Course: IT RISK MANAGEMENT AND CONTROL

Week 3

# Topic: Identifying IT Risks

Lecturer: Ninyikiriza Deborah Lynn

## TODAYS outline

1. Review of week 2 Material
2. Identifying IT Risks (Types of IT Risks)
3. The IT risk Identification process
4. IT Risk Identification Tools and Techniques
5. The Importance of Identifying IT Risks

# Week 2 Review

Before we start looking at week 3 material, let's first do a quick review of our previous lecture material (week 2)

In week 2, we discussed the following;

## 1. IT Risk Management Frameworks and Standards

- The processes and tools that organizations use to manage and mitigate the potential risks associated with the use of technology.

# Week 2 Review cont..

## 2. Major IT Risk Management Frameworks

- NIST Risk Management Framework (RMF)
- COBIT (Control Objectives for Information and Related Technology)
- ISO/IEC 27005
- FAIR (Factor Analysis of Information Risk)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

# Week 2 Review cont..

## 3. Major IT Risk Management Standards

- 1. ISO/IEC 27001
- 2. ISO 31000
- 3. PCI DSS (Payment Card Industry Data Security
- Standard)
- 4. ITIL (Information Technology Infrastructure Library)

# Key Components of IT Risk Management

- **Risk Identification:** Recognizing potential risks to IT assets such as systems, data, and infra structure.
- **Risk Assessment**: Evaluating the potential impact and likelihood of identified risks. Typically, this involves qualitative and quantitative methods.
- **Risk Mitigation**: Implementing controls to reduce the impact or likelihood of the risk occurring .
- **Risk Monitoring:** Continuously monitoring and reviewing the risk environment to adapt to ch anging threats and vulnerabilities.
- **Risk Governance:** Establishing clear accountability, policies, and oversight for IT risk manag ement across the organization

# Identifying IT Risks

## Reminder: How do we define IT Risk?

**Risk:** Likelihood that a loss may happen.

**IT Risk:** Likelihood that an event that harms or reduces the value of IT assets may happen.

- ✓ These risks or potential threats or vulnerabilities could negatively impact an organization's info rmation technology systems, operations, and data.
- ✓ These risks can rise from various sources and take different forms.

Lets talk about are the major types of IT risks;

# TYPES OF IT RISKS

## 1. Cybersecurity Risks

- Cybersecurity risks are potential dangers that could harm computers, networks, or data.
- These involve acts in which someone might access sensitive information or disrupt digital systems.

**NOTE**: Therefore, they are threats to the safety and privacy of one's online information.

# Cybersecurity Risks cont…

**Examples explained:**

- **Malware:** Viruses, worms, ransomware, and other malicious software which can corrupt data or disable systems.
- **Phishing:** Social engineering attacks by the use of emails where attack ers trick individuals into revealing sensitive information by pretending to be from legitimate organizations**.**
- **Denial of Service (DoS) Attacks**: A type of network attack which results into an interruption of network service to users, devices or applications.
- **Hacking and Unauthorized Access:** An act by attackers to exploit syst em vulnerabilities/ weaknesses with an aim of gaining unauthorized acc ess manipulate data, or disrupt services.
- **Insider Threats:** Acts to carry out harm or steal data, originating from wi thin an organization, typically by individuals who have authorized access to sensitive systems, data, or networks.

# TYPES OF IT RISKS cont..

## 2. Operational Risks

- Operational IT risks refer to the potential problems or disruptions that arise from failures or weaknesses in a company's information technology syste ms, processes, or infrastructure.
- These risks can include system crashes, data breaches, cyberattacks, soft ware bugs, or human errors that negatively impact a business's operations
- Essentially, we define them as the risk of IT-related issues causing financi al loss, reputational damage, or operational delays.

# Operational Risks cont...

**Examples explained;**

- **System Downtime:** Interruptions in service due to hardware or software failure, often impacting business continuity**.**
- **Human Error:** Mistakes by IT staff or users, such as incorrect configurations or accidental data deletion.
- **Third-party Provider Failure:** Relying on external vendors or service providers (e.g., cloud services) that may experience is sues or outages.
- **Inadequate Backup Procedures:** Insufficient or ineffective d ata backup strategies, which can result in data loss.

# TYPES OF IT RISKS cont..

## 3. Compliance and Legal Risks

- Compliance and legal IT risks refer to the potential problems that arise when a company fails to follow laws and regulations, or internal policies related to information technology.
- These risks include penalties, lawsuits, or reputational damage if the co mpany does not properly protect data, adhere to cybersecurity standard s, or comply with privacy regulations.

- Simply, it's the risk of legal consequences from not meeting IT-related rules and obligations.

# Compliance and Legal Risks cont...

**Examples explained;**

- **Non-Compliance:** Failure to meet industry regulations e.g; GDPR (General Data Protection Regulation) or internal policies, leading to fines and legal consequences**.**
- **Data Privacy Breaches:** Inadequate protection of personal or sensitive data, resulting in legal liabilities.
- **Licensing Issues:** Using software or tools without proper licenses, leading to legal action or fines.

# TYPES OF IT RISKS cont..

## 4. Strategic Risks

- Strategic IT risks refer to the potential problems that arise when a company’s technology decisions or investments do not align with i ts long-term business goals.
- This can happen if outdated or poorly chosen technologies limit th e company’s growth, competitive advantage, or ability to innovate.
- Basically, it's the risk of technology choices negatively impacting a company’s overall strategy and success.

# Strategic Risks cont.……

**Examples explained;**

- **Outdated Technology:** A company continues to use aging systems that ar e no longer supported or scalable and lack integration with newer technolog ies which leads to increased maintenance costs or reduced effectiveness.
- **Failed Digital Transformation:** A company may invest heavily in digital tr ansformation projects like cloud platforms, implementing AI solutions wit hout proper planning, leadership, or alignment with  long term business goals.
- **Failure to Innovate:** Not adopting new technologies when necessary whi ch undermines customer trust, and disrupts business operations thus ca using a competitive disadvantage.

# TYPES OF IT RISKS cont..

## 5. Financial Risks

- Financial IT risks refer to potential financial losses caused by failures or inefficiencies in a company's IT systems.
- These risks can come from data breaches, system downtime, IT project cost overruns, or fraud.
- Thus, it's the risk of losing money due to technology-related issues or poor IT management.

# Financial Risks cont…

**Examples explained;**

- **Cost Overruns:** IT projects exceeding budgets, impacting the financial health of the organization**.**
- **Poor Return on Investment (ROI):** Refers to a situation where the fin ancial returns or benefits gained from IT investments are lower than ex pected or inadequate in comparison to the amount of money, time, or r esources that were put into it leading to financial losses.
- **Unplanned Expenditures:** Unexpected costs related to emergency re pairs, security breaches, or equipment failures.

# TYPES OF IT RISKS cont..

## 6. Reputational Risks

- Reputational IT risks refer to the potential damage to a company's reputation caused by failures in its information technology systems.
- This can happen through events like data breaches, cyberattacks, or poor service reliability, which can lead to a loss of trust among c ustomers, partners, or the public.
- Essentially, it's the risk of a company's image and credibility being harmed due to IT-related issues.

# Reputational Risks cont..

**Examples explained;**

- **Data Breaches:** If a company's IT systems are hacked and customer data is leaked, it can lead to loss of trust and a damaged reputation.
- **Website Outages:** If a company's website or online services are down frequently, it creates frustration for customers and may lead them to se ek alternatives.
- **Slow or Unreliable Services:** If a business's app or system is slow or unreliable, customers may share negative reviews, affecting the busin ess's image.
- **Poor Data Handling:** Mismanagement of customer data, like losing re cords or mishandling sensitive information, may cause strong negative reactions or criticism from the public in response to a particular event o r action.

# TYPES OF IT RISKS cont..

## 7. Project Risks

- IT Project risks refer to potential issues that can arise during an IT-related pr oject that may hinder its success.
- These risks include delays in software development, technical glitches, bud get overruns, or a lack of skilled personnel.
- Therefore, they are obstacles that an IT project may face that prevent it fro m being delivered on time, within the budget, or meeting the desired goals.

# Project Risks cont..

**Examples explained;**

- **Project Delays:** Missed deadlines for key IT initiatives due to resource shortages or unforeseen issues.
- **Failure to Meet User Expectations:** Delivering IT solutions that don’t meet the needs of the end users, reducing adoption rates or effectiveness.
- **Project Scope Change:** Expanding project requirements without proper management, leading to delays or failure**.**

# TYPES OF IT RISKS cont..

## 8. Physical and Environmental Risks

- Physical and environmental IT risks refer to the potential threats to a company’s IT systems caused by physical damage or environmental factors.
- These risks include incidences like fires, floods, power outages, or equipment damage that can disrupt or destroy technology infrastructure.
- Therefore, it's the risk of IT systems being harmed by physical events or natural disasters.

# Physical and Environmental Risks cont..

## Examples explained;

- **Natural Disasters:** Events like floods, earthquakes, or fires that can physical ly damage IT infrastructure.
- **Power Outages:** Loss of electricity can result in system downtime or hardwa re damage if there are inadequate backup systems.
- **Theft or Vandalism:** Intentional damage to hardware or infrastructure, witho ut the owner’s or data center's consent, affects the appearance, functionality, or value of the targeted property.

# TYPES OF IT RISKS cont..

## 9. Technological Risks

- Technological IT risks refer to potential problems that arise from the use of technology itself.
- These risks include system failures, outdated software, hardware malfuncti ons, or vulnerabilities in new technologies.
- In short form, it's the risk of technology not working as expected, leading t o disruptions or security issues.

# Technological Risks cont..

**Examples explained;**

- **Hardware Failures:** Components like servers, storage devices, or networking equipment malfunctioning.
- **Incompatibility:** Integrating systems or software that don't work well together, causing disruptions.
- **Software Bugs:** Flaws in code that can disrupt operations or create vulnerabil ities.

# RISK IDENTIFICATION

- Risk identification aims at arriving at a collection of threats, threat source s, vulnerabilities, incidents, and risks.
- Since cyber-systems are computer based, there is normally a lot of data and information available.
- This data may be from event logs, intrusion detection systems and other monitoring tools, vulnerability scanners, results from penetration tests or other kinds of security tests, source code reviews, and so on.
- Besides other various techniques, Identifying risks also involves full expl oitation of such information.

# RISK IDENTIFICATION CONT…..

**Qn**: **Who performs Risk identification?**

- Typically, Risk identification is done in close cooperation with maintenance personnel, technical managers, security managers, or others who have detailed knowledge about the technical infrastructure.

# THE RISK IDENTIFICATION PROCESS

## What is IT Risk Identification process?

- IT risk identification process is a systematic approach that specifically focuses on identifying potential risks associated with information technology systems, projects, and infrastructure.
- Since modern organizations rely on technology, this process is crucial for safeguarding data, ensuring system integrity, and maintaining operational continuity.

# Risk Identification process

**1. Establish IT Objectives**

- Clearly define the IT goals and objectives aligned with the organization’s overall strategy.
- Understanding what you want to achieve helps to identify risks that could impede these goals

**2. Collect Relevant Information**

- Gather data and insights related to the IT environment in the particular or ganization such as ;
- Current IT infrastructure; System architecture; Previous incidents and his torical data; Regulatory compliance requirements etc

# Risk Identification process cont..

### 3. Identify Risk Sources

- Identify potential IT Risk sources, such as;
  - **Technical Risks**: Hardware and software failures, network outages, and compatibility issues.
  - **Human Factors**: User errors, insider threats, and lack of training.
  - **Security Risks:** Cyberattacks, data breaches, and vulnerabilities in appli cations.
  - **Process Risks**: Inadequate change management, poor project manage ment, and insufficient documentation.

# Risk Identification process cont..

**4. Utilize IT-Specific Risk Identification Techniques**

- Employ various methods to uncover risks, in IT environments such as;
  - **Threat Modeling**: Analyze potential threats to systems and data.
  - **Vulnerability Assessments**: Identify weaknesses in the IT infrastruct ure that could be exploited.
  - **Penetration Testing**: Simulate cyberattacks to discover security gaps.
  - **interviews and Brainstorming Sessions**: Involve IT staff and stakeh olders to discuss potential risks

# Risk Identification process cont..

**5. Categorize Identified Risks**

- Organize identified risks into categories to facilitate management and response, such as;
  - **Operational Risks**: Risks affecting the daily operations of IT services.
  - **Compliance Risks**: Risks associated with failing to meet legal and regulatory requirements
  - **Strategic Risks**: Risks impacting the long-term goals of the IT department.

**6. Document Risks in a Risk Register**

- Create a risk register to document each identified IT risk, including;
  - Description of the risk
  - Potential impact and likelihood of occurrence
  - Responsible parties for monitoring and managing the risk
  - Existing controls or mitigation measures in place.

# Risk Identification process cont..

**7. Review and Update Regularly**

- Continuously monitor and review the risk register to ensure it reflects the current IT l andscape and any changes in technology, processes, or business objectives.
- Regular updates may include:
  - New technology implementations
  - Changes in regulatory requirements
  - Lessons learned from incidents

**8. Communicate Findings to Stakeholders**

- Share identified risks and the risk management strategy with relevant stakeholders, including IT staff, management, and other departments, to ensure collective awaren ess and alignment.

# RISK IDENTIFICATION TOOLS &TECHNIQUES

## 1. Risk Assessment Frameworks:

- These tools an be used as effective tools for identifying IT risk s by providing a structured way to analyze potential threats, v ulnerabilities, and impacts to an organization's technology sys tems or IT environments
- The frameworks may incude NIST, ISO 27001) etc which can provide structured approaches for identifying risks.

# How frameworks work?

1) **They help in Systematic Identification:**

   Frameworks guide through a step-by-step process to identify diff erent types of risks based on the organization's operations.

2) **They help in assessing Vulnerabilities:**

   By pinpointing to areas where the IT system is vulnerable, such as outdated software, poor access control, or weak network secu rity measures.

3) **They help in prioritizing Risks:**

   By ranking risks by their potential impact and likelihood of occurr ence, helping to focus on the most critical threats.

# How frameworks work?

4) **They perform a Comprehensive Coverage:**

   By covering a wide range of IT environments, ensuring that no important area s (like cloud security, third-party risks, or internal system vulnerabilities) are ov erlooked.

5) **They perform a consistent Approach:**

   By providing a consistent approach for evaluating risks across different syste ms and departments ensuring nothing is missed and everyone follows the sa me standards.

6) **They follow compliance and Best Practices:**

   By ensuring that they are aligned with industry best practices and regulatory r equirements thus reducing the chance of overlooking key risks.

# RISK IDENTIFICATION TOOLS & TECHNIQUES CONT…

## 2. Extraction of information from System logs and Tests

- Data and information available from event logs, intrusion detection systems and other monitoring tools, vulnerability scanners, results from penetration tests or other kinds of security tests, source code reviews can be fully exploited.
- This can be done to identify the specific sources of relevance, and to select from these sources only those elements that are relevant to the assessment.
- A systematic walk-through of the target description, including the attack surface and assets, is performed in order to identify any such information sources to be used.
- These sources are mapped to the relevant parts of the target assessment.

# System logs and Tests cont…

**Example;**

- In an electric company, any test results concerning the metering termin al interface to the Internet can be mapped to the particular part of the at tack surface.
- These test results then help us to identify vulnerabilities and threats for attacks through this interface.

# RISK IDENTIFICATION TOOLS &TECHNIQUES CONT…

## 3. Extraction from people who know the target of the assessment

- people who know the target of assessment well from their particular view points can be used to identify risks.
- Selection of these people depends on the assessment eg; if an electrifica tion company, these people may include the developers of the central sy stem or metering nodes, the maintenance team, operators of the central system, the information security officer, and managers of the distribution system operator.
- Potential electricity customers may also be used.

# RISK IDENTIFICATION TOOLS & TECHNIQUES CONT…

## 4. Extraction from external experts

- External experts may also possess valuable knowledge for the assessme nt although they may not know the specific target of assessment.
- They may provide general knowledge about typical threat sources, vulner abilities, attack types, and trends.
- When interacting with external experts, risk identifiers must not disclose c onfidential information unless this has been approved by the party or orga nization on whose behalf the assessment is done.

# RISK IDENTIFICATION TOOLS & TECHNIQUES CONT…

## 5. General extraction from people via Interviews and Surveys/questionnaires:

- Interviews can be arranged to gather information from people about perceived risks.
- They may follow a strict structure where all questions are planned in advance, but an open format with key themes to be covered may be used but with considerable openness to additional inputs from the interviewee.
- Interviews may provide very valuable information, but must be used with care.
- They are quite resource intensive and depend on the right persons being willing and available to participate.
- Carrying out the interviews and compiling and aggregating results also require skill from the risk assessors.

**Advantage:** The technique can reveal specific vulnerabilities and concerns that might be overlooked.

# RISK IDENTIFICATION TOOLS & TECHNIQUES CONT…

## 7. Brainstorming Sessions

- These involve bringing together teams from various departments to generate ideas about potential risks.
- This collaborative approach can uncover risks that may not be apparent to individual stakeholders.
- This involves gathering together relevant stakeholders and personnel with first-hand knowledge about specific parts or aspects of the target to contribute to the identification process in meeting sessions.

# Brainstorming cont...

- In brain storming sessions, personalities of participants play a maj or role, and there is a danger that the more outspoken persons do minate while others hardly contribute, thus not all views are broug ht forward.
- Individual participants may also take the opportunity to pursue the ir own agenda and focus only on issues that are within their own a rea of interest.
- The discussion can digress off topic and that the available time m ay not be properly distributed between the topics to be covered.

# Brainstorming cont...

- Therefore Successful brainstorming requires a highly skilled risk assessor to lead the sessions and plans must be made in advance on how to structure a nd guide the discussions.
- **Technique Advantage:** The participants are able to discuss and to follow u p on each other’s ideas and think of ways in which threats can exploit this v ulnerability
- **Technique disadvantage:** gathering together all the participants for a brain storming session may also be difficult

# 8. Threat Modeling

- This technique involves identifying potential threats to the system by mapping out how an attacker could exploit vulnerabilities.
- Common methods include;
  - STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
  - PASTA (Process for Attack Simulation and Threat Analysis

# RISK IDENTIFICATION TOOLS & TECHNIQUES CONT…

## 9. Historical Data Analysis.

- The technique involves reviewing past incidents, security breaches, and near misses to provide valuable insights into potential future ris ks.
- Organizations can analyze trends and patterns in past data to predi ct and mitigate similar risks in future.

# 10. Environmental Scanning.

- Environmental Scanning is a threat identification technique that involves Keeping an eye on external factors such as regulatory changes, technological advancements, and emerging threats so as to identify risks that could impact the organization.
- It also involves monitoring industry news, threat intelligence reports, and changes in laws or regulations.

# 11. Control Assessment

- Control Assessment Risk identification technique involves evaluating exis ting security controls and measures that can help identify gaps or weakne sses in the current risk management approach.
- This technique involves testing the effectiveness of controls and assessin g whether they adequately mitigate identified risks.

# The Importance of IT Risk Identification

Risk identification is important to organizations in a way that ;

- **It enhances Security Posture:** Continuous identification of risks helps to protect sensitive data and IT assets from threats.
- **It improves Operational Resilience:** Understanding potential incidences allows organizations to prepare and respond effectively.
- **It supports Compliance Efforts:** Identifying risks related to compliance ensures that organizations meet legal and regulatory requirements.
- **It facilitates Informed Decision-Making:** By providing a clearer underst anding of IT risks, enabling better strategic planning and investment decis ions by organizations.

# Conclusion

- Identification of IT risks is very important to organizations.
- By systematically identifying IT risks, organizations can implement effective risk management strategies to minimize negative impacts and ensure the security and reliability of their technology systems/ IT assets.

# Week 3 Summary

**1. Identifying IT Risks**

**Risk;** potential threats or vulnerabilities that could negatively impact an organization’s information t echnology systems, operations, and data.

**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 systems eg software bugs

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

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

# Week 3 Summary cont….

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

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

**Project Risks:** potential issues that can arise during an IT-related project tha t may hinder its success Eg project delays, cost over run

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

**Technological risks:** potential problems that arise from the use of technolog y itself eg hardware malfunction

# Week 3 Summary 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 Summary cont….

## 3. Risk identification tools and techniques

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

**i) Risk Assessment Frameworks: (**ISO 31000, NIST SP 800-30, COBIT) etc provides structured ap proaches for identifying risks by offering guidelines on assessing risk in IT environments**.**

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

# Week 3 Summary cont….

## Risk identification tools and techniques cont…

**iii) Extraction from people who know the target of assessment:** Depending on the assessment t hese people may include the developers of the system, the maintenance team, operators of the syst em, the information security officer and managers, etc

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

# Week 3 Summary 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 advanc e to reveal specific vulnerabilities and concerns that might be overlooked.

**vi) Brainstorming Sessions:** The technique Involves bringing together teams from vario us departments with first-hand knowledge about specific parts or aspects of the target to g enerate ideas about potential risks which helps to uncover risks that may not be apparent to individual stakeholders.

# Week 3 Summary cont….

**Risk identification tools and techniques cont….**

**vii) Threat Modeling:** The technique involves identifying potential threats to the system by mapping out how an attacker could exploit vulnerabilities. Eg PASTA (Process for Attack Simu lation and Threat Analysis)

**viii) Historical Data Analysis:** The technique Involves reviewing past incidents, security bre aches, to provide valuable insights into potential future risks.

# Week 3 Summary cont….

**Risk identification tools and techniques cont….**

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

**x) Control Assessment:** The technique involves testing the effectiveness of existing secu rity controls and measures to assess whether they adequately mitigate identified risks

# References


- Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug and Ketil Stølen, SpringerBriefs in Compu ter Science
- Managing risks in Information systems  Darril Gibson and Andy Igonor, jones and Barttlet  Learning Company.