identify, evaluate, and mitigate pot ential threats to an organization's information technology infrastructure

Steps;

- ✓ Identify Assets
- ✓ 2. Identify Threats
- ✓ 3. Identify Vulnerabilities
- ✓ 4. Assess the Risk Impact and Likelihood
- ✓ 5. Prioritize Risks
- ✓ 6. Develop Risk Mitigation Strategies
- ✓ 7. Document and Communicate the Findings

Week 4 Summary

3. Conducting an IT Risk Assessment cont..

Steps cont..

- ✓ 8. Implement and Monitor risk mitigation plans
- ✓ 9. Review and Update the Risk Assessment

Conclusion: Conducting an IT risk assessment involves a structured process of identi fying and analyzing risks, followed by the implementation of effective mitigation strateg ies.

Week 5: Risk Evaluation and Prioritization

Qn: What is Risk Evaluation and Prioritization in IT risk management?

1. Risk evaluation

- In IT risk management, Risk evaluation is the process of assessing/analyzing identified risks in terms of their potential impact and likelihood.
- The goal is to assess how significant each risk might be if it occurs and how likely it is to happen, which allows organizations to make informed decisions on how to handle those risks which require immediate attention or fast mitigation.
- This process helps organizations to allocate resources effectively and ensure that critical IT systems are protected.

Risk Evaluation and Prioritization

Risk Evaluation cont..

- The evaluation involves assessing the impact and likelihood of each identified IT risk.
- This is done to understand the potential consequences of a ris k materializing and the probability that it will happen.

Risk evaluation steps:

- **1. Identify potential risks.**
- The first step is to identify potential risks related to IT operation s.
- The risks may include data breaches, system failures, cyber-at tacks, or compliance violations.
- The risks can therefore be anything from technical failures to e xternal threats like cyberattacks.

Risk Evaluation and Prioritization

Risk evaluation steps cont…

2. Assess the potential Impact of each risk.

For each identified risk, assess its potential impact if it occurs.

N.B: Impact refers to the consequences or damages that the organization might suffer due to the identified risks.

The impact assessed in step 2 can either be;

High Impact: The impact may result in severe financial losses, legal penalti es, major system downtime, or loss of customer trust.

Medium Impact: The impact might cause operational disruptions or modera te financial losses and is manageable.

Low Impact: The impact may result in minor inconveniences with little to no financial or reputational loss.

Risk Evaluation and Prioritization

Risk evaluation steps cont…

3. Assess Likelihood.

- Likelihood is the probability that the risk will materialize.

NB. Materialization refers to the process by which a potential risk transforms i nto an actual event or outcome, leading to a negative impact on an organizatio n, project, or system.

- For each risk, assess how often similar risks have occurred or how vulnerab le the IT system is to such risks.

The likelihood can be graded as;

High Likelihood: A risk that has a high probability of occurring based on past experience or known vulnerabilities.

Medium Likelihood: A risk that is possibale but may not occur frequently.

Low Likelihood: A rare event that has a low probability of happening.

Risk Evaluation and Prioritization

Risk evaluation steps cont…

4. Combine Impact and Likelihood.

- After assessing the impact and likelihood, you can evaluate the overall risk level.
- Risks with both high impact and high likelihood should be treated as cri tical risks, while risks with low impact and low likelihood may be less cri tical.

Example: An Example of risk evaluation: (A Cybersecurity Risk)

Scenario: Imagine an e-commerce company that relies on its website for online sales. One of the risks identified is the possibility of a cyberattack, specifically a Distributed Denial of Service (DDoS) attack that could shut down the website.

Risk Evaluation and Prioritization

- **An Example of risk evaluation cont…**

Step 1: Identify the risk (A cyber security risk has been identified)

Step 2: Assess the Impact

- If a DDoS attack occurs, the website could be down for hours or even days.
- **Impact:** The company could lose significant sales revenue during the downtime, damage its reputation among customers, and potentially in cur penalties for not meeting service-level agreements (SLAs) with pa rtners.
- Since the company's core business depends on the website, the imp act is rated as High.

Risk Evaluation and Prioritization

- **An Example of risk evaluation cont…**

Step 3: Assess the Likelihood

- If after analyzing past incidents, the company discovers that other e-comme rce businesses in the same sector have experienced DDoS attacks recently ,
- And, the IT team also finds that the company's current defenses (firewalls a nd traffic monitoring) are outdated and not well equipped to handle a large-scale attack.
- Based on these factors, the likelihood is rated as Medium-High because the threat is real, and the company's defenses are not strong.

Risk Evaluation and Prioritization

- **An Example of risk evaluation cont…**

Step 4: Combine Impact and Likelihood

- Since the **impact is high** (significant financial and reputational damage) and the **likelihood is medium-high** (a probability due to the weak defenses and industry trend), the overall risk level is evaluated as Critical.

Risk Evaluation and Prioritization

- **An Example of risk evaluation cont…**

Step 5: Conclusion/decision about mitigation

- Based on this risk evaluation, the company would prioritize this risk for imme diate action.
- They may choose to invest in advanced DDoS protection services, update fir ewall rules, or purchase cyber insurance to mitigate the risk.

Risk Evaluation and Prioritization

Risk Evaluation Tools for our Example:

- **Risk Matrix:** A common tool that helps plot risks based on their impact a nd likelihood. For example, the DDoS attack would be placed in the high-i mpact, medium-high-likelihood rows, indicating it needs urgent attention.
- **Risk Register:** This is a document where all risks, along with their evalua tion (impact and likelihood), are recorded. Eg; the DDoS attack would be registered as a high-priority risk requiring immediate mitigation.

Risk Evaluation and Prioritization

Conclusion:

- In the example, the risk evaluation process helped the company understand how serious a DDoS attack could be and how likely it would happen.
- This understanding allows the company to make informed decisions on how to prioritize resources and control measures such as investing in new security technology or developing a response plan.

Risk Evaluation Criteria

- Risk Evaluation Criteria are the standards or benchmarks a n organization uses to assess and measure the significanc e of risks.
- These criteria provide a structured approach to determine whether a risk is acceptable, needs mitigation, or should be prioritized.
- The evaluation process considers both the impact and likeli hood of risks, but the criteria go deeper by considering the organization's risk appetite, regulatory requirements, and st rategic objectives.

Key Components of Risk Evaluation Criteria

1. Impact Criteria

This criterion assesses the potential damage or loss that could occur if a risk t akes place.

The impact is evaluated in several areas;

- **Financial Impact**: Loss of revenue, increased costs, or financial penalties.
- **Operational Impact**: Disruption of services, production delays, or resource inefficiencies.
- **Reputational Impact**: Damage to the organization's public image or loss of customer trust.
- **Legal and Regulatory Impact**: Fines, lawsuits, or compliance breaches.
- Example: A data breach could result in significant financial costs from legal penalties and reputation damage, so it may be categorized as high impact.

Components of Risk Evaluation Criteria cont..

2. Likelihood / Probability Criteria

- This measures the probability or frequency with which a risk is expected to occur.
- Likelihood is assessed based on historical data, known vulnerabilities, and external factors such a s industry trends and can be grouped as;

- **Rare:** The event has a very low chance of happening e.g; once in 10 years.
- **Unlikely:** The event might happen, but it is not frequent e.g; once in 5 years.
- **Possible:** The event could occur but not often e.g; annually.

Components of Risk Evaluation Criteria cont..

Likelihood / Probability Criteria cont..

- **Likely:** The event is expected to occur periodically e.g; several times a year.
- **Almost Certain:** The event is very likely to happen soon or frequently.
- Example: If cyberattacks have frequently targeted similar companies in the same sector, the likelihood of a similar attack could be rated as likely or almost certain.

Components of Risk Evaluation Criteria cont..

3. Risk Appetite and Tolerance

- Risk appetite defines the amount of risk an organization is willing to a ccept in correspondence to its objectives.
- These criteria help in deciding whether the organization is comfortabl e with a particular risk or if it requires mitigation.
- **Risk Appetite:** A company may have a higher tolerance for financial risks if it is in a growth phase, but a very low appetite for risks that co mpromise customer data.
- **Risk Tolerance:** The level of the risk the company is willing to tolerat e before taking corrective action e.g; a 5% variance in service uptime .

Components of Risk Evaluation Criteria cont..

4. Legal and Regulatory Compliance Criteria

- Some risks are evaluated based on how they affect the organization's ability to comply with laws, industry standards, and regulations.
- A failure to comply can lead to severe penalties, making regulatory risks a pr iority.
- Example: A financial institution may evaluate the risk of non-compliance with data protection laws e.g; **General Data Protection Regulation (GDPR**) as a high impact and likely, making it a top priority to address.

Components of Risk Evaluation Criteria cont..

5. Business Continuity Criteria

- The criteria assesses how risks impact the organization's ability to continue operations amidst the disruptions.
- If a risk threatens business continuity (eg; a major IT failure), it may be given higher priority of mitigation.
- Example: For a cloud service provider, the risk of a prolonged outa ge could have significant consequences, so the business continuity criteria would rank this risk as critical.

Components of Risk Evaluation Criteria cont..

6. Stakeholder Impact Criteria

- This assesses how risks affect key stakeholders, such as customers, shareholders, employees, and partners.
- Risks that negatively affect stakeholders, particularly in critical areas like customer service or shareholder value, will usually be evaluated as high-priority.
- Example: A risk that leads to customer dissatisfaction or loss could severely damage a company's market position, and would therefore be rated highly.

Components of Risk Evaluation Criteria cont..

7. Time-Based Criteria

- Time sensitivity is another critical factor in evaluating risks.
- This criterion focuses on how quickly risks must be addressed.

Companies may have;

- **Immediate risks:** Risks that require immediate action e.g; a ranso mware attack in progress.
- **Short-term risks:** Risks that need mitigation in the near future e.g; outdated software vulnerabilities.
- **Long-term risks:** Risks that are lower in priority and can be addres sed over time e.g; potential future regulatory changes.

Components of Risk Evaluation Criteria cont..

8. Cost vs. Benefit Analysis Criteria

- This criterion evaluates the financial costs of mitigating or accepting a risk versus the potential benefits.
- Organizations might tolerate some risks if the cost of mitigation is higher t han the potential impact.
- **Example:** If upgrading all systems to prevent a low-probability event woul d cost millions, the organization may opt for partial mitigation, weighing th e cost-benefit ratio.

Components of Risk Evaluation Criteria cont..

Example of Risk Evaluation Using Criteria:

- Let’s consider a risk evaluation scenario for an IT company concerned abo ut data breaches;
- **Impact:** A data breach could expose sensitive customer information, leadi ng to a loss of trust, regulatory fines, and costly remediation efforts. This is rated as **high** across financial, reputational, and regulatory criteria.
- **Likelihood:** Based on industry analysis, similar companies have faced fre quent cyberattacks. The likelihood of a breach is *rated as* **likely.**
- **Risk Appetite:** The company has a **very low appetite** for risks that compr omise customer data, meaning this risk is unacceptable.

Components of Risk Evaluation Criteria cont..

Example of Risk Evaluation Using Criteria cont..

- **Compliance:** Failure to comply with data protection laws like GDP R could result in significant fines, making this a **high priority risk** f rom a regulatory standpoint.
- **Business Continuity:** A large-scale data breach could disrupt ser vices and impact business continuity, pushing this risk **higher** on th e priority list.
- **Cost vs. Benefit:** The cost of implementing advanced security me asures is high, but given the severe consequences of a breach, the benefit outweighs the cost. So the mitigation must be given **high** pr iority.

Conclusion

- Based on risk evaluation criteria, the company would likely categori ze this data breach risk as **high priority,** necessitating immediate a ction such as investing in stronger cybersecurity defenses.
- Therefore, risk evaluation criteria provide a structured and systemati c way to assess risks by examining their potential impact, likelihood, and aligning them with the organization's goals and limitations.
- By using these criteria, organizations can make informed decisions about which risks to prioritize and how to allocate resources for miti gation them.

RISK PRIORITISATION

- Risk prioritization in IT risk management is the process of ranki ng identified risks based on their potential impact and likelihood of occurrence.
- This helps organizations allocate resources and attention to the most critical risks that could affect their systems, data, or operat ions.

Risk Prioritization cont…

An example of Risk Prioritization in IT Risk Management.

- A certain company hosts a web-based application for its clients. Duri ng an IT risk assessment, the following risks get identified;
- **Risk A:** Cyberattack e.g ransomware on the company's network.
- **Risk B:** Outdated software leading to system vulnerabilities.
- **Risk C:** Hardware failure in the data center.
- **Risk D**: Inadequate user training leading to security breaches.
- **Risk E:** Power outage at a local office.

Risk Prioritization cont..

- To prioritize these risks, the company uses a risk matrix or risk ass essment tool that assesses each risk based on two criteria:

1) Impact: How much damage the risk could cause if it materializes/ happens.
2) Likelihood: How likely it is that the risk will occur.

How to prioritize these risks;

Step-by-step Process:

1. Risk A (Cyberattack):

- **Impact**: **High** (a cyberattack could compromise sensitive data, resulting i n legal penalties, and cause reputational damage).
- **Likelihood**: **High** (cyberattacks are frequent and targeted toward compa nies in this sector).
- **Priority**: **Critical** (must be addressed immediately with cybersecurity me asures).

2. Risk B (Outdated software):

- **Impact**: **Medium** (vulnerable software could lead to potential exploits.
- **Likelihood**: **Medium** (the software is due for an update, but there's no i mmediate threat).
- **Priority**: High (important but not as urgent as a cyberattack).

How to prioritize these risks;

Step-by-step Process Cont…

3. Risk C (Hardware failure):

- **Impact**: **Medium** (could cause downtime but backup systems may mitigate major damage).
- **Likelihood**: **Low** (the company has good hardware monitoring syste ms).
- **Priority**: **Medium** (important to monitor but not an immediate threat) .

4. Risk D (User training):

- **Impact**: **High** (poor training could lead to human errors like phishing attacks).
- **Likelihood**: **Medium** (some incidents have already occurred due to lack of training)
- **Priority**: **High** (focus on training initiatives to reduce the likelihood of errors).

How to prioritize these risks;

Step-by-step Process Cont…

5. Risk E (Power outage):

- **Impact**: **Low** (temporary office downtime, but no data loss or system damage).
- **Likelihood**: **Low** (rare occurrence in the region, backup power systems available).
- **Priority**: **Low** (minimal focus needed).

How to prioritize these risks;

Final Risk Prioritization:

1. **Risk A: Cyberattack** (Critical priority, high impact and High likelihood).
2. **Risk D: Inadequate user training** (High priority, high impact, medium likelihood).
3. **Risk B: Outdated software (**High priority, medium impact, medium likelihood).
4. **Risk C: Hardware failure** (Medium priority, medium impact, low likelihood).
5. **Risk E: Power outage** (Low priority, low impact and low likelihood).

IT Risk Prioritization

Outcome:

- Based on this prioritization, the web-based application host comp any facing these risks should immediately invest in enhanced cyb ersecurity measures (to address **Risk A**) and start introducing/im plementing user training programs (to mitigate **Risk D**).
- Less critical issues, like outdated software **(Risk B)** and hardwar e failure **(Risk C)**, are scheduled for future actions, while the risk of power outage (**Risk E)** is considered acceptable for the compa ny at present.

Conclusion:

- Risk prioritization enables IT teams to focus their limited resources on the most pressing issues that could harm the organization.
- It ensures continuous management of risks that have the greatest potential to disrupt operations or expose the company to threats.

Risk Prioritization Techniques

- Risk prioritization techniques are essential for helping organizations focus th eir efforts on addressing the most critical risks first.
- These techniques help identify, evaluate, and rank risks based on their pote ntial impact and likelihood, ensuring that resources are allocated to the area s that matter most.
- Some commonly used risk prioritization techniques Include-;

Risk prioritization techniques cont…

1. Risk Matrix Technique

- This is one of the most popular techniques for risk prioritization.
- The risk matrix plots risks based on their likelihood and impact.

How it works:

Likelihood: How likely is it that the risk will occur?

Impact: How severe would the consequences be if the risk occurs?

- The matrix usually has a grid with levels like low, medium, high for both probability and impact.
- The risks are plotted in the grid, and the ones that fall in the high li kelihood, high impact zone are treated as top priority.

Risk Matrix technique cont...

Example

Risk	Likelihood (L)	Impact (I)	Risk Score (L x I)	Priority
Data breach	High (5)	Severe (5)	25	High
Delayed project delivery	Medium (3)	Moderate (3)	9	Medium
Server downtime	Low (2)	High (4)	8	Medium
Poor user feedback	Medium (3)	Low (2)	6	Low
Regulatory compliance fail	Rare (1)	Severe (5)	5	Low

Table 1. Risk Matrix Technique

Risk Matrix technique cont...

Risk matrix Example explained.

- **Likelihood:** How likely is the risk event? Rated from 1 (Rare) to 5 (High).
- **Impact:** What would be the severity if the risk occurs? Rated from 1 (Low) to 5 (Severe).
- **Risk Score:** The overall risk score is the product of Likelihood and Impact (L x I).
- **Priority:** Based on the risk score, risks are categorized into prioriti es such as High, Medium, or Low, allowing teams to focus on critic al risks.

Risk prioritization techniques cont..

2. Failure Modes and Effects Analysis (FMEA)

- FMEA is a systematic approach used in risk prioritization.
- It focuses on identifying ways in which risks could happen, their effe cts, and then ranking them based on three criteria which is;
- **Severity (S):** How bad is the effect of the risk?
- **Occurrence (O):** How frequently is the risk likely to happen?
- **Detection (D):** How likely may the risk be detected before it causes harm?
- A Risk Priority Number (RPN) is calculated using the formula:

$$\mathbf{RPN = Severity \times Occurrence \times Detection}$$

Higher RPN values indicate more critical risks, which should be prioriti zed or mitigated first.

Risk prioritization techniques cont..

3. SWIFT (Structured What-If Technique)

- SWIFT involves brainstorming parties about possible risks by asking "What if?" questions.
- This technique helps identify risks that might be critical by using open-ended dis cussions among teams.
- Once risks are identified, they are ranked based on their likely hood and impact and risks with high impact and likelihood are mitigated first.
  - **Likelihood:** Which scenario is likely to occur?
  - **Impact**: What would happen if it occurred?
- This technique is useful for uncovering unanticipated risks and fostering collaborative risk identification.

Risk prioritization techniques cont..

4. Cost-Benefit Analysis technique

- This technique helps prioritize risks by comparing the costs of mitigating the risk with the benefits of reducing the risk.
- The risks that have the highest benefit-to-cost ratio are given priority, meani ng they provide high value for the resources spent to mitigate them.

Risk prioritization techniques cont..

5. Delphi risk prioritization Technique

- The Delphi technique is a consensus-building method involving a group of e xperts who individually first evaluate and prioritize risks.
- After ranking the risks individually, experts' responses are aggregated and s hared within the group.
- The process is repeated until a consensus is reached on the highest-priority risks.

Risk prioritization techniques cont..

6. Quantitative Risk Analysis (Monte Carlo Simulation)

- This technique uses statistical methods to calculate the probability of different risk outcomes.
- Monte Carlo simulation is often used to simulate the effect of various risks on a project or process and estimate the overall impact.
- By running numerous simulations, organizations can see which risks have the greatest chance of causing significant problems, allowing th em to prioritize those risks accordingly.

Risk Appetite and Tolerance

- Risk Appetite and Risk Tolerance are essential concepts used to def ine an organization's approach to taking and managing risks.
- Both terms are critical in risk evaluation and prioritization, helping o rganizations to balance potential gains against potential losses.

1. Risk Appetite

- ✓ It is the amount of risk an organization is willing to accept in respect to its objectives.
- ✓ It’s a high-level, strategic view of how much risk the organization is comfortable taking on.
- ✓ Risk appetite helps to set the boundary for risk-taking activities.
- ✓ It reflects the organization’s culture about risk, which may be influen ced by factors such as corporate culture, financial strength, stakeho lder expectations, and the nature of the business.

Risk Appetite and Tolerance

2. Risk Tolerance

- ✓ Risk tolerance refers to the specific limits of risk that an organization is willing to tolerate within its risk appetite.
- ✓ It is more operational than risk appetite, defining the acceptable vari ation in achieving objectives.

Explanation:

- ✓ While risk appetite is broad, risk tolerance is detailed and specific, oft en expressed in quantitative terms.
- ✓ It provides actionable guidelines for decision-makers when managin g risks. It answers questions like, "How much deviation from expecte d performance are we willing to accept before we need to act?“
- ✓ Deviation refers to a situation where actual outcomes or performance differ from expected or planned results.

Risk Appetite and Tolerance

Relationship Between Risk Appetite and Tolerance

- **Risk Appetite is the big picture**: How much total risk is the organization willing to take on to achieve its goals?
- **Risk Tolerance is the detailed picture:** Within that overall appetite, how much variability or fluctuation is acceptable before corrective measures ar e needed?

Summary Week 5

1. Risk Evaluation

- The process of assessing identified risks in terms of their potential impact an d likelihood.

Risk evaluation steps:

1. Identify potential risks.

2. Assess the potential Impact of each risk.

3. Assess Likelihood.

4. Combine Impact and Likelihood.

Summary Week 5

2. Risk Evaluation Criteria

- ✓ Impact Criteria
- ✓ Likelihood / Probability Criteria
- ✓ Risk Appetite and Tolerance
- ✓ Legal and Regulatory Compliance Criteria
- ✓ Business Continuity Criteria
- ✓ Stakeholder Impact Criteria
- ✓ Time-Based Criteria
- ✓ Cost vs. Benefit Analysis Criteria

Summary Week 5

3.Risk Prioritization

- ✓ The process of ranking identified risks based on their potential impact and likelihood of occurrence which helps organizations to attend to the most critical risks that could affect their systems, data, or operations.

4. Risk Prioritization Techniques

These help organizations focus their efforts on addressing the most critical risks first.

1. Risk matrix technique

The risks are plotted in the grid, and the ones that fall in the high likelihood, high impact zone are treated as top priority.

2. Failure Modes and Effects Analysis (FMEA)

Risk Priority Number**(RPN)** is calculated by =Severity×Occurrence×Detection

Higher RPN values indicate more critical risks, which should be prioritized or mitigated first.

Summary Week 5

4. Risk Prioritization Techniques cont..

3. SWIFT (Structured What-If Technique)

It involves brainstorming parties with "What if?" questions about possible risks, th eir impact and likelihood. Risks with high impact and likelihood are attended first.

4. Cost-Benefit Analysis technique

- Prioritizes risks by comparing the costs of mitigating the risk with the benefits o f reducing the risk and the risks with the highest benefit-to-cost ratio are given first priority.

5. Delphi risk prioritization Technique

- A method that involves a group of experts who individually first evaluate and pri oritize risks and after discuss until they a reach consensus on the highest-priori ty risks.

Summary Week 5

4. Risk Prioritization Techniques cont..

6. Monte Carlo simulation Technique

- ✓ A technique often used to simulate the effect of various risks on a project and estimate the overall impact thus through simulations organizations can see which risks have the greatest chance of causing significant problems, allowing them to mitigate those risks first.

5. Risk Appetite and Tolerance

Risk Appetite: The amount of risk an organization is willing to accept in respective of its objectives.

Risk Tolerance: The specific limits of risk that an organization is willing to tolerate within its risk appetite.

References

- *Quantitative Risk Management: Concepts, Techniques, and Tools“, Alexander J. Mc Neil, Rüdiger Frey, and Paul Embrechts, Princeton University Press, 2015 (Revised Edition)*
- *Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Stølen, SpringerBri efs in Computer Science, page 91*
- *Fundamentals of Risk Management: Understanding, Evaluating ul Hopkin, Kogan Pa ge, 2022*
- *Cyber-Risk Management, Atle Refusal, Bjørnar Solhaug and Ketil Stølen, SpringerBri efs in Computer Science, page 95*
- *Risk Assessment and Decision Analysis with Bayesian Networks, Norman Fenton, M artin Neil, CRC Press (Taylor & Francis Group), 2018*
- *Cyber-Risk Management, Atle Refusal, Bjørnar Solhaug and Ketil Stølen, SpringerBri efs in Computer Science, page 92*
- *Quantitative Risk Management: Concepts, Techniques, and Tools“, Alexander J. McN eil, Rüdiger Frey, and Paul Embrechts, Princeton University Press, 2015.*

End of Week 5

We have come to the end of lecture 5.

Thanks for staying with me till the end of lecture 5.

NEXT LECTURE we will look at-;

Week 6: Risk Mitigation Strategies

See u There!