IT RISK MANAGEMENT AND CONTROL

Week 1: Introduction to IT Risk Management

LECTURER : Ninyikiriza Deborah Lynn – Minf, BCS

Department of Information Technology

Kumi University, Uganda- East Africa

Email: dninyikiriza000@gmail.com

COURSE OUTLINE

1. Course description
2. Course Goals
3. Learning outcomes
4. Introduction to IT Risk Management
5. The importance and objectives of IT risk management
6. Key concepts and definitions
7. The risk management life cycle

COURSE DESCRIPTION

- This course provides a comprehensive understanding of IT risk management principles, methodologies, and controls.
- It covers the identification, assessment, and mitigation of IT risks, along with the implementation of effective control measures to safeguard organizational assets.

COURSE GOALS

- ✓ The course aims at helping students to understand the fundamental concepts of IT risk management.
- ✓ It also aims at helping learners to Identify and assess various types of IT risks.
- ✓ To help students to develop and implement risk management strategies.
- ✓ To enable students learn about IT control frameworks and standards.
- ✓To help students to apply risk management practices to real-world scenarios.

LEARNING OUTCOMES

At the end of this course, students will be able to:

- Possess the knowledge and skills necessary to identify, assess, and manage risks associated with information technology.
- Understand IT Risk Concepts such as define and explain key concepts related to IT risk management, including risk assessment, risk mitigation, and risk control.
- Understand different types of IT risks, such as cybersecurity threats, data breaches, and system failures.

LEARNING OUTCOMES CONT…

- Students will also be able to perform Incident Management and Response there by developing and implementing incident response plans and strategies to address and manage IT security incidents.
- They will also understand the procedures for reporting and managing breaches or failures.

LEARNING OUTCOMES CONT…

- Students will also understand Compliance and Regulatory Requirements by recognizing and complying with relevant legal, regulatory, and industry standards related to IT risk management.
- Lastly, they will be able to assess the impact of compliance requirements on IT risk management practices.

INTRODUCTION TO IT RISK MANAGEMENT

➢ *TO BE UNDERSTOOD FIRST;*

What is;

- Information Technology (IT)?
- A risk ?
- An IT Risk ?
- IT Risk management ?

What is Information technology (IT)?

- ✓ Information technology is the use of computer systems to manage, process, protect, retrieve and exchange information.

- ✓ Information Technology is now so important to organizations that IT investments which include computers, networks, software, and employees are now one of the largest expenses for most organizations.

COMPONENTS OF INFORMATION TECHNOLOGY

To define IT components;

- These refer to the various elements that make up an IT system or infrastructure.
- ✓ Different IT components work together to create and manage technology systems by storing, retrieving, processing and transmitting data for specific purposes.
- ✓ Therefore, each component has specific functions that contribute to the overall operation and effectiveness of IT systems.

COMPONENTS OF IT

Figure 1. Components of Information Technology [8]

COMPONENTS OF IT CONT…

1. Hardware

- The physical devices and equipment used in computing and networking.

They include;

- ✓ **Servers** which provide centralized resources and services to client devices.
- ✓ **Desktops and Laptops** that act as end-user devices for personal and professional use.
- ✓ **Network Devices such as (Routers, Switches)** which facilitate data communication and network connectivity.
- ✓ **Storage Devices like (HDDs, SSDs)** that store data and applications.
- ✓ **Peripherals (Printers, Scanners)** that provide additional functionality to computers.

COMPONENTS OF IT CONT…

2. Software

- Programs and applications that run on hardware to perform specific tasks.

They include;

- ✓ **Operating Systems such as Windows, Linux, macOS** which manage hardware resources and provide a user interface.
- ✓ **Application Software like Office Suites, and Browsers** which perform specific tasks such as word processing, web browsing, and data analysis.
- ✓ **Middleware which** connects different software applications and services.
- ✓ **Security Software such as Antivirus and Firewalls** which protects systems from malware and unauthorized access.

COMPONENTS OF IT CONT…

3. Cloud computing

➢ This involves the delivery of computing resources and services over the internet.

- In simple terms, it is a component of IT that allows one to use powerful computing resources and services without having to invest in or maintain the underlying infrastructure themselves.

Includes;

✓ Different levels of cloud services **such as (IaaS, PaaS, SaaS)** ie; infrastructure, platforms, and software.

COMPONENTS OF IT CONT…

4. Networks

- Networks facilitate communication and data transfer between devices.

They include;

- **Network Infrastructure such as (Cabling, Fiber Optics)** which are physical components that carry network signals.
- **Networking Devices like (Modems, Network Interface Cards)** that enable connectivity and data exchange between devices.
- **Protocols such as (TCP/IP, HTTP/HTTPS)** that define rules and formats for data transmission and communication.

COMPONENTS OF IT CONT…

5. Databases

- Databases store, manage, and retrieve data efficiently.

They include;

- **Database Management Systems (DBMS)**, like **(MySQL, Oracle)** all which is Software that manages databases and provides access to data.
- **Data Models** that define the structure and organization of data within the database.
- **Query Languages** like **(SQL)**, which are used to retrieve and manipulate data in the database.

COMPONENTS OF IT CONT…

6. Internet and web technologies

- These are tools and protocols used to access, navigate and interact with information on the internet.

Examples include;

- Web browsers, websites, web servers, Hypertext Markup Language, cascading style sheets, JavaScript, HTTP and other internet-related technologies.

COMPONENTS OF IT CONT…

7. Security

- This is an IT component that protects IT systems and data from threats and vulnerabilities.

Good security practices to protect IT systems include;

- **Installing firewalls** to monitor and control incoming and outgoing network traffic.
- **System encryption** to secure data by converting it into an unreadable format for unauthorized users.

SECURITY CONT…

- **Performing Access Controls** which helps to manage who can access and use various resources and information.
- **Implementing Security Information and Event Management (SIEM)** which monitors, detects, and responds to security incidents.

UNDERSTANDING RISK!

What is a risk?

- ✓A risk is a likelihood that a loss will occur.
- ✓Organizations of all sizes face risks.
- ✓Some risks may be severe and other may be minor and acceptable.

NOTE

- Organizations use risk management techniques to identify and differentiate severe risks from minor risks.
- When properly done, managers can intelligently decide how to deal with any type of risk.

What is an IT risk?

- IT risk is a quantitative measure of the potential damage caused by a threat, a vulnerability or by an event (malicious or nonmalicious) that affects the set of IT assets owned by an organization.
- Risk exposure leads to potential losses and therefore it can be also defined as a measure of the average loss that may be expected from that exposure.

Examples of IT organizational assets that may be affected by risks;

i. Desktops and PCs

ii. Mobile devices and wireless networks eg PDAs, WIFI/Bluetooth devices

iii. Application servers

iv. Web servers

Examples of IT Assets continued..

v. Mail servers

vi. Database servers like (data ware house, storage), and other corporate data such as reports, memos, and records.

vii. Network elements such as switches, firewalls, appliances etc

viii. Mobility support systems such as virtual private network nodes, wireless email servers etc

OBJECTIVES OF IT RISK MANAGEMENT

1. **To Identify Risks** by recognizing potential threats and vulnerabilities that could affect IT systems and all its data.
   - This can be done by Conducting regular risk assessments and audits.
2. **To Assess Risks** and evaluate the likelihood and impact of identified risks to understand their potential effect on the organization.
   - This can be done by the use of qualitative and quantitative methods to assess risk levels and prioritize them.

OBJECTIVES CONT…

3. **To Mitigate Risks** by implementing controls and strategies that reduce the probability or impact of identified risks by developing and applying preventive, detective, and corrective measures.
4. **To Monitor and respond to risks** by continuously overseeing risk factors and control effectiveness to ensure that they remain effective and relevant.

OBJECTIVES CONT…

5. **To Communicate Risks** and ensure that relevant stakeholders are informed about risks and the measures put in place to manage them.
   - Done by providing regular updates and reports on risk status and management efforts.
6. **To Ensure Compliance** by ensuring that IT risk management practices align with legal, regulatory, and industry standards.
   - Done by regularly reviewing and updating policies to meet compliance requirements.

THE IMPORTANCE OF IT RISK MANAGEMENT

1. **It protects sensitive information,** there by safeguarding confidential data, such as personal information, financial records, and intellectual property, from unauthorized access, breaches, and loss.
2. **It maintains business continuity,** by identifying and mitigating risks thus helping to ensure that IT systems and services remain operational even in the face of disruptions.

THE IMPORTANCE CONT…

3. **It improves Strategic Decision-Making,** where by understanding the risk landscape allows organizations to make informed decisions about IT investments and strategies. This Aligns IT strategies with business objectives and risk tolerance.
4. **It enhances Operational Efficiency,** there by identifying and addressing vulnerabilities and inefficiencies. IT risk management can streamline processes and improve overall IT performance through reducing operational costs and enhancing productivity.

THE IMPORTANCE CONT…

5. **It Protects Financial Assets,** since IT risks such as fraud or data breaches can have significant financial consequences.
   - ✓ Risk management helps in minimizing these risks and their financial impact.
   - ✓ It safeguards against unexpected financial losses and supports long-term financial stability.

THE IMPORTANCE CONT…

6. **It Supports Regulatory Compliance**

- ✓ Many industries are subject to strict regulations regarding data security and privacy.
- ✓ Effective IT risk management helps to ensure compliance with laws and this avoids legal penalties and maintains trust with customers and partners.

THE IMPORTANCE CONT…

7. **It Fosters Trust and enhances good Reputation**

- ✓ Effective risk management practices build trust with stakeholders, including customers, partners, and investors, by demonstrating a commitment to security and reliability.
- ✓ This therefore enhances the organization’s reputation and competitive advantage.

KEY CONCEPTS AND DEFINITIONS

1. **Security threat**

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

2. **Vulnerability**

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

eg;

A software flaw that permits an exogenous agent to use a computer system without authorization or use it to a level higher than the authority granted.

KEY CONCEPTS AND DEFINITIONS CONT…

3. **Risk exposing events/risk events**

- ✓ These are incidences that expose the organization to potential harm, damage, or loss, by exploiting vulnerabilities in information technology systems, processes, or practices.
- ✓ These events can lead to negative consequences like data breaches, system outages, or financial losses.

KEY CONCEPTS AND DEFINITIONS CONT…

4. **Malicious events**

- ✓ These are actions taken with an intention to cause harm or damage to an organization's information systems, data, or operations.
- ✓ A direct attack can be done on the organizations firewalls, routers, websites, or data ware house by an individual or groups.

KEY CONCEPTS AND DEFINITIONS CONT…

5. Information Security

- In IT risk management, Information security spans the area of confidentiality, integrity and availability.
- **Confidentiality** is the protection against unauthorized access, appropriation, or use of assets.

Information security Continued…

- **Integrity** protection against unauthored manipulation, modification, or loss of assets.
- **Availability** is the protection against blockage, or limitation of benefit from an asset that is owned.

When do we consider that there is a breach in Information Security?

- When the three are abused.

When is Confidentiality abused?

- A breach of confidentially occurs when a person knowingly accesses a computer without authorization or uses it beyond the given authority.

Eg;

When a hacker views or copies private information such as credit card number etc.

When do we consider that there is a breach in information security?

- When the three are abused.

When is Integrity abused?

- A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered or destroyed without authorization.

Eg;

When a hacker uses a worm or virus to alter the source code in order to gain unauthorised access.

When do we consider that there is a breach in information security?

- When the three are abused.

When is availability abused?

- ✓ A breach of availability occurs when an authorized user is prevented from timely and reliably accessing data or a system.

Eg;

When a denial of service (DoS) attack happens.

RISK MANAGEMENT

When any breach happens, organizations face challenges on how to organize and run an efficient and effective information risk security management program. Organizations face challenges with;

i. How to identify risk events.
ii. How to assess the risks.
iii. How to mitigate or manage the environment to reduce risks.

IT RISK MANAGEMENT

So, what is IT risk management ?

- ✓ IT risk management also known as information security risk management is the process of reducing IT related risks.
- ✓ When we talk of a process, we mean a well defined or repeatable sequence of activities. Therefore risk management is a continuous process.
- ✓ Risk management is important to every organization, a company that ignores risk may fail when a single threat is exploited.

NOTE;

IT systems today contribute to the success of most companies. Therefore, if companies don't properly manage IT risks they may greatly contribute to company failure.

THE RISK MANAGEMENT LIFE CYCLE

- Effective risk management starts by understanding threats and vulnerabilities.
- IT risk management is made of five processes;

1. Risk identification or Identification of threats, vulnerabilities, or risk events impacting the set of IT assets owned by an organization.
2. Risk assessment also known as risk analysis.
3. Risk mitigation planning.
4. Risk mitigation implementation.
5. Evaluation of the mitigation effectiveness.

RISK IDENTIFICATION

What is Risk Identification?

- Risk identification can be defined as a process of identifying threats, vulnerabilities or events which are malicious or non malicious, planned or unplanned, impacting the set of IT assets owned by an organization.

RISK ASSESSMENT

What is Risk assessment?

- The process of calculating quantitatively the potential damage or monetory costs caused by a threat, a vulnerability, or by an event impacting the set of IT assets owned by an organization.

Risk assessment cont…

Qn. How is the damage calculated in risk assessment?

- The potential damage to the IT assets or business may be based on the previous internal and external events, input from audits and experts etc.
- This may help to determine the potential damage or quantify the probability that damage will occur.

RISK MITIGATION PLANNING

What is Risk mitigation planning?

- The process of controlling IT related risks.
- This incudes cost benefit analysis, and the selection, implementation , testing and security evaluation of safeguards.

NOTE;

- Risk mitigation planning considers both effectiveness and efficiency including the impact on the mission and constraints due to the policies, regulations and laws.

RISK MITIGATION IMPLEMENTATION

What is Risk mitigation implementation?

- The process of deploying and placing in-service equipment or solutions identified during the risk mitigation planning phase or actuating new corrective processes.

EVALUATION OF THE MITIGATION EFFECTIVENESS

What is involved?

- This involves monitoring the environment for effectiveness against the previous set of threats, vulnerabilities or events and also determining if new or different threats, vulnerabilities or events result from the modifications made to the environment.

WEEK 1 SUMMARY

a) In this lecture we have discussed Information Technology and some of its components such as hardware, software, cloud computing, databases etc.

b) We have learnt about IT risk which we defined as a quantitative measure of the potential damage caused by a threat, a vulnerability or by an event that affects the set of IT assets owned by an organization.

c) We have discussed IT Risk management, its objectives and its importance. Also key concepts such as threat, vulnerability, Information Security etc, have been discussed.

d) Lastly, we have learnt about the Risk Management life cycle which comprises of five step processes.

In our next lecture we shall look at IT Risk Management Frameworks and Standards.

See you in our next lecture!

REFERENCES

[1] Fundamentals of Information Technology Roy, Shambhavi; Daniel, Clinton; and Agrawal, Manish,2023, page 8.

[2] Managing risks in Information systems, Darril Gibson , second edition, Information systems security and assurance series, 2013, page 2

[3] Managing risks in Information systems, Darril Gibson , second edition, Information systems security and assurance series, 2013, page 3

[4] Managing risks in Information systems, Darril Gibson , second edition, Information systems security and assurance series, 2013, page 4

[5] Information Technology Risk management in Enterprise Environments, Jake Kouns and Daniel Minoli Wiley, 2011, page 15

[6] Information Technology Risk management in Enterprise Environments, Jake Kouns and Daniel Minoli, Wiley, 2011, page 16

[7] Information Technology Risk management in Enterprise Environments, Jake Kouns and Daniel Minoli, Wiley, 2011, page 17

[8] Retrieved September 16, 2024,from, https://www.techtarget.com/searchdatacenter/definition/IT