Course: IT RISK MANAGEMENT AND CONTROL

Week 6

Topic: Risk Mitigation Strategies

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 5 Material
2. Understanding Risk Mitigation
3. Risk Mitigation Options
   - Avoidance, Reduction,
   - Transfer, Acceptance
4. Developing Risk Mitigation Plans
5. Implementing Controls

Week 5 Review

Before we start looking at week 6 material, let’s first do a quick review of our previous lecture material (week 5)

In week 5, we discussed the following;

Week 5 Review

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.

Week 5 Review

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

Week 5 Review

3.Risk Prioritization

- ✓ The process of ranking identified risks based on their potential impact and l ikelihood of occurrence which helps organizations to attend to the most criti cal 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×Detecti on
- ✓ Higher RPN values indicate more critical risks, which should be prioritized or mitigated first.

Week 5 Review

4. Risk Prioritization Techniques cont..

3. SWIFT (Structured What-If Technique)

- It involves brainstorming parties with "What if?" questions about possibl e risks, their 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 be nefits of reducing the risk and the risks with the highest benefit-to-cost r atio are given first priority.

5. Delphi risk prioritization Technique

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

Week 5 Review

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.
- ✓ Through simulations, organizations can see which risks have the greatest chance of causing significant problems, allowing them to mitigate those ri sks first.

5. Risk Appetite and Tolerance

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

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

Understanding Risk Mitigation Strategies

Definition.

- IT risk mitigation strategies are options used for reducing the im pact and likelihood of risks associated with technology, data, an d information systems.
- These strategies are designed to protect an organization’s IT i nfrastructure, ensure business continuity, and safeguard data a gainst cyber threats, hardware failures, software issues, and hu man error.
- Effective risk mitigation helps organizations avoid operational di sruptions, financial losses, reputational damage, and legal com plications.

Risk Mitigation Options

- Lets talk about IT risk mitigation options;

1. Risk Avoidance

- Risk avoidance involves changing business practices or elim inating specific activities that could introduce risks.
- In IT, such activities may include;

➢ Not adopting risky technology:

- If a particular technology or software is known to have vulner abilities, a company may decide not to use it.

Risk Mitigation Options cont..

1. Risk Avoidance cont…

➢ **Avoiding non-essential integrations:**

- If integrating systems increases the risk of data breaches or o perational failures, the company should avoid certain connecti ons.
- While risk avoidance eliminates the threat entirely, it may not always be practical as it could mean missing out on opportunit ies or business advantages.

Risk Mitigation Options cont..

2. Risk Reduction

- Risk reduction focuses on minimizing the impact or likelihood of risks.
- This is the most commonly used strategy in IT and involves implementing controls and safeguards.

Key approaches to Risk Reduction

a) Applying Technical Controls which include;

- **Firewalls and Intrusion Detection Systems (IDS)**

Firewalls prevent unauthorized access to a network, while ID S monitor network traffic for suspicious activity, helping to redu ce the risk of cyberattacks.

- **Encryption.**

Encrypt sensitive data to ensure that even if it is intercepted, it cannot be easily read by unauthorized parties.

Key approaches to Risk Reduction

a) Applying Technical Controls cont…

- **Add Multi-Factor Authentication (MFA).**

This adds an extra layer of security beyond just passwords, thus reducing the risk of unauthorized access.

- **Perform patch Management.**

Regularly apply security patches and updates to software a nd systems to close vulnerabilities that could be exploited b y attackers.

Key approaches to Risk Reduction

b. Implementing Procedural Controls

- **Access Controls**: Implementing role-based access control ens ures that employees only have access to the data and systems necessary for their roles, thus reducing the risk of internal data breaches.
- **Change Management Processes:** A formal change in manage ment process ensures that changes to IT systems are carefully planned, tested, and reviewed to avoid introducing new risks.
- **Data Backup and Recovery:** Regular backup data to ensure t hat critical data can be restored in the event of hardware failure , data corruption, or ransomware attacks.

Key approaches to Risk Reduction

c. Security Awareness Training

- **Employee Training:** Since human error is a major source of IT risk, training employees to recognize phishing attempts, follow secure password practices, and adhere to data security protocols is critical.
- **Simulated Attacks:** Conducting simulated phishing attacks or social engineering tests can help identify employees who might be vulnerable and need additional training.

Risk Mitigation Options cont..

3. Risk Transfer

- Risk transfer involves shifting the risk to another party, typically t hrough insurance or outsourcing.

Strategies used in Risk Transfer include;

- **Cybersecurity Insurance.**
  - This helps to protect against the financial costs associated with data breaches, ransomware attacks, and other cyber incidents.
  - Cyber insurance policies typically cover costs like legal fees, dat a recovery, regulatory fines, and customer notification.

Risk Mitigation Options cont..

3. Risk Transfer cont…

- **Outsourcing IT Functions;**

Some organizations outsource certain IT functions, such as data storage or cybersecurity, to specialized third-party provi ders.

This transfers some of the risk to the service provider, who may be better equipped to manage it.

Risk Mitigation Options cont..

4. Risk Acceptance

- Risk acceptance is the decision to accept a certain level of risk without taking specific actions to mitigate it.
- This strategy is usually chosen when the cost of mitigating the risk outweighs the potential impact or when the risk is deemed low enough to not warrant immediate action.

Example:

- A company might accept the risk of occasional downtime on a non-critical system, choosing not to invest in expensiv e high-availability solutions.
- Risk acceptance requires continuous monitoring to ensure that the risk level remains acceptable over time.

Risk Mitigation Options cont..

4. Risk Sharing

- Risk sharing is a strategy where multiple parties share the res ponsibility for managing a specific risk.

Risk sharing normally takes place in;

- **Collaborative Security Efforts:**

Partnering with other companies, industry groups, or government agencies to share threat intelligence and best practices for cyber security.

- **Joint Ventures:**

Sharing the risks (and benefits) of IT projects with partners, such as in collaborative software development or joint IT infrastructure projects.

- Risk sharing helps to distribute the financial and operational im pact of risks across multiple parties.

Developing Risk Mitigation Plans

- Developing Risk Mitigation Plans is a critical step u nder risk mitigation strategies, aimed at outlining sp ecific actions and processes to reduce the impact o r likelihood of identified risks.
- A Risk Mitigation Plan is essentially a documented approach that details how an organization will handl e and reduce risks that could negatively affect its op erations, projects, or objectives.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans.

1. Identify Risks;

- Before creating a mitigation plan, it's essential to identify a nd document all potential risks that could impact the organi zation or project.
- This step usually involves conducting a risk assessment to understand the nature of each risk.
- Risks could be internal eg; system failures, human error or external (e.g., regulatory changes, cyber threats).

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

2. Assess Risks;

- After identifying the risks, assess their likelihood and pot ential impact.
- This helps in prioritizing risks, determining which ones r equire immediate action, and how severe their consequ ences could be.
- A common tool used in this stage is a risk matrix that cat egorizes risks based on their probability and impact (e.g. , low, medium, or high risk).

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

3. Select Mitigation Strategies;

- Based on the risk assessment, select appropriate risk mitig ation strategies to address each identified risk.
- These strategies generally fall into four main categories:
  - **Avoidance:** Altering processes or decisions to completel y avoid a specific risk.
  - **Reduction:** Implementing controls or measures to minimi ze the impact or likelihood of the risk.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

3. Select Mitigation Strategies cont….

- **Transfer:** Shifting the risk to a third party, typically throug h insurance or outsourcing.
- **Acceptance:** Acknowledging the risk and deciding not to take any action (usually for low-priority risks).

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

4. Develop Specific Mitigation Actions;

- For each risk, develop specific actions or risk respons e plans to mitigate its impact.
- These actions should be detailed, including what need s to be done, by whom, and within what timeframe.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

4. Develop Specific Mitigation Actions cont..

Examples;

Cybersecurity Risk: Installing firewalls, conducting regul ar security audits, and employee training help to reduce th e likelihood of a data breach.

Perform operational Risk: Implement redundancy syste ms e.g, backup power supplies to ensure business contin uity during outages.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

5. Assign Responsibilities.

- Assign clear roles and responsibilities for the implementatio n of each risk mitigation action.
- Identify the individuals or teams responsible for carrying out the tasks, monitoring the risk, and report the progress.

6. Set Timelines.

- Establish timelines for implementing the mitigation actions.
- This ensures that each step of the plan is executed on time and allows for tracking progress against deadlines.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

7. Resource Allocation.

- ✓ Determine the resources (financial, human, technological) required to implement the risk mitigation plan.
- ✓ Ensure that the necessary tools, staff, or budget are available to execute the plan effectively.

8. Develop Contingency Plans.

- ✓ In some cases, even after mitigation, a risk may still materialize.
- ✓ Therefore, a contingency plan outlines what steps to take if the risk event occurs despite the mitigation efforts.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

8. Develop Contingency Plans Cont...

Example: A contingency plan for a data breach might inv

olve immediately isolating the affected systems, notifying

affected users, and engaging incident response teams.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

9. Monitor and Review;

- Risk mitigation is an ongoing process.
- Regularly monitor the status of the risks and the effectiveness of the mitigation actions.
- Use key performance indicators (KPIs) and metrics to measure progress and determine if adjustments are needed.
- Schedule periodic reviews to ensure the mitigation plan remains relevant as new risks emerge or circumstances change.

Developing Risk Mitigation Plans cont…

Steps in Developing Risk Mitigation Plans cont….

10. Document the Plan;

- The entire risk mitigation process should be documente d thoroughly in a formal Risk Mitigation Plan.
- This document serves as a reference for the team and s takeholders, outlining the identified risks, chosen strate gies, actions, and responsibilities.
- It should also include information on how and when to r eport on risk mitigation progress and who the key decisi on-makers are.

Example: Implementing a Risk Mitigation Plan in IT

Assume that a company is concerned about the risk of cybe rattacks.

1. Identified Risk: A cyberattack could disrupt operations or lead to data breaches.

2. Mitigation Strategy: Risk reduction (implement technical and procedural controls).

3. Perform Actions:

- Install firewalls and intrusion detection systems (technic al control).
- Regularly update and patch systems (technical control).
- Conduct employee training on phishing attacks (proced ural control).

Example: Implementing a Risk Mitigation Plan in IT

4. Assign responsibility: The IT security team is responsible f or implementing these actions, and the Chief Information Office r (CIO) is responsible for oversee progress.

5. Set timeline: All actions to be completed within 6 months.

6. Create a contingency Plan: If a breach occurs, inform the i ncident response team to contain the breach, notify affected us ers, and restore affected systems.

- By following these steps, the company reduces its risk of cy berattacks and is prepared to handle them effectively if they occur.

Advantages of Developing a Risk Mitigation Plan

- **It encourages proactive Risk Management:** By planni ng ahead, organizations can reduce their chances of risk s getting critical issues.
- **Minimizes Financial Impact**: Well-planned mitigation ac tions can prevent or reduce financial losses.
- **Increases Operational Resilience:** Organizations can c ontinue functioning smoothly even when risks materialize , due to the contingency plans in place.
- **Improves Stakeholder Confidence:** Having a clear pla n reassures stakeholders (e.g., customers, investors) tha t risks are being managed effectively.

Implementing Controls

- Implementing Controls under risk mitigation strategies inv olves deploying specific actions, technologies, or procedu res to reduce the likelihood or impact of risks.
- The goal is to safeguard an organization’s operations, as sets, and information by continuously managing vulnerabil ities.
- Controls are categorized based on their purpose in the ri sk management process.

Implementing Controls cont..

Types of Controls:

1. Preventive Controls.

- These controls are designed to **prevent** risks from occ urring.
- They are active measures put in place to stop threats before they impact the system or process.

Example: Installing firewalls, enforcing strong password policies, and using multi-factor authentication to prevent unauthorized access.

Implementing Controls cont..

Types of Controls cont…

***2. Detective Controls*.**

- These controls focus on detecting risks or incidents as they happen or immediately after they have happened.
- The idea is to identify and alert the organization about the p otential threats so that corrective action can be taken immed iately.

Example: Using security monitoring systems, intrusion detecti on systems (IDS), and regular audit logs to detect abnormal ac tivities or breaches.

Implementing Controls cont..

Types of Controls cont…

3. Corrective Controls.

- These are reactive controls aimed at correcting issues or mi nimizing damage once a risk event occurs.
- They help restore systems to their normal state and reduce t he impact of the risk.

Example: Data backups, disaster recovery plans, and incident response procedures to restore operations after a cyberattack or system failure.

Implementing Controls

Types of Controls cont…

***4.* Physical Controls.**

- These controls involve physical measures to protect t he organization’s resources and infrastructure.

Example: Security cameras, biometric access control, a nd locked server rooms to prevent unauthorized physica l access to critical areas.

The process of Implementing Controls.

1. Identify Key Risks;

- ✓ Start by identifying the critical risks that require mitigation.
- ✓ This could be based on the risk assessment process, foc using on the highest priority risks.

2. Select Appropriate Controls;

- ✓ Choose the right types of controls (preventive, detective, corrective, or physical) based on the nature of the risk an d the organization's goals.
- ✓ Prioritize controls that offer the best cost-benefit balance.

The process of Implementing Controls.

3. Deploy Controls;

- ✓ Implement the selected controls across the organization.
- ✓ This may involve installing new technology, updating procedure s, or providing training to staff to ensure they understand and fo llow the controls.

The process of Implementing Controls.

4. Test and Monitor.

- After deployment, continuously monitor the effectiveness of the controls to ensure they are mitigating the intended risks.
- This step involves regular testing, audits, and updates to the controls as needed.

5. Adjust and Improve.

- Over time, risks evolve, and new threats emerge.
- It’s important to update and refine controls to keep pace with these changes and ensure they remain effective.

The Importance of Implementing Controls

- **They reduce risk exposure ie. c**ontrols help minimize th e organization's exposure to risks, reducing the likelihood and severity of negative events.
- **They enhance operational resilience ie.** with strong con trols in place, organizations are better equipped to handle disruptions and recover quickly.
- **They improves compliance, ie.** implementing controls e nsures that the organization meets industry standards, le gal regulations, and internal policies.

Important conclusion

- Implementing controls is a core component of risk mitigati on, focusing on continuous, real-time, and corrective mea sures to manage risks effectively.
- These controls, when appropriately chosen and continuou sly monitored, protect an organization from significant thr eats and ensure continuity of operations.

Week 6 Summary

Today we have learnt about;

1. IT risk mitigation strategies

- Are options used for reducing the impact and li kelihood of risks associated with technology, dat a, and information systems

Week 6 Summary

2. Risk Mitigation Options

- ✓ Risk Avoidance
- ✓ Risk Reduction
- ✓ Risk Transfer
- ✓ Risk Acceptance

Week 6 Summary

3. Developing Risk Mitigation Plans

- A process aimed at outlining specific actions and processes to reduce the impact or likelihood of identified risks.

Steps;

1. Identify Risks.
2. Assess Risks.
3. Select Mitigation Strategies.
4. Develop Specific Mitigation Actions.
5. Assign Responsibilities.

Week 6 Summary

3. Developing Risk Mitigation Plans cont..

Steps Cont…

6. Set Timelines and Milestones.

7. Resource Allocation.

8. Develop Contingency Plans.

9. Monitor and Review.

10. Document the Plan.

Week 6 Summary

4. Advantages of Developing a Risk Mitigation Plan

- It encourages continuous risk management
- Minimizes Financial Impact
- Increases Operational Resilience
- Improves Stakeholder Confidence

Week 6 Summary

5. Implementing controls

This involves deploying specific actions, technologies, o
r procedures to reduce the likelihood or impact of risks.

6. Types of controls

- ***Preventive Controls.***
- ***Detective Controls*.**
- ***Corrective Controls.***
- **Physical Controls.**

Week 6 Summary

7. The process of Implementing Controls

1. Identify Key Risks

2. Select Appropriate Controls

3. Deploy Controls:

4. Test and Monitor.

5. Adjust and Improve.

.

Week 6 Summary

The Importance of Implementing Controls

- They reduce risk exposure
- They enhance operational resilience
- They improves compliance with standard laws/ rules

References

- *"Risk Management Framework: A Lab-Based Approach to Securing I nformation Systems"James Broad, Syngress, 2013*
- *Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Støle n, SpringerBriefs in Computer Science, page 97*
- *Fundamentals of Risk Management: Understanding, Evaluating ul Hop kin, Kogan Page, 2022*
- *"Project Risk Management: A Practical Implementation Approach", Mi chael M. Bissonette, Management Concepts Press, 2016*
- *Cyber-Risk Management, Atle Refusal, Bjørnar Solhaug and Ketil Støle n, SpringerBriefs in Computer Science, page 98*
- *Enterprise Risk Management: From Incentives to Controls", James La m, Wiley,2014.*

End of Week 6

We have come to the end of lecture 6.

Thanks for staying with me till the end of lecture 6.

NEXT LECTURE we will look at-;

Week 7: IT Control Frameworks

See u There!