Week 2

Topic: IT Risk Management Frameworks and Standards

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 1 Material
2. IT Risk Management Frameworks and Standards
3. Key IT Risk Management Frameworks
4. Key IT Risk Management Standards

Week 1 Review

Before we start looking at week 2 material, let's first do a quick review of our previous lecture material (week 1)

In week 1, we discussed the following;

a) **Information Technology**;

Information technology which we defined as the use of computer systems to manage, process, protect, retrieve and exchange information.

b) **Components of Information Technology**

We looked at the key components of information Technology such as hardware, software, cloud computing, databases etc, and how each of them performs a specific purpose to meet a common goal.

Week 1 Review cont….

c) **Risk**

We defined a risk as a likelihood that a loss will happen.

d) **IT Risk**

A quantitative measure of the potential damage caused by a threat, a vulnera bility or by an event that affects the set of IT assets owned by an organization.

e) **IT Risk management**

IT risk management also known as information security risk management is the process of reducing IT related risks.

Week 1 Review cont….

f) **Objectives IT Risk management**

- To Identify Risks
- To Assess Risks
- To Mitigate Risks
- To Monitor and respond to risks
- To Communicate Risks
- To Ensure Compliance

g) **Importance IT Risk management**

- It protects sensitive information
- It maintains business continuity
- It improves Strategic Decision-Making
- It enhances Operational Efficiency,

Week 1 Review cont…

Key concepts and definitions

h) Security threat

An occurrence, situation or activity that has the potential to cause harm to the IT assets.

i) Vulnerability

Also known as weakness is a lack of safeguard that may be exploited by a threat, causing harm to IT assets**.**

J) Risk exposing events/risk events

These are incidences that expose the organization to potential harm, dama ge, or loss, by exploiting vulnerabilities in information technology systems, processes, or practices.

Week 1 Review cont…

Key concepts and definitions cont.…

K) Malicious events

These are actions taken with an intention to cause harm or damage to an org anization's information systems, data, or operations.

L) Information Security

- **Confidentiality:** The protection against unauthorized access, appropriati on, or use of assets.
- **Integrity:** The protection against unauthored manipulation, modification, or loss of assets.
- **Availability**: The protection against blockage, or limitation of benefit from an asset that is owned.

Week 1 Review cont…

m) IT risk management Life Cycle;

Made of five processes;

Risk identification or Identification of threats & vulnerabilities

1. Risk assessment also known as risk analysis.
2. Risk mitigation planning.
3. Risk mitigation implementation.
4. Evaluation of the mitigation effectiveness.

Understanding Definition

- **How do we define IT Risk Management Frameworks and Standards?**
- These refers to the processes and tools that organizations use to manage and mitigate the potential risks associated with the use of technology.
- These risks can affect business operations, regulatory compliance, data integrity, and the conf identiality, availability, or security of information systems.
- A strong IT risk management framework helps organizations identify, assess, manage, and mi tigate these risks systematically. This involves policies, processes, governance structures, an d tools that ensure that risks are managed appropriately.

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

Major IT Risk Management Frameworks and Standards

1. ISO/IEC 27001 (Information Security Management System)
2. ISO 31000 (Risk Management Guidelines)
3. NIST Cybersecurity Framework (CSF)
4. COBIT (Control Objectives for Information and Related Technologies)
5. ITIL (Information Technology Infrastructure Library)
6. FAIR (Factor Analysis of Information Risk)
7. OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation)
8. ISO/IEC 27005

Frameworks and Standards

Frameworks

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

Standards

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

IT RISK MANAGEMENT FRAMEWORKS

- Several frameworks have been developed to guide organizations through the process of IT Risk Management.
- These frameworks differ slightly in focus but share common goals of protecting inform ation assets and ensuring business continuity.

1. NIST Risk Management Framework (RMF)

- NIST was developed by National Institute of Standards and Technology (NIST)
- This framework focuses on providing a structured process for integrating risk manage ment into the system development lifecycle (SDLC).
- It is widely used in both government and private sectors.

NIST RFM Cont...

How does NIST work?

Step 1. Categorize Information Systems: Determine the security impact level of systems based on the types of data it processes, stores, or transmits.

- ✓ **Benefit:** After understanding the data, one can be able to assign a security c ategory to guide the level of protection needed.

Step 2. Select Security Controls. Choose the appropriate security controls to protect the system based on its categorization.

- ✓ Always refer to NIST Special Publication 800-53, which provides a catalog of security controls organized according to their impact levels (low, moderate, hi gh) and ensure to match the controls to the specific needs of the system and organization.
- ✓ **Benefit:** Helps to select a tailored set of security controls that will mitigate ide ntified risks.

NIST RFM Cont…

How does NIST work?

Step 3. Implement Security Controls: Apply the selected security controls to the sys tem and ensure they are properly configured and functioning**.**

- ✓ Document how the controls are deployed in system policies, procedures, and config urations.
- ✓ **Benefit:** At this step you have a system with the necessary security controls in plac e, documented in an implementation plan.

Step 4. Assess Security Controls: Test the effectiveness of the controls to ensure th ey meet the organization’s security requirements.

- ✓ Conduct assessments through testing, reviews, and audits to verify functionality, by using tools like vulnerability scans, penetration tests and document assessment res ults.
- ✓ **Benefit:** At this step you have an assessment report detailing the effectiveness of t he controls and any risks that remain.

NIST RFM Cont…

How does NIST work?

Step 5. Authorize Information Systems: Determine if the system can operate at an acceptable risk level based on the results of the security control assessment.

- ✓ This can be done by the authorizing official through reviewing the assessment report and evaluating the risk posture.
- ✓ This helps to decide if the system can be Authorization to Operate (ATO) or denial of Authorization (DOA), or asked to carry out requiring further mitigation.
- ✓ **Benefit:** At this step the system is either approved for operation or requires further remediation.

NIST RFM Cont…

How does NIST work?

Step 6. Monitor Security Controls: Continuously track the performance and effectiveness of security controls throughout the system's lifecycle.to ensure t hat there are no new risks.

- ✓ This can be done by conducting regular assessments of the system, for risk s, vulnerability scans, and updates to the security plan to detect changes th at could affect security, and thus Implement corrective actions when control s are found to be ineffective.
- ✓ **Benefit:** At this step you have a continuously monitored system with an up dated risk profile and adaptive security measures.

Why use NIST?

- **Uses a risk-based approach:** The RMF ensures that security decisions a re made based on the specific risk profile of each system.
- **Ensures compliance:** It helps organizations comply with government reg ulations.
- **Uses a structured Process:** It provides a clear, step-by-step process for managing information security and risks.
- **Performs continuous Monitoring:** It emphasizes ongoing risk assessme nt and adjustment, which is crucial for maintaining cybersecurity in dynami c environments.

Conclusion: NIST integrates risk management with compliance activities, m aking it ideal for highly regulated industries.

Frameworks CONT….

2. COBIT (Control Objectives for Information and Related Technology)

IT is a governance and management framework developed by ISACA (In formation Systems Audit and Control Association)

✓ COBIT focuses at providing governance and management framework that h elps organizations to align IT with business objectives while managing risks.

Key Concerns of COBIT:

1. Governance and Management Objectives: Structured around key process es that provide guidance on managing IT risks and aligning IT strategies with e nterprise goals.

2. Control Objectives: These are specific practices that help ensure IT risk m anagement, business value, and compliance with laws.

COBIT RMF Cont.…

How does COBIT work? (COBIT RMF Process)

1. Risk Identification.

✓ Identify the potential IT risks that could affect the organization's ability to achieve it s business goals. This includes both internal and external threats.

2. Risk Assessment.

✓ Evaluate the likelihood and impact of each risk using qualitative or quantitative met hods. The assessment helps prioritize risks based on their potential harm to the or ganization.

3. Risk Response.

✓ Choose how to handle each risk, whether by mitigating, transferring, accepting, or avoiding it. Ensure that risk responses align with the organization's risk appetite an d tolerance.

COBIT RMF Cont.…

4. Risk Monitoring.

- ✓ Continuously monitor the risks and the effectiveness of controls in plac e by tracking key indicators to detect changes in risk levels or the emer gence of new risks.

5. Risk Reporting.

- ✓ Regularly report about IT risks to senior management, ensuring that ris k-related information is available for decision-making and resource allo cation.

COBIT RMF Cont.…

Benefits of Using COBIT RMF:

- **It aligns IT with Business Goals** by ensuring that IT risk management i s directly responsible for achieving the organization's overall business ob jectives.
- **COBIT performs comprehensive Risk Management** and provides a ho listic approach to identifying, assessing, and mitigating risks across all IT processes and technologies.
- **It enhances proactive Risk Management by** helping organizations to a nticipate and manage IT risks before they become significant threats thus improving resilience.
- **It uses well standardized Controls and governance practices** that ali gn with industry standards thus increasing compliance with regulations**.**

COBIT RMF cont…

Important Conclusion:

- The COBIT Risk Management Framework (RMF) provides a structured and comprehensive approach of managing IT-related risks in alignment with business goals.
- It does so by integrating IT risk management into enterprise risk management (ERM) and emphasizing continuous monitoring.
- This helps organizations stay resilient and manage risks in advance in this rapidly changing technology environment.

Frameworks CONT….

3. ISO/IEC 27005

- It is an international standards developed by International Organization for Sta ndardization (ISO) and International Electrotechnical Commission (IEC)
- ISO/IEC 27005 Risk Management Framework focuses on Information Security Management Systems (ISMS).
- The frame work specifically, provides detailed guidelines for implementing risk management in the context of information security, complementing the overall security governance framework established by ISO/IEC 27001.
- It helps organizations to identify, assess, and manage risks to their informatio n assets to ensure the confidentiality, integrity, and availability of information.

Frameworks CONT….

How does ISO/IEC 27005 manage risks?

The frame work uses a6 steps approach to manages information security risks;

Step 1: Context Establishment

- Defines the organizational context in which risk management will take place, in cluding external and internal factors
- **Benefit:** Step 1 gives a clear understanding of the organization's environment, critical assets, and the criteria for managing and assessing risks

Step 2: Risk Identification

- Identifies potential security risks that could impact the organization’s informatio n systems.
- **Benefit:** Step 2 pinpoints a list of risks to the organization’s information assets, linked to potential threats, vulnerabilities, and their consequences.

Frameworks CONT…

ISO/IEC 27005 Approach to managing risks

Step 3: Risk Assessment

- Evaluates the identified risks to determine their likelihood and potential impact on the organization.
- **Benefit.** Step 3 ranks the risks by their severity and prioritizes those requiring im mediate attention.

Step 4: Risk Treatment

- Decides how to address each identified risk, selecting an appropriate strategy bas ed on the organization's objectives and risk appetite.
- **Benefit.** Outlines a risk treatment plan that details the actions to be taken, respon sible parties, resources needed, and deadlines for managing each risk.

Frameworks CONT….

ISO/IEC 27005 Approach to managing risks cont….

Step 5: Risk Communication

- Ensures clear and continuous communication about risks and the risk manageme nt process across the organization.
- **Benefit.** At this step the organization is well-informed and everyone understands t he risks and their roles in managing them.

Step 6: Risk Monitoring and Review

- Continuously monitors the risk environment and the effectiveness of risk treatment measures to ensure that risks remain within acceptable limits.
- **Benefit.** At this step the organization has a risk management process that adapts t o changing threats and vulnerabilities, with updated risk assessments and treatme nt plans as needed.

Frameworks CONT…

- **Benefits of using ISO/IEC 27005 RMF:**
- **Comprehensive Risk Management:** Provides a structured and standardized a pproach to identifying, assessing, and treating risks.
- **Flexible in nature:** It can be applied to any organization, regardless of size, ind ustry, or the nature of its IT assets**.**
- **Aligns with International standards:** Aligns with ISO/IEC 27001, ensuring org anizations follow a consistent and integrated approach to information security.
- **Business focus:** Helps organizations align their risk management activities wit h broader business objectives and regulatory requirements.
- **Adaptability:** Its regular monitoring and review processes allow organizations t o adapt to evolving threats and changing business environments.

Frameworks CONT….

4. FAIR (Factor Analysis of Information Risk)

- FAIR framework is a quantitative model designed to help organizations und erstand, measure, and manage information security and operational risks.
- It uses Data-driven and analytical approach, allowing organizations to asse ss and prioritize risks in monetary terms (such as financial losses).
- It provides a systematic way to quantify and compare risks, which can hel p in decision-making, especially around cybersecurity and IT investments.
- Its focuses on analyzing how frequently risks might occur and their potentia l financial impact.

Frameworks CONT…

- **How FAIR Works cont..**

Step 1: **Identify the Scenario**

- Define the specific risk scenario you want to analyze eg a cyberattack on the c ompany's customer database.

Step 2: Evaluate Threat Event Frequency (TEF)

- Determine how often the threat is likely to act against the asset in the scenario.

Step 3: Assess Vulnerability

- Calculate the likelihood that the threat will succeed when it acts.

Step 4: Determine Loss Event Frequency (LEF)

- Using vulnerability data, estimate how often the loss event will occur.

Frameworks CONT…

How FAIR Works cont..

Step 5: Quantify Loss Magnitude

- Evaluate both primary and secondary losses associated with the event

Step 6: Calculate and Express Risk

- The final step is to calculate the overall risk by combining the Loss Event Frequency (LEF) with the Loss Magnitude.
- This gives a quantitative risk value that can be expressed in terms of mon etary loss or other metrics relevant to decision-makers.

Frameworks CONT….

Why choose FAIR?

- **Quantitative Risk Analysis:** Allows organizations to measure risk in financial terms eg potential loss in dollars, making it easier to compare and prioritize risks.
- **Informed Decision-Making:** Provides a clearer basis for decision-making. This hel ps organizations allocate resources more effectively to mitigate the most significant risks**.**
- **Alignment with Business Goals:** Helps security teams to communicate risks to bu siness leaders (financial impact). This bridges the gap between technical staff and b usiness stakeholders.
- **Scalability and Flexibility:** Can be applied to a wide range of risk scenarios, from c yberattacks and data breaches to physical security risks.
- **Improved Risk Prioritization:** By quantifying risk factors, organizations can prioritiz e which risks to address first based on their potential financial impact and likelihood.

Frameworks CONT….

5. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability E valuation)

OCTAVE was Developed by Carnegie Mellon University's Software Eng ineering Institute.

It is a risk-based framework that focuses on the organization's assets, id entifying critical information assets and associated risks.

Frameworks CONT…

How OCTAVE works;

- **Asset Identification**: Identify and prioritize critical assets.
- **Risk Identification**: Assess the vulnerabilities and threats associated with these assets.
- **Risk Mitigation**: Develop a strategy to mitigate or transfer the identified ri sks.

- **Benefits:** OCTAVE is designed for organizational self-assessment and is pa rticularly useful for organizations that want a less formal and more flexible a pproach to risk management.

IT RISK MANAGEMENT STANDARDS

- Several standards complement the frameworks mentioned above.
- These standards offer prescriptive guidelines and methodologies that can be adopted to ensure consistency and compliance.

1. ISO/IEC 27001

Purpose: Provides requirements for establishing, implementing, maintaining, an d improving an Information Security Management System (ISMS).

It provides a systematic approach to securing sensitive information by managing people, processes, and IT systems.

It focuses on risk management as a critical component of an organization's info rmation security management strategy.

Core Focus: Continuous improvement and alignment with risk management pra ctices, making it ideal for regulatory compliance.

STANDARDS cont..

How ISO/IEC 27001 Standard works

1. Establishing the ISMS (Information Security Management System)

- The ISMS is a framework for managing information security risks, ensu ring the confidentiality, integrity, and availability of sensitive information.

2. Risk Assessment and Management

- Conduct a risk assessment to identify potential security risks (e.g., data breaches, insider threats, system failures).

STANDARDS cont..

How ISO/IEC 27001 Standard works

3. Select Security Controls

- Organizations can select which controls to apply based on their specific risks, though the implementation is often tied to the results of the risk as sessment.

4. Continual Improvement (Plan-Do-Check-Act)

- ISO/IEC 27001 follows the PDCA cycle (Plan-Do-Check-Act), ensuring continuous improvement of the ISMS.

STANDARDS cont..

How ISO/IEC 27001 Standard works

5. Documentation and Records

- The standard emphasizes thorough documentation of policies, processes, pr ocedures, risk assessments, controls, and corrective actions.

6. Perform Internal and External Audits

- Organizations seeking ISO/IEC 27001 certification undergo an external audit by an accredited certification body to verify that their ISMS meets the standar d's requirements.

7. Certification

- Once an organization successfully implements ISO/IEC 27001 and passes ex ternal audits, it can receive certification.

STANDARDS cont..

Why choose ISO/IEC 27001?

- **Improved Security Posture:** Ensures a strong security framework is in place to protect against cyber threats and data breaches.
- **Compliance:** Helps meet legal, regulatory, and contractual obligations r elated to data protection and privacy.
- **Reputation:** Enhances trust with customers and stakeholders by showi ng a commitment to securing information.
- **Risk Management:** Provides a structured approach to identify, assess, and mitigate information security risks.

STANDARDS Cont…

2. ISO 31000

- **ISO 31000** is an international standard for risk management that provid es a set of guidelines and principles for managing risks effectively.
- It is a more general risk management standard that can be applied to a ny type of organization, not just those focused on IT, regardless of size, industry, or sector, to identify, assess, and manage risks.
- Although it is not specific to IT, it is often used in conjunction with ISO 2 7005 for a comprehensive risk management strategy.

STANDARDS Cont…

Benefits of ISO 31000:

- **Holistic Risk Management**: It provides a comprehensive approach that inte grates risk management across all parts of an organization.
- **Enhanced Decision-Making:** Risk-informed decision-making leads to better strategic and operational outcomes.
- **Adaptability:** The framework is flexible and can be tailored to any organizati on's needs and risk environment.
- **Improved Governance**: By aligning risk management with corporate govern ance, ISO 31000 supports compliance and accountability.
- **Proactive Risk Management**: Helps organizations be proactive rather than reactive by identifying potential risks early and addressing them effectively.
- **Stakeholder Confidence:** Demonstrates that the organization has a structu red, responsible approach to managing risks, which can enhance the confid ence of customers, regulators, and investors.

STANDARDS Cont…

3. PCI DSS (Payment Card Industry Data Security Standard)

- **Purpose:** A compliance standard for organizations that handles credit c ard data.
- PCI DSS focuses on protecting cardholder data and involves specific IT r isk management practices to ensure data security.
- **It uses** Security controls for protecting payment systems from breaches and fraud.

STANDARDS Cont…

4. ITIL (Information Technology Infrastructure Library)

The ITIL (Information Technology Infrastructure Library) standard is a set of best practices for deliv ering IT services effectively and efficiently

It provides a framework that helps organizations manage their IT services to align with business ne eds, improve service quality, and ensure consistent delivery

- It includes aspects of risk management, particularly in service continuity, incident management, and security management.
- It focuses at operational risk management related to IT services, ensuring business continuity, a nd minimizing the impact of incidents on the organization.

STANDARDS Cont…

ITIL Cont…

ITIL organizes its practices into five main stages of the service lifecycle:,

- 1. **Service Strategy**

Define the strategy for IT services, including planning and identifying ho w IT services can support business goals**.**

2. Service Design

- Create and design new IT services or modify existing services to meet current or future needs.

3. Service Transition

- Ensure that newly designed or changed services are effectively imple mented into the live environment

STANDARDS Cont…

4. ITIL (Information Technology Infrastructure Library)

4. Service Operation

- Deliver and manage IT services at agreed-upon service levels, while ensuring busines s continuity and stable performance

5. continual Service Improvement (CSI)

- Continuously evaluate and improve IT services and processes based on performance data and customer feedback.

ITIL Cont…

Benefits of ITIL

- **Improved Service Delivery:** ITIL ensures that IT services are aligned with business needs and delivered with high quality.
- **Efficiency and Consistency:** The standard standardizes processes redu cing redundancy and streamlining IT operations.
- **Risk Management:** By focusing on managing incidents, problems, and ch anges effectively, ITIL helps reduce service disruptions and the associated risks.
- **Customer Satisfaction:** ITIL emphasizes meeting and exceeding service levels, which leads to better customer experiences.

Conclusion: Harmonizing Frameworks and Standards

- Many organizations use a combination of frameworks and standards to build a robust IT risk m anagement program.
- For example, they might use **ISO/IEC 27005** for cybersecurity risk, **FAIR** for quantifying financ ial risk, and **COBIT** for aligning IT risks with overall business strategy.
- The choice of which frameworks and standards to adopt depends on the organization's risk pr ofile, regulatory environment, and the maturity of its IT risk management program.
- These tools help organizations to systematically identify, assess, mitigate, and monitor IT risks to protect their data, assets, and reputation in a rapidly evolving technological landscape.

Week 2 Summary

- we have defined IT Risk Management Frameworks and Standards as the proc esses and tools that organizations use to manage and mitigate the potential ri sks associated with the use of technology

Major Risk Management Frameworks

- **1.** NIST Risk Management Framework (RMF)
- 2. COBIT (Control Objectives for Information and Related Technology)
- 3. ISO/IEC 27005
- 4. FAIR (Factor Analysis of Information Risk)

Week 2 Summary

- we said several Risk Management standards complement the frameworks.
- These standards offer prescriptive guidelines and methodologies that can be a dopted to ensure consistency and compliance

Major Risk Management Standards

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

References

- *NIST Risk Management Framework (RMF), National Institute of Standards and Technology (NIST), U.S. Department of Commerce*
- *ISO/IEC 27005 (Information Security Risk Management), International Organization for Standardization (ISO), ISO*
- *COBIT (Control Objectives for Information and Related Technology), ISACA (Information Systems Audit and Control Association), ISACA*
- *FAIR (Factor Analysis of Information Risk), Jack A. Jones and Jack Freund, The Open Group / Elsevier*
- *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), CERT Division, Software Engineering Institute (SEI), Carnegie Mellon University*