Course: IT RISK MANAGEMENT AND CONTROL

Week 4

Topic: Risk Assessment and Analysis

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 3 Material
2. Understanding Risk Assessment and Analysis
3. Risk Assessment Methodologies
   - Qualitative vs. Quantitative Risk Assessment
4. Conducting IT Risk Assessments

Week 3 Review

Before we start looking at week 4 material, let’s first do a quick review of our previous lecture material (week 3)

In week 3, we discussed the following;

1. Identifying IT Risks

Risk; potential threats or vulnerabilities that could negatively impact an organizati on’s information technology systems, operations, and data.

Week 3 Review

Types of IT Risks

Cybersecurity Risks: potential dangers that could harm computers, networks , or data eg malware.

Operational Risks: weaknesses in a company's information technology syste ms eg software bugs.

Compliance and Legal Risks: potential problems that arise when a company fails to meet IT related laws, regulations, or internal policies.

Strategic Risks: potential problems that arise when a company's technology decisions or investments do not align with its long-term business goals.

Week 3 Review cont…

Financial Risks: potential financial losses caused by failures or inefficiencies in a company's IT systems

Reputational Risks: potential damage to a company's reputation caused by fail ures in its information technology systems

Project Risks: potential issues that can arise during an IT-related project that m ay hinder its success Eg project delays, cost over run

Physical and Environmental Risks: potential threats to a company’s IT system s caused by physical damage or environmental factors

Technological risks: potential problems that arise from the use of technology it self eg hardware malfunction

Week 3 Review cont…

2. The Risk identification process

- Establish IT Objectives
- Collect Relevant Information
- Identify Risk Sources
- Utilize IT-Specific Risk Identification Techniques
- Categorize Identified Risks
- Document Risks in a Risk Register
- Review and Update Regularly
- Review and Update Regularly

Week 3 Review cont…

3. Risk identification tools and techniques

Goal: To arrive at a collection of threat sources, threats, vulnerabilities, incide nts, and risks.

i) Risk Assessment Frameworks: (ISO 31000, NIST SP 800-30, COBIT) etc provide structured approaches for identifying risks by offering guidelines on a ssessing risk in IT environments**.**

ii) Extraction of information from System logs and Tests: Exploiting data, from event logs, intrusion detection systems and other monitoring tools, result s from penetration tests helps to identify any such information sources.

Week 3 Review cont…

Risk identification tools and techniques cont…

iii) Extraction from people who know the target of assessment: Depen ding on the assessment these people may include the developers of the sy stem, the maintenance team, operators of the system, the information secu rity officer and managers, etc

iv) Extraction of information from external experts: These may provide general valuable information about typical threat sources, vulnerability and attack types, and trends although they do not know the specific target of as sessment.

Week 3 Review cont…

Risk identification tools and techniques cont….

v) Extraction from people via Interviews and Surveys/questionnaires: The technique may use an open format with key themes or strict structured questions planned in advance to reveal specific vulnerabilities and concern s that might be overlooked.

vi) Brainstorming Sessions: The technique Involves bringing together tea ms from various departments with first-hand knowledge about specific parts or aspects of the target to generate ideas about potential risks which helps t o uncover risks that may not be apparent to individual stakeholders.

Week 3 Review cont…

Risk identification tools and techniques cont….

vii) Threat Modeling: The technique involves identifying potential thre ats to the system by mapping out how an attacker could exploit vulnera bilities. Eg PASTA (Process for Attack Simulation and Threat Analysis)

viii) Historical Data Analysis: The technique Involves reviewing past i ncidents, security breaches, to provide valuable insights into potential fu ture risks.

Week 3 Review cont…

Risk identification tools and techniques cont…

ix) Environmental Scanning: The technique Involves keeping an eye on external factors such as regulatory changes, technological advance ments, and emerging threats to identify risks that could impact the orga nization.

x) Control Assessment: The technique involves testing the effectiven ess of existing security controls and measures to assess whether they adequately mitigate identified risks

Week 3 Review cont…

4. Importance of IT Risk Identification.

- It enhances Security Posture.
- It improves Operational Resilience.
- It supports Compliance Efforts.
- It facilitates Informed Decision-Making.

Risk Assessment and Analysis

Qn: What is Risk Assessment and Analysis?

Risk assessment and analysis can be defined as the activities done with an ai m of understanding and documenting the risk picture for specific parts of a syst em or an organization.

- The assessment includes the estimation of the risk level, and the identificati on of options for risk treatment.
- The results from risk assessment serve as a decision basis for risk manage ment, including the decision for which controls and measures can be chosen to implement to mitigate risk.
- The risk assessment process is divided into five steps;

Understanding Risk Assessment

The Risk Assessment process

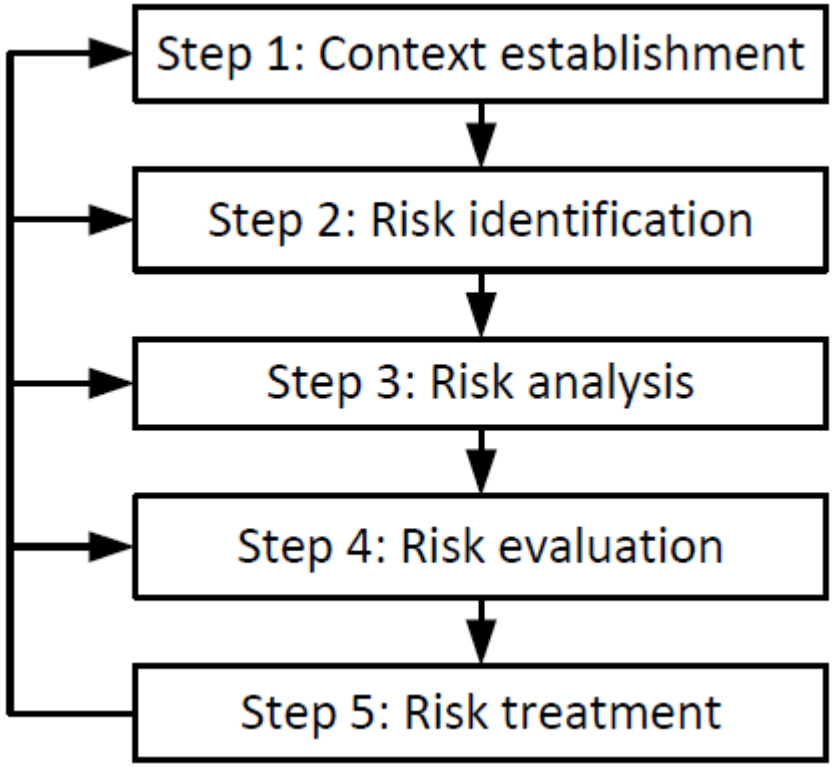

Fig 1: The Risk Assessment process [1]

Risk Assessment process cont…

Step 1. *Context Establishment*

- Context establishment is the first step in the risk assessment process which in volves the documentation of both the external and the internal context relevan t to the assessment in question.
- The **external context** includes the relationships with external stakeholders, a s well as the relevant societal, legal, regulatory, and financial environment.
- The **internal context** includes the relevant goals, objectives, policies, and cap abilities that may determine how risk should be assessed.
- This step defines the goals and objectives of the risk assessment, and therefo re requires the participation of decision makers.

Risk Assessment process cont…

Step 1. ***Context Establishment cont….***

- It is useful also to decide and clearly specify the desired scope and focu s of the assessment.
- The scope of the assessment is the extent of the risk assessment which defines what is held inside and outside of the assessment.
- The focus of the assessment is the main area of attention in any risk ass essment and the focus is within the scope of the assessment.
- The identification and documentation of the assets with respect to which the risk assessment is conducted is a crucial step in context establishme nt, and in defining the focus of the assessment.

Risk Assessment process cont…

Step 1. *Context Establishment cont…*

- However before asset identification is done, it is important to be specific about the party of the risk assessment by asking questions like;
    1. **Who are they (Party/organization)?**
    2. **What assets do they hold?**
    3. **How critical, important, or valuable are those assets held?**
    4. **To what degree do these assets require protection?**
- All the above can be determined only by considering the party.
- A risk assessment is typically conducted with respect to one party, but it is possible to allow for two or more.

Risk Assessment process cont…

- **Step 2.** ***Risk identification***
- Risk identification are the activities aimed at identifying, describing, and docu menting risks and their possible causes.
- In risk assessment, risk identification is done based on the description of the t arget of the assessment.
- Note: **The *target of assessment*** is the parts and aspects of the system that are the subject of the risk assessment.
- Note: **A *system*** is a set of related entities that forms an integrated whole and has a boundary to its surroundings.

Risk Assessment process cont…

Step 2. *Risk identification cont…*

- To perform risk identification, we must keep two things in mind.

    1. ***First:*** A risk is always associated with an incident.
    2. ***Secondly:*** There are three elements necessary for a risk to happen, ie; Asset, Vulnerability, and Threat.

- **An asset** refers to any valuable resource or component within an organization t hat is critical to its operations and success.
- **A vulnerability** is a weakness, flaw, or deficiency that can be exploited by a thre at to cause harm to an asset.
- **A threat** is an action or event that is caused by a threat source and that may lea d to an incident.
- **A threat source** is the potential cause of an incident.
- Without assets there is nothing to harm, without vulnerabilities there is no way to cause harm, and without threats there are no causes of harm.

Risk Assessment process cont…

Step 2. *Risk identification cont…*

- We therefore conduct risk identification with respect to the identified ass ets by identifying threats and understanding how the threats may lead to incidents (and thereby risks) by exploiting vulnerabilities.
- Examples of vulnerabilities may be insufficient staff training, lack of back -up copies of critical operator manuals etc
- The severity of a vulnerability depends on the threats that may exploit th em.
- Threats may lead to incidents, but in order to identify threats and underst and how they arise, we need to understand their initial causes ie; the thr eat sources.

Risk Assessment process cont…

Step 2. *Risk identification cont….*

- A threat source can be human or non-human ie natural source, and it ca n be tangible or intangible.
- Examples of human threat sources are intruders, thieves and negligent employees, while natural causes such as lightning or flood are non-hum an threat sources.
- Malware is an example of an intangible threat source.

Risk Assessment process cont…

Step 2. *Risk identification cont…*

- How a threat source causes a threat that can lead to a risk by exploiti ng vulnerabilities.

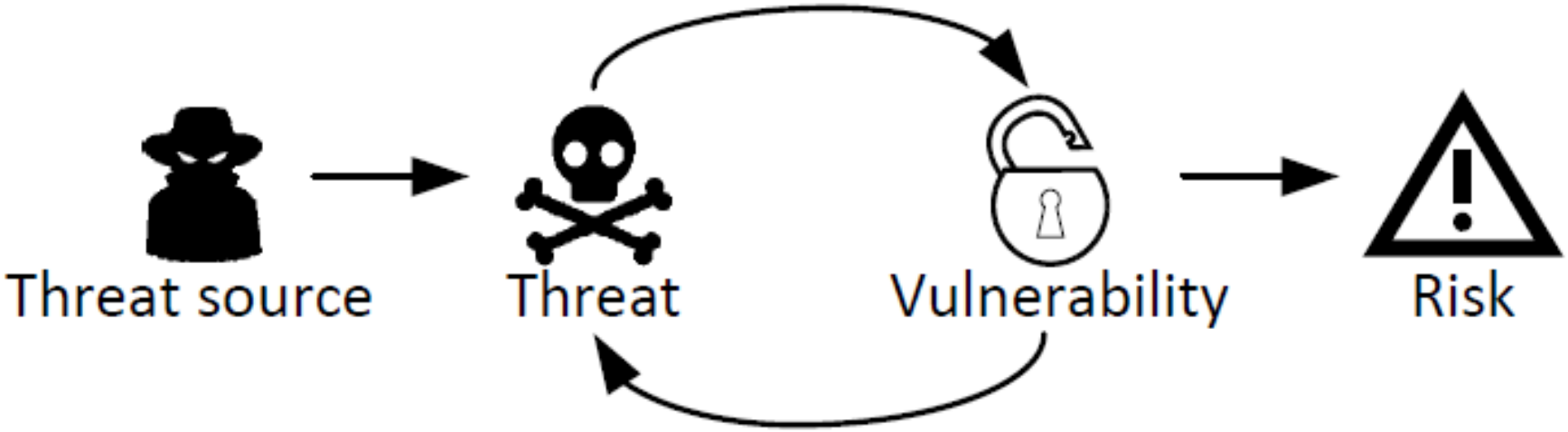

Fig 2. How threat sources lead to risks [5]

Risk Assessment process cont…

Step 2. *Risk identification cont….*

- According to figure 2, the arrow pointing forward illustrates that threat source s can lead to threats which eventually cause risks.
- During risk identification we seek to understand and document how this can happen with respect to the identified assets.
- In practice we often structure the risk identification by starting at one end an d working our way to the other end, for example, by first identifying potential incidents and then trying to understand how and why they can arise.

Step 2. *Risk identification cont….*

Risk identification Questions

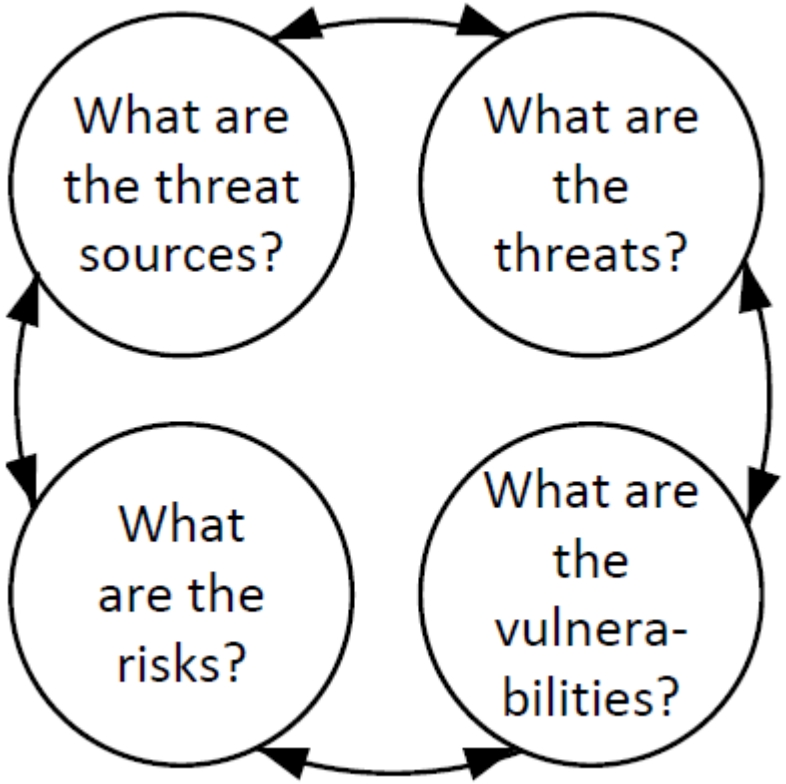

Fig 3: Risk Identification questions [5]

Risk Assessment process cont…

Step 2. *Risk identification cont….*

- As illustrated in figure 2, we can still go back and forth while gradually building the risk picture in our assessment by asking our selves different questions.
- For example, a threat that we identify for a given incident can trigger the identification of its source.
- The identified threat can also trigger us to quickly find out the vulnerabilities that this th reat may take advantage of.
- After identifying the vulnerability, we can also ask our selves the possible risks that the vulnerability may cause.
- We could still develop a question as what are the sources of all these risks formed, an d wat risks these sources are causing etc until we get back as shown in figure 3 above.

Risk Assessment process cont…

Step 2. *Risk identification cont….*

- Risk identification should be done in a clear and systematic manner by using tech niques for doing the identification, and applying suitable formats for describing and documenting the results.
- ***Reminder:*** The Techniques for risk identification include brainstorming, extraction from experts, interviews, environmental scanning, control assessment, gathering h istorical data etc.
- Risk assessors may also use modeling techniques such as event trees, Bayesian networks, attack trees, CORAS diagrams, or threat modeling to support the descri ption of risks and how they are related to threats and threat sources.
- N.B: Modeling techniques can describe risks by analyzing past data to find trends or behavior and be able to predict outcomes, thus enabling quick decision making.

Risk Assessment process cont…

Step 2. *Risk identification cont….*

- However, the identification technique to use depends on a variety of factors such as the desired level of detail, the available resources and the expertis e and experience of the risk assessors.
- Whatever techniques and level of detail are choose for the risk identificatio n and documentation, there is need to ensure that assessors describe all th e elements of the risk picture they need for the purpose and objectives of th e risk assessment.
- At the very least the documentation should include threat sources, vulnerab ilities, risks, and assets.

Risk Assessment process cont…

Step 3. Risk Analysis

- Risk analysis involves the activities that are aimed at estimating and deter mining the level of the identified risks.
- The risk level is derived from the combination of the likelihood and consequ ence.
- The objective of this step, therefore, is to estimate likelihoods and consequ ences for the identified incidents using the scales defined during context es tablishment.
- An incident represents one risk for each of the assets it harms, and we nee d to estimate the consequence for each of these assets.
- The impact or severity of an incident can be determined only by considerin g the party in question.

Risk Assessment process cont…

Step 3. ***Risk Analysis cont…***

- The consequence estimation should therefore be conducted by a walk-thro ugh of all identified incidents and assigning the estimates with the involvem ent of personnel representing the party or someone who can judge conseq uences on behalf of the party.
- Likelihood estimation is to determine the frequency or probability of incident s to occur by using the defined likelihood scale.
- This requires the use of techniques for gathering empirical data such as int erviews and brainstorming sessions to gather expert opinions, inspection of logs or other statistical and historical data etc

Risk Assessment process cont…

Step 3. *Risk Analysis cont…*

- Many of the risk-modeling techniques such as Bayesian networks, attack trees, and CORAS diagrams, also come with support for likelihood estimation and documentation.
- How we choose to model or document the risks during the risk identification may therefore have some implications on which techniques are available for the likelihood estimation.

Risk Assessment process cont…

Step 3. *Risk Analysis cont…*

- In risk analysis, the desired level of detail of the risk assessment and documentation is another important factor.
- Sometimes assessors may only be interested in the likelihoods of the incidents and make their best estimates directly for these events.
- However, they need to understand how risks are most likely to arise, and which threat sources are most important.
- In that case they should also try to estimate the likelihood that threat sources initiate threats, and what likelihood that such threats may lead to incidents

Risk Assessment process cont…

Step 3. *Risk Analysis cont…*

- This information will not only help to understand the most important threat s ources and vulnerabilities, but also to determine the likelihood of the resulti ng incidents.
- Once assessors have estimated the likelihood and consequences for each i ncident, they can calculate the risk level of all identified risks.

Risk Assessment process cont…

Step 4. Risk Evaluation

- Risk evaluation involves the activities that deal with the comparison of the risk a nalysis results with the risk evaluation criteria to determine which risks should be considered for treatment.
- In principle this step is quite straightforward given the risk estimates and evaluati on criteria.
- For example, if the assessors have specified the risk evaluation criteria using th e risk matrix, they simply plot each risk into the matrix to determine the risk level.
- However, because the risk evaluation is a decision point in the overall risk asses sment process, assessors take time to confirm the risk evaluation criteria and co nsolidate the risk estimates.

Risk Assessment process cont…

Step 4. *Risk Evaluation cont…*

- Decision makers and other personnel involved in the risk assessment often gai n new knowledge and ideas about the risks and their consequences and asses sors must therefore make sure that the initially defined criteria are still appropri ate.
- For the consolidation of the risk assessment results assessors focus on the ris k estimates that they are uncertain about, and where this uncertainty implies d oubt about the actual risk level.
- Assessors need to investigate the identified risks to see whether certain sets of risks should be aggregated and evaluated as a single risk.
- This helps to avoid the pitfall of accepting a set of risks that individually are no n-critical and unacceptable in combination.

Risk Assessment process cont…

Step 4. *Risk Evaluation cont…*

- A final recommendation for the risk evaluation is to group risks that share ele ments in common.
- The shared elements in common may include threat sources, threats, vulne rabilities, assets etc and these risks may be treated by the same means.
- Therefore, in preparation for the risk treatment and to facilitate cost-efficient t reatment, assessor usually go through the identified risks and group them a ppropriately.

Risk Assessment process cont…

Step 5. Risk Treatment

- Risk treatment means the activities aimed at identifying and selecting mean s for risk mitigation and reduction.
- A ***treatment*** is an appropriate measure to reduce risk levels.
- Following principles, assessors should seek to treat all risks that are unacce ptable, but in the end this is a question of cost and benefit, no matter the ris k level.
- If a low risk is very cheap to eliminate, assessors might do so even if the ris k in principle is acceptable.
- And, similarly, if the cost of treating a very high risk is unbearable there may be no other option than to accept it.

Risk Assessment process cont…

Step 5. ***Risk Treatment cont…***

- The risk treatment activity, therefore, should involve both the identification and the analysis of treatments.
- The treatment identification can be done similarly to the risk identification, for example via brainstorming or by the use of available lists and repositor ies.
- The selection of which treatments to implement should be the result of an analysis of the costs and benefits of the identified treatments.
- The analysis should take into account that some treatments can create n ew risks, and that some groups of treatments can reduce the effect of eac h other.

Risk Assessment process cont…

Step 5. ***Risk Treatment cont…***

- There are four main options for risk treatment, namely-; risk reduction, risk retention, risk avoidance, and risk sharing.
- Risks may be reduced by reducing the likelihood or consequence of in cidents.
- To do this, options to remove threat sources, to reduce the severity of v ulnerabilities, and reduce the likelihood of threats by other means are s ought.

Risk Assessment process cont…

Step 5. *Risk Treatment cont…*

- Risk retention is to accept the risk by informed decision. This is typicall y an option for risks that are acceptable according to the risk criteria, or risks that are too costly to treat given the alternative options.
- Risk avoidance is simply to avoid the activity that gives rise to the risk i n question, which sometimes is the only option for unacceptable risks.
- Risk sharing is to transfer the risk or parts of it to another party, for exa mple, by insurance or sub-contracting.

Risk assessment Methodologies

- Risk assessment methodologies are processes used to identify, analyze, an d evaluate risks in order to manage or reduce them.
- They help organizations to understand potential dangers, their likelihood, an d their impact.

Risk assessment methodologies 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 elimina te risks.

- Different risk assessment methods like qualitative, quantitative, or hybrid ap proaches, can be used depending on the situation.

Qualitative vs. Quantitative Risk Assessment

- Qualitative and Quantitative Risk Assessments are two approaches used to evaluate risks
- The difference between Qualitative and Quantitative IT Risk Assessment lies in how they measure and evaluate risks.

1. Qualitative Risk Assessment:

- Qualitative risk assessment involves evaluating risks based on expert judgment, experience, opinions, and descriptions rather than relying on numeric data.
- Since the methodology relies on expert opinions, brainstorming sessions, risk matrices, and experience etc, we therefore say the method is subjective.

Qualitative vs. Quantitative Risk Assessment

- Qualitative risk assessment methodology often uses categories of scales such as ‘hi gh, medium, low, minor, moderate, severe etc to describe the likelihood and impact o f risks.
- Qualitative risk assessment is easier and faster to perform than quantitative risk asse ssment as it helps to prioritize risks for more detailed analysis and mitigation.

Tools & Methods:

- **Risk Matrices:** A matrix that plots risk likelihood against impact to prioritize risks.
- **Risk Registers:** A document that records identified risks, their assessment, and any action plans.
- **SWOT Analysis:** Analyzing strengths, weaknesses, opportunities, and threats to ass ess risk.

Qualitative vs. Quantitative Risk Assessment

Benefits of Qualitative risk assessment

- The methodology is simple and quick to conduct.
- It is good for getting an overall understanding of risks.
- The methodology requires less data and fewer resources.
- Easy for teams without specialized risk analysis training.

Limitations of Qualitative risk assessment

- The methodology is not very precise, thus difficult to compare risks objectively.
- It is subjective and therefore results can be biased.
- It does not provide precise numeric estimates of risks.
- It is less effective for highly complex projects which require detailed risk quantification.

Qualitative vs. Quantitative Risk Assessment

2. Quantitative Risk Assessment:

- Quantitative risk assessment describes risks with numbers and data.
- It focuses on using numerical data to evaluate risks, providing measurable e stimates of probability, impact, and overall risk levels.
- The method is highly data driven thus it requires high-quality, reliable data to perform effectively.
- The data is based on measurable data like past incidents, financial losses, e tc.
- The methodology relies on numerical data, historical records, and statistical analysis.
- It often involves mathematical models, statistical techniques, and probabilisti c simulations, probabilities and statistics to calculate risk levels.

Qualitative vs. Quantitative Risk Assessment

Quantitative Risk Assessment cont….

It may use tools like fault tree analysis, Monte Carlo Simulations statistical models.

- Monte Carlo Simulations: A probabilistic method that uses random variables to simul ate a wide range of potential outcomes.
- Fault Tree Analysis (FTA): A top-down, deductive failure analysis that focuses on und erstanding the root causes of risks.
- Sensitivity Analysis: Examines how sensitive risk outcomes are to changes in variabl es.
- It provides detailed and specific information on the likelihood (expressed as a percen tage) and financial impacts (expressed in dollars, time, etc.).
- Expected Monetary Value (EMV): Uses probabilities and financial impact to estimate the average risk cost.

Quantitative Risk Assessment cont….

Benefits of Quantitative risk assessment

- The method is more precise and allows comparison of different risks with hard data.
- It is more accurate and gives detailed results.
- The methodology is useful for complex projects where accuracy is necessary.
- It facilitates cost-benefit analysis of risk mitigation options.

Limitations of Quantitative risk assessment

- It requires detailed and accurate data, data which may not always be available or co mplex to gather.
- It is time-consuming and resource-intensive.
- It requires specialized expertise and tools.

Qualitative vs. Quantitative Risk Assessment

Qn: When do we use each of the methodologies discussed?

1. Qualitative:

- The method is best to used in initial risk identification, small projects, or in sit uations when data is limited.

2. Quantitative:

- The method is ideal for complex and big projects where accurate risk estima tes are crucial (e.g., large construction, engineering, or financial projects).

NOTE: (Mixed Approach)

- In many cases, organizations use both qualitative and quantitative assessme nt methodologies together.
- They start with a qualitative approach to prioritize risks before performing a d etailed quantitative analysis on the most critical risks.

Qualitative vs. Quantitative Risk Assessment

Important Conclusion.

- Both methods play a crucial role in risk assessment.
- Qualitative is more descriptive and easy to implement but le ss precise.
- Quantitative provides exact measurements and data-driven i nsights but needs more effort and information.
- Therefore, both methods can complement each other in risk assessments to give wonderful results.

Conducting IT Risk Assessments

- Conducting an IT Risk Assessment is a structured process to identify, ev aluate, and mitigate potential threats to an organization's information tec hnology infrastructure.
- This process helps ensure the security, availability, and integrity of syst ems, data, and services.
- Below are the key steps involved in conducting an IT risk assessment:

Conducting IT Risk Assessments

1. Identify Assets

Key Questions:

1) What are the most critical assets that support business operations?
2) Which assets store or process sensitive data?
3) Which assets are essential for business continuity?

Steps;

- The first step is to identify all critical IT assets that need protection.
- Assets may include, hardware, servers, computers, and network devices.
- Identify existing software such as applications, operating systems, and databases
- Data such as customer information, intellectual property, and financial records.
- Define personnel like employees, third-party vendors, and contractors.
- Processes such as business workflows and critical IT operations in organization.

Conducting IT Risk Assessments

2. Identify Threats

- Once the assets are identified, the next step is to identify the potential threats to those assets.
- Threats can be internal or external, and they include a wide range of risks such as Cybersecu rity threats, Malware, phishing, denial of service (DoS) attacks, and hacking.
- Identify physical threats such as theft, vandalism, natural disasters, and equipment failure.
- Identify human threats such as Insider threats, human error, malicious actions by employees or contractors.
- Identify technical failures such as Software bugs, system crashes, and hardware failure.
- Define regulatory threats such as non-compliance with laws like GDPR, HIPAA, or PCI-DSS.

Key Questions:

1) What are the potential sources of these threats?
2) Are there any known vulnerabilities in the existing systems?

Conducting IT Risk Assessments

3. Identify Vulnerabilities

Key Questions:

1) Are there known vulnerabilities in the hardware, software, or network?
2) Are security controls like firewalls, intrusion detection systems, and antivirus u p to date?
3) Is sensitive data encrypted while being exchanged or where it is saved?

Steps;

- Vulnerabilities are weaknesses in systems, processes, or configurations that c ould be exploited by threats.
- Identifying the Vulnerabilities is crucial for understanding where protection may be lacking.

Conducting IT Risk Assessments

3. Identify Vulnerabilities cont…

Common vulnerabilities include:

- Outdated software ie; Lack of patches and updates.
- Weak access controls ie; Poor password policies, inadequate role-based access.
- Unencrypted data ie; Sensitive data stored or transmitted in plaintext.
- Improper configurations ie; Misconfigured firewalls, open ports.
- Lack of monitoring ie; Inadequate logging and real-time threat detection.

Conducting IT Risk Assessments

4. Assess the Risk Impact and Likelihood

Key Questions:

1) What would be the financial impact of a data breach or system downtime?
2) How likely is it that a cyber attack or natural disaster will occur?

Steps;

- Assess the potential impact and likelihood of each identified threat exploiting a vulnerability.
- This involves evaluating both qualitative and quantitative aspects of risks.

Conducting IT Risk Assessments

4. Assess the Risk Impact and Likelihood cont…

- **Impact:** Determine the potential consequences of a risk event, such as financial loss, data breaches, service interruptions, or legal penalties.
- **Likelihood:** Determine the probability that a given threat will successfu lly exploit a vulnerability.

Methods:

- **Qualitative risk assessment**: Use risk matrices to categorize risks into lo w, medium, or high levels of impact and likelihood.
- **Quantitative risk assessment**: Use metrics like monetary value, downtim e estimates, or number of records exposed to calculate potential risk expos ure (e.g., in dollar terms).
- Mixed Approach.

Risk Assessment process cont…

5. Prioritize Risks

Key Questions:

1) Which risks pose the greatest threat to business continuity?
2) How can resources be allocated to mitigate the highest-priority risks?

Steps;

- Once risks are identified and assessed, the next step is to prioritize them based on their likelihood and impact.
- This helps in allocating resources effectively to address the most critical risks first.
- **High-risk:** High-impact, high-likelihood risks that need immediate attention eg-; out dated software on critical systems.
- **Medium-risk:** Risks that could have a significant impact but are less likely to occur.
- **Low-risk:** Risks with low impact and low likelihood that may not need immediate a ction but should be monitored.

Conducting IT Risk Assessments

6. Develop Risk Mitigation Strategies

Key Questions:

1) What security controls can be implemented to mitigate high-impact ris ks?

2) How can we ensure that these controls are sustainable and scalable?

Steps;

- For each high-priority risk, develop a mitigation plan that outlines specifi c actions to reduce or eliminate the risk.
- Risk mitigation strategies typically fall into four categories ie;

1. Risk avoidance: Eliminate the risk entirely e.g; shut down a system th at has been identified with vulnerabilities or risks.

Conducting IT Risk Assessments cont...

6. Develop Risk Mitigation Strategies cont…

2. Risk mitigation: Implement controls to reduce the likelihood or impact eg; install security patches, and configure firewalls.
3. Risk transfer: Shift the risk to a third party eg by purchasing cybersecurity insur ance or outsourcing IT operations by hiring external companies or service provi ders to manage all or part of an organization's IT functions.
4. Risk acceptance: Acknowledge and accept the risk if the cost of mitigation is to o high relative to the benefit eg low-probability risks with minor impact.

Examples.

- Perform technical controls: Firewalls, encryption, intrusion detection systems, acc ess controls.
- Implement procedural controls like implement security policies, incident response plans, and disaster recovery plans.
- Physical controls like secure facilities, biometric access, and video surveillance.

Conducting IT Risk Assessments cont..

7. Document and Communicate the Findings

Key Questions:

1) How will the assessment findings be communicated to leadership and IT teams?
2) Are stakeholders aware of their roles and responsibilities in risk management

Steps;

- All identified risks, their assessments, and mitigation strategies should be documente d in a Risk Register or Risk Management Plan.
- This document should be communicated to stakeholders, including IT teams, manag ement, and compliance officers, to ensure awareness and accountability.

Key Components of a Risk Register include;

- Identified risks.
- Likelihood and impact of each risk.
- Risk owners (responsible individuals).
- Mitigation measures and timelines.
- Monitoring and review process.

Conducting IT Risk Assessments cont..

8. Implement and Monitor risk mitigation plans

Key Questions:

1) Are the selected security controls effectively mitigating the identified risks?
2) Are there any emerging risk that need to be addressed?

- Implement the selected mitigation strategies and continuously monitor their effec tiveness.
- This involves ensuring that security controls are working as intended and that ne w risks are identified and addressed promptly.

Activities;

- **Monitor system logs**: Use security information and event management (SIEM) t ools to monitor for anomalies or threats.
- **Regular audits**: Conduct periodic reviews to ensure compliance with security po licies and regulatory requirements.
- **Penetration testing:** Perform vulnerability assessments and penetration tests to evaluate system security.

Conducting IT Risk Assessments cont..

9. Review and Update the Risk Assessment

Key Questions.

1. How often should the IT risk assessment be reviewed and updated?
2. What new risks have emerged since the last assessment?

What to know;

- IT risk assessments are not one-time tasks but rather they need to be regularly reviewed and updated as the organization's IT environment, threat landscape, or regulatory requirements evolve.
- Regularly updating risk assessment ensures that new vulnerabilities are identified, and existing controls remain effective.

Conducting IT Risk Assessments cont..

9. Review and Update the Risk Assessment cont…

Why perform Updates?

- Changes in IT infrastructure eg existence of new systems, cloud migration etc.
- New regulatory requirements.
- Emerging cyber threats such as zero-day vulnerabilities, advanced persistent threats etc.
- Post-incident reviews eg; after a security breach or failure.

Conducting IT Risk Assessments

Conclusion:

- Conducting an IT risk assessment involves a structured process of id entifying and analyzing risks, followed by the implementation of effect ive mitigation strategies.
- Regular reviews, communication with stakeholders, and ongoing mo nitoring are essential to ensuring the security and reliability of IT syst ems.
- This approach helps organizations to reduce vulnerabilities, prevent c yber attacks, and maintain compliance with legal and regulatory stan dards.

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 context relevant to the assessment in question.

Step 2. *Risk identification*

✓ Risk identification are the activities aimed at identifying, describing, and 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 th e level of the identified risks.

Step 4. *Risk Evaluation*

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

Step 5. *Risk Treatment*

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

Week 4 Summary

2. Risk assessment methodologies

Risk assessment methodologies are processes used to identify, analyze, and evaluate risks in o rder 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, experience, 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..

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

Conclusion: Conducting an IT risk assessment involves a structured process of identifying and analyzing risks, followed by the implementation of effective mitigation strategies.

Thanks for being with me till the end;

Next week we will look at;

Week 5: Risk Evaluation and Prioritization

See You There!

References

- *[1]Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Stølen, SpringerBriefs in Computer Science pages 14*
- *[2] Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Stølen, SpringerBriefs in Computer Science pages 16*
- *[3] Cyber-Risk Management, Atle Refusal, Bjørnar Solhaug and Ketil Stølen, SpringerBriefs in Computer Science page 17*
- *[4] Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Stølen, SpringerBriefs in Computer Science page 18*
- *[5] Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Stølen, SpringerBriefs in Computer Science page 19*
- *[6] Managing risks in Information systems Darril Gibson and Andy Igonor, jon es and Barttlet Learning Company.*