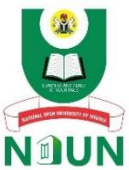
**COURSE GUIDE**

# CYB 415
# DISASTER AND INCIDENCE RISK MANAGEMENT

**Course Team** Dr. Jacob Olusola Odelola- (Course Developer/Writer)
University of Ibadan Ibadan
Prof. Francisca Chika Anyanwu- (Content Editor)
University of Ibadan Ibadan




**NATIONAL OPEN UNIVERSITY OF NIGERIA**

National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone
Nnamdi Azikiwe Expressway
Jabi, Abuja

Lagos Office
14/16 Ahmadu Bello Way
Victoria Island, Lagos

E-mail : centralinfo@nou.edu.ng
URL: www.nou.edu.ng



Printed 2024

ISBN: 978-978-786-280-3

## INTRODUCTION

CYB 415 is a two-credit unit course that has a minimum duration of one semester. It is a compulsory course for graduate students enrolled in BSc Cybersecurity at the National Open University of Nigeria. The course guides you through the techniques and methodologies for effective Disaster and Incidence Risk Management

## COURSE COMPETENCIES

- Understanding cyber disaster and incident risk management principles and framework.
- Identifying and assessing cyber threats and vulnerabilities.
- Developing and implementing cyber risk mitigation and control measures.
- Communicating effectively with stakeholders during cyber crises.

## COURSE OBJECTIVES

- To understand the fundamentals of cyber disaster and incident risk management.
- To identify and assess cyber risks and threats to organizational assets.
- To develop strategies for mitigating and controlling cyber risks.
- To design and implement effective cyber incident response and recovery plans.

## WORKING THROUGH THIS COURSE

To successfully finish this course, you should go through the study units, watch the videos and listen to the audios, complete all assessments, explore the provided links, engage in discussion forums, read the recommended books and other materials, work on your portfolios, and actively take part in the online facilitation.

Each study unit includes an introduction, intended learning outcomes (ILOs), main content, conclusion, summary, and references or further readings. The introduction outlines what to expect from the unit. Be sure to review the ILOs, as they define what you should be able to accomplish by the end of the unit. After completing each unit, you can assess your progress by checking if you've met the ILOs. The content is delivered through texts, videos, and links organized into modules and units. Follow the provided links when instructed; if you're working offline, copy and paste the link into your browser. You can download audio and video materials to view offline, and the texts can be printed or saved on your computer or external drive. The conclusion summarizes

the key takeaways from the unit, and the unit summaries are also available as downloadable audio and video files.

There are two primary types of assessments: formative and summative. Formative assessments are designed to help you track your progress and are provided through in-text questions, discussion forums, and Self-Assessment Exercises.

Summative assessments are used by the university to evaluate your academic performance. These assessments include a Computer-Based Test (CBT) for continuous assessment and a final examination. A minimum of three CBTs will be administered, along with one final exam at the end of the semester. You are required to complete all CBTs and the final exam..

There are 16 study units in this course divided into four modules. The modules and units are presented as follows:

**STUDY UNITS**

**MODULE 1 FUNDAMENTAL RISK CONCEPT AND TERMINOLOGY**

Unit 1: Concept of Risk.
Unit 2: Regulatory Requirements and Best Practices.
Unit 3: Links between Risk, Incident, and Safety Culture in the workplace.
Unit 4: Key Risk Management Implementation Issues.

**MODULE 2: PRACTICAL RISK ASSESSMENT DEMONSTRATION**

Unit 1: Risk Assessment Demonstration
Unit 2: Risk Control Options.
Unit 3: Risk Prioritization and Decision Making.
Unit 4: Risk Assessment Strategies.

**MODULE 3: INCIDENT INVESTIGATION BASICS AND TERMINOLOGY**

Unit 1: Incident Investigation.
Unit 2: Process of Incident Investigation.
Unit 3: Interviewing and Facts Gathering Techniques.
Unit 4: Root Cause Analysis. (RCA)

**MODULE 4: PRACTICAL INCIDENT INVESTIGATION EXECUTION.**

Unit 1: Incident Investigation execution.
Unit 2: Case Study on Incident Investigation.
Unit 3: Incident Investigation, Report Writing and Presentation.
Unit 4: Practical Integration of Risk Management and Incident.

## REFERENCES AND FURTHER READINGS

Alamdari, A. M., Jabarzadeh, Y., Adams, B., Samson, D., & Khanmohammadi, S. (2023). An analytic network process model to prioritize supply chain risks in green residential megaprojects. Operations Management Research, 16(1), 141–163. https://doi.org/10.1007/s12063-022-00288-2

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://www.mdpi.com/2079-9292/12/6/1333

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15–26. https://www.academia.edu/download/106082632/1188.pdf

Mathew, A. J. (2024). Unscripted Practices for Uncertain Events: Organizational Problems in Cybersecurity Incident Management. Science, Technology, & Human Values, 01622439241240411. https://doi.org/10.1177/01622439241240411

Möller, D. P. F. (2023). Cybersecurity in Digital Transformation. In D. P. F. Möller, Guide to Cybersecurity in Digital Transformation (Vol. 103, pp. 1–70). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-26845-8_1

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, 132, 103309. https://www.sciencedirect.com/science/article/pii/S0167404823002195

Quinn, T. P. (2023). An Assessment of the US'Preparedness for Foreign Cybersecurity Threats. Northeastern Illinois University. https://search.proquest.com/openview/6fb153bf0b341eaadfa4e0c8e608e290/1?pq-origsite=gscholar&cbl=18750&diss=y

## PRESENTATION SCHEDULE

The presentation schedule outlines important dates for completing your computer-based tests, participating in forum discussions, and attending facilitation sessions. It's crucial to submit all assignments on time, avoiding any delays. Be mindful of plagiarism, as it is a serious academic offense and carries strict penalties.

## ASSESSMENT

There are two main forms of assessments in this course that will be scored. The Continuous Assessments and the final examination. The continuous assessment shall be in three-fold. **There will be two Computer Based Assessments. The computer-based assessments will be given in accordance to the university academic calendar. The timing must be strictly adhered to**. The Computer Based Assessments shall be scored a maximum of 10% each, while your participation in discussion forums and your portfolio presentation shall be scored maximum of 10% if you meet 75% participation. Therefore, the maximum score for continuous assessment shall be 30% which shall form part of the final grade.

The final examination for CYB 415 will last a maximum of two hours and will account for 70% of your total course grade. It will consist of 70 multiple-choice questions designed to assess cognitive reasoning.

**Important Note**: You can earn an additional 10% if you participate in at least 75% of the course forum discussions and submit your portfolios. Failing to meet this participation requirement will result in the loss of the 10% from your total score. You are required to upload your portfolio via Google Docs.

**What should your portfolio include?** Your portfolio should contain notes or jottings on each study unit and activity, along with details on the time you spent on each unit or activity.

## HOW TO GET THE MOST FROM THE COURSE

To get the most out of this course, it's essential to have a personal laptop and reliable internet access. This will allow you to learn from anywhere in the world. Use the Intended Learning Outcomes (ILOs) to guide your self-study throughout the course. After completing each unit, assess your progress by checking whether you have achieved the ILOs.

Carefully go through each unit, take notes, and participate in the scheduled online real-time facilitation sessions. If you miss a session,

you can review the recorded version at your convenience, as each real-time facilitation session will be recorded and posted on the platform.

In addition to real-time facilitation, make sure to watch the video and audio-recorded summaries for each unit. These summaries focus on the key points of each unit. You can access them by clicking the links provided in the text or through the course page.

Complete all self-assessment exercises, and remember to follow the course rules.

## FACILITATION

You will receive online facilitation. The facilitation is learner-centred.

The mode of facilitation shall be asynchronous and synchronous. For the asynchronous facilitation, your facilitator will:

- Present the theme for the week;
- Direct and summarise forum discussions;
- Coordinate activities in the platform;
- Score and grade activities when need be;
- Upload scores into the university-recommended platform;
- Support you to learn. In this regard, personal emails may be sent.
- Send you videos and audio lectures; and podcast

For the synchronous:

- There will be eight hours of online real-time contact in the course.

  This will be through video conferencing in the Learning Management System. The eight hours shall be of one-hour contact for eight times.

- At the end of each one-hour video conferencing, the video will be uploaded for viewing at your pace.
- The facilitator will concentrate on the main themes that are must-know in the course.
- The facilitator is to present the online real-time video facilitation timetable at the beginning of the course.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

Do not hesitate to contact your facilitator. Contact your facilitator if you:

- do not understand any part of the study units or the assignment.
- have difficulty with the self-assessment exercises
- have a question or problem with an assignment or with your tutor's comments on an assignment.

Also, use the contact provided for technical support.

Be sure to read all comments and notes from your facilitator, especially regarding your assignments, and actively participate in the forums and discussions. Engaging in these discussions allows you to connect with others in the program and raise any issues you encounter during your studies. To get the most out of course facilitation, prepare a list of questions in advance for the discussion sessions. Active participation will greatly enhance your learning experience.

Lastly, respond to the course questionnaire. This feedback helps the university identify areas where you face challenges and make improvements in the course materials and lectures.

## COURSE INFORMATION

You are welcome to CYB 415, Disaster and Incidence Risk Management a two-unit course. Please upload your profile such as picture, workplace address, GSM number and other details on your wall. What are your expectations in this course? I am sure you are going to enjoy the course, please fasten your seat belt as you take off. Once again you are welcome.

**MAIN COURSE**

# MODULE 1 FUNDAMENTAL RISK CONCEPT AND TERMINOLOGY

## INTRODUCTION

Organizations are prone to various kinds of risks that have the potential to hinder the attainment of their organizational goal. Some risks, if not properly managed, can lead an organization into bankruptcy or even extinction in extreme cases. Hence, effective risk management is vital for the subsistence of any organization. (Coccia, 2023).

Unit 1 Concept of Risk.
Unit 2 Regulatory Requirement and Best Practices.
Unit 3 Links Between Risk, Incident and Safety Culture.
Unit 4 Key Risk Management Implementation Issues.

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

## UNIT 1 CONCEPT OF RISK.

### Contents



### 1.0 Introduction

You will learn from this unit the definition, terminologies and concepts of Risk. After studying the unit, you will be equipped with skills to define a risk and identify a threat, vulnerability and consequences. You

will also have the requisite background knowledge for risk analysis in the context of cybersecurity while focusing on the CIA Triad (Confidentiality, Integrity, and Availabity).

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Appraise that a risk entails the potential for harm or loss to an organization's digital assets, data, or reputation.

## 3.0 Main Content

### 3.1 What is a Risk?

Organisations are prone to various kinds of risks that have the potential to hinder the attainment of their organisational goal. Some risks, if not properly managed, can lead an organisation into bankruptcy or even extinction in extreme cases. Hence, effective risk management is vital for the subsistence of any organisation.

"Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:

(i) the adverse impacts that would arise if the circumstance or event occurs; and
(ii) the likelihood of occurrence." (Joint Task Force Transformation Initiative, 2012).

ISO 31000 describes risk as the deviation of organisational objectives from their expected values caused by uncertainty in the organisation process. Uncertainty, in this case, refers to inadequate information about an event, its consequence, or its likelihood of occurrence. In other words, you know you are facing a risk when you are in a situation that makes you uncertain about your chances of realising your objectives and when you can realise them. From the description above, how will you classify the organisatiional risks?

In cybersecurity, risk is commonly defined as the combination of threat, vulnerability, and consequence.

Risk = Threat x Vulnerability x Consequence


**Figure 1.1:** Organizational risk and its component

Risk represents the potential for loss when a threat occurs. It is the combination of the probability that a threat will exploit a vulnerability and the severity of the resulting consequences.

## 3.2 Threat

A threat is any potential event that can cause harm to an organization's digital assets. Threat actors include nation-states, cybercriminals, hacktivists, insiders, and even developers of substandard products. Common cybersecurity threats include phishing, ransomware, DDoS attacks, and denial of service. (Thakur, 2024).

## 3.3 Vulnerability

A vulnerability is a flaw or deficiency in the design, implementation, operation, or management of an asset that could be exploited by a threat. Examples include unpatched software, misconfigured systems, weak passwords, or lack of employee training.

## 3.4 Consequence

The consequence is the potential damage inflicted on an organization due to a successful cyberattack. This can include financial loss, data breaches, service disruptions, and reputational damage. Consequences can be direct (e.g. data theft) or indirect (e.g. customer churn after a breach).

## 3.5 CIA Triad

The Confidentiality, Integrity and Availability (CIA) triad are the three core principles that guide cyber security efforts.

**Confidentiality** ensures information is only accessible to authorized entities.

focuses on the accuracy and reliability of data and systems.

**Availability** guarantees that systems and data are accessible whenever they are required.

Balancing these three principles is a fundamental challenge in cyber security.

## 3.6 Risk Management

Risk management is the ongoing process of identifying, assessing, and justifying risks to an organization's digital assets. This involves implementing security controls, monitoring systems, and regularly reviewing risks to minimize the potential for threats to occur. A risk-based approach helps prioritize security efforts and investments based on the potential impact on the business. (Hodson, 2024).

## 4.0 Self-Assessment Exercise(s)

1) What is Risk

Answer
Risk entails a potential for loss when a threat occurs. This can include financial

loss, data breaches, service disruptions and reputational damage/ Risk = Threat x Vulnerability x consequence.

2) Explain briefly the CIA triad

Answer
CIA is an acronym for confidentiality, integrity and availability: they are the core pillars that guide cybersecurity efforts.

- Confidentiality: Ensures data is accessible only to authorized parties.
- Integrity: focuses on the accuracy and reliability of data.
- Availability: guarantees that data/systems are accessible wherever they are required.

3) What is risk management?

Answer
Risk management is the process of identifying, assessing, and justifying risks to an organization's digital assets, and this may include implementing security controls, monitoring systems, and regulator reviewing risks to minimize the potential for threats to over.

## 5.0 Conclusion

You have learnt from this unit about the definition, terminologies, and concept of risk. You have also been equipped with skills to identify threats, vulnerability, and consequence. You have also been given the requisite background knowledge for risk analysis in cybersecurity

## 6.0 Summary

At the end of this unit, you have learnt by definition that risk is a potential for loss when a threat occurs. This can include financial loss, data breaches service disruptions, and reputational damage. You have also been exposed to ways of carrying out risk analysis.
In the next unit, you will be introduced to different types of regulatory requirements and best practices in disaster, incidence, and risk management.

## 7.0 References/Further Readings

Coccia, M. (2023). New Perspectives in Innovation Failure Analysis: A taxonomy of general errors and strategic management for reducing risks. Technology in Society, 75, 102384. https://www.sciencedirect.com/science/article/pii/S0160791X23001896

Hodson, C. J. (2024). Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls. Kogan Page Publishers.

https://books.google.com/books?hl=en&lr=&id=ZyjyEAAAQBAJ&oi=fnd&pg=PR1&dq=Risk+management+is+the+ongoing+process+of+identifying,+assessing,+and+justifying+risks+to+an+organization%27s+digital+assets.+This+involves+implementing+security+controls,+monitoring+systems,+and+regularly+reviewing+risks+to+minimize+the+potential+for+threats+to+occur&ots=0MA5NP4cTI&sig=iooSV620RfkJn5H8WHxdRensa2U

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education (JASE), 4(1), 1–20. http://jase.a2zjournals.com/index.php/ase/article/view/42

# UNIT 2 REGULATORY REQUIREMENT AND BEST PRACTICES.

## Contents



## 1.0 Introduction

You will learn from this unit how to conform to regulatory requirements and best practices in disaster, incidence risk management.
After studying this unit, you will be able to understand and conform to regulatory requirements and base practices.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Basically conceptualize regulatory requirements and least practices.
- Learn how to conform to and carry out the regulatory requirements and best practices.

## 3.0 Main Content

In its Quarterly Cyber Regulations Updated February 2023, the Wall Street Journal highlighted upcoming regulations from multiple U.S. agencies that will impact investment firms' cybersecurity risk management, governance, and incident disclosure policies (Quinn, 2023).
In today's digital age, where technology plays a vital role in our personal and professional lives, cybersecurity has become a crucial concern. With cyber threats on the rise, organizations, and individuals must be aware of the compliance standards and regulations put in place to protect sensitive data and mitigate risks. (Möller, 2023)

Cybersecurity compliance refers to adhering to specific rules, regulations, and standards to protect sensitive information and ensure the security of digital systems. Compliance frameworks provide guidelines on how organizations should implement security controls, handle data breaches, and safeguard customer privacy**.**

### 3.1 Cyber Security Regulations

Cybersecurity regulations are essential for maintaining the integrity and trustworthiness of digital platforms. They provide a structured approach to address potential risks and protect against cyber threats. Compliance with these regulations not only helps organizations avoid legal consequences but also enhances their reputation and builds customer trust. (AL-Hawamleh, 2024).

1. General Data Protection Regulation (GDPR)
The General Data Protection Regulation (GDPR) is a European Union regulation that sets guidelines for the collection, storage, and processing of personal data. It empowers individuals with more control over their data and imposes strict penalties on organizations that fail to comply with its provisions. (Aslan et al., 2023).

2. Payment Card Industry Data Security Standard (PCI DSS)
The Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that handle credit card information. It ensures the secure handling of cardholder data and promotes the adoption of robust security measures to prevent data breaches and unauthorized access.

3. Health Insurance Portability and Accountability Act (HIPAA)
HIPAA is a U.S. law that sets standards for safeguarding individuals' medical records and other personal health information. It applies to healthcare providers, health plans, and healthcare clearinghouses,

enforcing strict regulations to maintain the confidentiality and integrity of patient data. (Oakley, 2023).

4. Federal Information Security Management Act (FISMA)

FISMA is a U.S. federal law that establishes guidelines for securing government information systems. It mandates federal agencies to create, implement, and sustain robust cybersecurity programs aimed at protecting sensitive information and critical infrastructure.

5. California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) grants California residents greater control over their personal data. It requires businesses to be transparent about the data they collect, offer opt-out options, and protect consumer information from unauthorized access.

6. International Organization for Standardization (ISO) Standards

ISO standards, such as ISO/IEC 27001 and ISO/IEC 27002, provide a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system. These standards are globally recognized and help organizations demonstrate their commitment to cybersecurity.

7. Cybersecurity Frameworks: NIST and CIS Controls

The National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) provide comprehensive cybersecurity frameworks. NIST's Cybersecurity Framework focuses on risk management and aligning cybersecurity efforts with business objectives. The CIS Controls offer specific guidelines for implementing essential cybersecurity measures.

8. Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) is a US law that sets standards for financial reporting and corporate governance. While it primarily focuses on financial accountability, it includes provisions for internal controls and data security, making it relevant to cybersecurity compliance.

9. European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA) plays a significant role in promoting cybersecurity in Europe. It provides guidance on various cybersecurity topics, including risk management, incident response, and critical infrastructure protection.

## 3.2 Additional Regulations

The Information Technology Act, 2000 governs India's cyber laws. Initially designed to provide legal recognition for e-Commerce and facilitate the registration of electronic records with the government, the

Act has since been amended to address the evolving tactics of cyber attackers and the misuse of technology. Enacted by the Parliament of India, (Patel et al., 2023). the IT Act stipulates severe punishments and penalties to protect the e-governance, e-banking, and e-commerce sectors. Its scope has been broadened to include all modern communication devices, making it a cornerstone of Indian legislation in the fight against cybercrime:

Section 43: This section applies to individuals who damage computer systems without the owner's consent. The owner is entitled to full compensation for any damages incurred.

Section 66: This section deals with acts committed dishonestly or fraudulently as outlined in Section 43Offenders under this provision may face up to three years in prison or a fine of up to Rs. 5 lakhs.

**Section 66B**: This section deals with the punishment for fraudulently receiving stolen communication devices or computers. Offenders can face up to three years in prison and a fine of up to Rs. 1 lakh, depending on the severity of the crime.

Section 66C: This section focuses on identity thefts involving fraudulent digital signatures, hacked passwords, or other unique identification features. Convictions can lead to three years in prison and a fine of up to Rs. 1 lakh.

Section 66D: This section was added to punish those who commit impersonation using computer resources.

Indian Penal Code (IPC) 1860: Identity thefts and related cyber frauds are also covered under the IPC, which works in conjunction with the Information Technology Act of 2000. Relevant sections include:

- Forgery (Section 464)
- Forgery for cheating (Section 468)
- False documentation (Section 465)
- Presenting a forged document as genuine (Section 471)
- Reputation damage (Section 469)

Companies Act of 2013: This act outlines the legal obligations for corporate stakeholders to improve daily operations through techno-legal compliances. The Serious Frauds Investigation Office (SFIO) has the authority to prosecute companies and their directors. Following the 2014 notification of the Companies Inspection, Investment, and Inquiry Rules, the SFIO has become more proactive in enforcement. The act covers regulatory compliances, including cyber forensics, e-discovery,

and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014, set strict guidelines for the cybersecurity responsibilities of company directors and leaders.

NIST Compliance: The Cybersecurity Framework (NCFS) by the National Institute of Standards and Technology (NIST) offers a standardized approach to managing cybersecurity risks. The framework emphasizes flexibility and cost-effectiveness, promoting the resilience and protection of critical infrastructure by:

- Improving the interpretation, management, and reduction of cybersecurity risks to mitigate data loss, misuse, and restoration costs
- Identifying and securing critical activities and operations
- Demonstrating organizational trustworthiness in securing critical assets
- Prioritizing investments to maximize cybersecurity ROI
- Addressing regulatory and contractual obligations
- Supporting broader information security programs

By integrating the NIST CSF framework with ISO/IEC 27001, organizations can simplify cybersecurity risk management and improve communication across the organization and supply chains using a common directive.

Final Thoughts: As reliance on technology grows, cyber laws in India and globally must continuously evolve. The shift to remote work during the pandemic has heightened the need for app security. Lawmakers must stay ahead of cybercriminals to prevent breaches. Effective control of cybercrimes requires collaborative efforts from lawmakers, internet and network providers, intermediaries like banks and shopping sites, and users. Only through diligent adherence to cyber laws can online safety and resilience be achieved.

## 3.3 Role of International Laws

In various countries, sectors within the computing and communication industries are regulated by governmental bodies. Specific rules govern the uses of computers and networks, particularly concerning unauthorized access, data privacy, and spamming. Additionally, there are restrictions on the use of encryption and equipment that could bypass copy protection schemes. Laws also cover internet trade, taxation, consumer protection, and advertising. Regulations on censorship versus freedom of expression, public access to government information, and individual access to information held by private entities are also

established. Some countries limit internet access through legal and technical means.

## 3.4 International Law for Cyber Crime

Cybercrime is inherently international, with no clear borders between countries. The diverse and complex nature of cybercrime necessitates international cooperation for effective combat. Various organizations and governments have collaborated to establish global standards for legislation and law enforcement, both regionally and internationally.

### 3.4.1 The Indian Cyberspace

Indian cyberspace began in 1975 with the establishment of the National Informatics Centre (NIC) to provide IT solutions for the government. Between 1986 and 1988, three key networks were created to connect various government agencies: INDONET, which linked IBM mainframe installations; NICNET, a nationwide VSAT network connecting central, state, and district administrations; and ERNET, which supported academic and research communities.

The New Internet Policy of 1998 opened the door for multiple Internet service providers (ISPs), driving the rapid growth of the Internet user base from 1.4 million in 1999 to over 150 million by December 2012. This growth was largely fueled by increased internet access through mobile phones and tablets. As part of the National Broadband Plan, the government aimed to raise broadband penetration from about 6% to 160 million households by 2016.

## 3.5 National Cyber Security Policy

The National Cyber Security Policy, established by the Department of Electronics and Information Technology, aims to protect public and private infrastructure from cyberattacks. It also seeks to safeguard personal, financial, banking, and sovereign data, especially in light of the US National Security Agency (NSA) leaks indicating surveillance of Indian users without legal or technical safeguards.

The Ministry of Communications and Information Technology defines cyberspace as a complex environment involving interactions between people, software, and services supported by a global distribution of information and communication technology.

### 3.5.1 Vision

To build a secure and resilient cyberspace for citizens, businesses, and government, while protecting user privacy.

### 3.5.2 Mission

To protect information and infrastructure in cyberspace, develop capabilities to prevent and respond to cyber threats, and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

### 3.5.3 Objective

The Ministry of Communications and Information Technology defines the following objectives:

- To create a secure cyber ecosystem in the country, fostering trust and confidence in IT systems and transactions in cyberspace, thereby enhancing IT adoption across all economic sectors.
- To establish an assurance framework for the design of security policies and promote compliance with global security standards and best practices through conformity assessments (covering products, processes, technology, and people).
- To strengthen the regulatory framework to ensure a secure and resilient cyberspace ecosystem.
- To establish and enhance national and sector-specific 24/7 mechanisms for gathering strategic information on threats to ICT infrastructure, and to create scenarios for response, resolution, and crisis management through effective predictive, preventive, protective, responsive, and recovery actions.

## 3.5 Cyber Security Best Practices

*1. Review and update:*
Review and update your cybersecurity risk management program to comply with new regulations from the U.S. Securities and Exchange Commission (SEC) and New York Department of Financial Services (if applicable). Ensure your program covers all the necessary elements, including incident reporting, information disclosure, governance, and oversight.

*2. Evaluate your Vendor Management Program*
If your firm works with third-party vendors (and it likely does), it's crucial to evaluate your vendor management program to make sure

they're compliant with the latest regulations. Establishing a third-party risk management program will help you review their cybersecurity policies and procedures, conduct third-party risk assessments, and establish a process for incident response and notification. (Learn more about third-party cybersecurity risk.)

*3. Update your Incident Response Plan*

Update your incident response plan (IR) so that it covers all the necessary elements, including incident detection, containment, investigation, and reporting. The new regulations require companies to report material cybersecurity incidents and periodic updates about previously reported incidents. An effective IR solution responds to a detected breach within minutes, shares regular updates until the incident has been contained and eradicated, defines remediation plans and delivers a full report with actionable recommendations.

*4. Control Over Personal Information*

The new privacy laws in the U.S. and EU give consumers more control over their personal information. To be compliant, firms need to have a process for receiving and responding to consumer requests, including access, deletion, and correction. Working with a cybersecurity provider who has experience navigating these policies can help firms take a comprehensive approach to privacy and security, which is essential for protecting personal information.

*5. Determine Which Regulations Apply*

Firstly, it is crucial to identify the laws and regulations that are relevant to your organization. Regulations like the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA) are just a few examples of the many regulations that impact different sectors. For instance, HIPAA pertains to healthcare providers, while GDPR governs personal information collected from EU citizens. Understanding which regulations apply to your business, whether it operates nationally or internationally, is essential. Additionally, you must evaluate how each regulation affects your organization. Each industry has unique requirements, and depending on your sector, specific regulations may necessitate additional training, registration, or compliance measures.

*6. Conduct a Risk Assessment*

A cybersecurity risk assessment helps an organization manage, control, and mitigate cybersecurity risks. It informs decision-making and streamlines appropriate responses. Utilizing a risk assessment process can significantly reduce compliance risks and enhance compliance management. Organizations can use a Risk Assessment Template to

develop a comprehensive risk assessment process, regardless of their size.

Alternatively, outsourcing to a team of experts to perform a risk assessment is another viable option. Whichever method is chosen, it is crucial to thoroughly evaluate your organization for vulnerabilities to avoid cybersecurity threats and manage compliance requirements.

*7. Perform Compliance Review*

A common misconception about cybersecurity compliance is that it only involves technical solutions. However, cybersecurity compliance also includes legal, financial, regulatory, operational, and administrative aspects. Therefore, an effective cybersecurity compliance program must address all these areas. The first step to creating such a program is conducting a compliance review. Organizations can outsource for a full external compliance review to gain additional insights and ensure they meet all compliance demands.

*8. Cybersecurity Awareness Training*

Implementing an effective cybersecurity awareness training program is a critical step organization can take to meet compliance needs and protect against cyber threats. This can be achieved by requiring employees to complete annual training courses related to cybersecurity and compliance standards. If a company already offers cybersecurity awareness training, it is beneficial to evaluate the program's effectiveness. Assess the current knowledge base and identify gaps. For example, some areas may need more focus, such as educating employees about mobile device management tools.

*9. Create Policies & Procedures*

Organizations should regularly update their cybersecurity compliance monitoring policies and procedures. This includes ensuring employees are aware of the company's policies on accessing sensitive information and are trained to recognize phishing emails. Employees should also be familiar with best practices for protecting themselves while accessing corporate systems. Policies and education should reinforce endpoint security. Security control is one of the most significant security compliance practices a company can implement. Therefore, the security team should ensure all security requirements are met with appropriate measures, policies, and procedures.

*10. Continuous Monitoring Plan*

To mitigate risk, continuous monitoring is necessary to detect new threats and vulnerabilities. After conducting an initial audit, an organization can begin developing a compliance monitoring plan. Start

by identifying the most critical risk areas and addressing known issues first.

*11. How to Create a Compliance Monitoring Plan?*

To create a continuous monitoring plan, the security team should first test the current security infrastructure to ensure tools are functioning correctly. Based on these tests, determine whether further security compliance procedures are needed. Document all security policies and procedures implemented to safeguard sensitive information. This documentation helps systematically align compliance needs, audits, and revisions of security efforts. The plan should specify the frequency and type of assessments, whether relying solely on automated tools or incorporating manual reviews. Each method's level of effort should be considered, as automated tools typically require less time and resources, while manual reviews require more.

*12. Final Thoughts*

Hackers continually devise new methods to penetrate systems and steal data, posing ongoing compliance risks. Therefore, cybersecurity compliance monitoring should be both regular and proactive. Companies should look for potential breach indicators before they occur and have a plan to respond swiftly if a breach happens. Employees must understand the importance of cybersecurity compliance and take steps to protect themselves from cyberattacks. Organizations should decide whether to develop a formal policy to govern the process or outsource compliance monitoring. Identifying potential vulnerabilities and addressing them promptly will help prevent breaches from becoming significant security issues.

## SELF-ASSESSMENT EXERCISE(S)

1) What are cybersecurity regulations?

Answer

They are the essentials for maintaining the integrity and truthworthiness of digital platforms. Compliance with these regulations not only helps organizations avoid legal consequences but also enhances customer trust.

2) State four (4) of the cybersecurity regulations

Answer

i. General data protection regulation
ii. Payment card industry data security standard (PCIDSS) iii. Health insurance portability and accountability Act (HIPAA).

## 5.0 Conclusion

You have learnt from this unit how to conform to regulatory requirements and best practices in disaster, incidence, and risk management. You also learnt about the need to understand and conform to regulatory requirements.

## 6.0 Summary

At the end of this unit, you have learnt in-depth of regulatory requirements and best practices in cybersecurity.

Essentially, you were able to conceptualize regulatory requirements and the need to conform to best practices. In the next unit, you will learn how to establish the links between risk, incident and safety culture.

## 7.0 References/Further Readings

AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1), 1315–1331. https://journal.uob.edu.bh/handle/123456789/5502

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://www.mdpi.com/2079-9292/12/6/1333

Möller, D. P. F. (2023). Cybersecurity in Digital Transformation. In D. P. F. Möller, Guide to Cybersecurity in Digital Transformation (Vol. 103, pp. 1–70). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-26845-8_1

Oakley, A. (2023). HIPAA, HIPPA, or HIPPO: What Really Is the Heath Insurance Portability and Accountability Act? Biotechnology Law Report, 42(6), 306–318. https://doi.org/10.1089/blr.2023.29329.aso

Patel, P. C., Oghazi, P., & Arunachalam, S. (2023). Does consumer privacy act influence firm performance in the retail industry? Evidence from a US state-level law change. Journal of Business Research, 162, 113881. https://www.sciencedirect.com/science/article/pii/S0148296323002394

Quinn, T. P. (2023). An Assessment of the US'Preparedness for Foreign Cybersecurity Threats. Northeastern Illinois University. https://search.proquest.com/openview/6fb153bf0b341eaadfa4e0c8e608e290/1?pq-origsite=gscholar&cbl=18750&diss=y

# UNIT 3 LINKS BETWEEN RISK, INCIDENT AND SAFETY CULTURE.

## Contents



## 1.0 Introduction

You will learn from this unit how to establish the links between risk, incident and safety culture after studying this unit, you will be able to understand the concept of safety culture in an environment**.**

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Study and understand the relationship between risk, incidents and safety culture.
- Learn the skills of implementing controls and mitigations to reduce the probability or impact of a cyberattack

## 3.0 Main Content

The relationship between risk incidents and safety culture in cybersecurity is a critical aspect that organizations need to address. Safety culture, which focuses on promoting a safe working environment and preventing accidents, can significantly impact cybersecurity practices and risk incidents. Research has shown that safety culture influences cybersecurity culture, indicating a connection between the two domains (Alsmadi, 2023).

In the context of cybersecurity, a strong safety culture can enhance risk incident prevention by instilling a mindset of vigilance, adherence to protocols, and a proactive approach to identifying and mitigating potential threats. By fostering a culture that values security and safety, organizations can create a more resilient environment that is better equipped to prevent and respond to cyber incidents effectively.

### 3.1 Understanding the relationship between risk incidents and safety culture

Understanding the relationship between risk incidents and safety culture in cybersecurity is crucial for organizations to develop comprehensive strategies that integrate both safety and security practices. By aligning safety culture principles with cybersecurity measures, organizations can enhance their overall risk management approach and better protect their digital assets from cyber threats.

### 3.2 Risk, Incident, and Safety Culture in the workplace

Essentially, the links between Risk, Incident, and Safety Culture in the workplace are:

#### 3.2.1 Risk

- Refers to the potential for harm or loss to an organization's digital assets, data, or reputation.
- Involves identifying, assessing, and prioritizing potential threats and vulnerabilities.
- Requires implementing controls and mitigations to reduce the likelihood or impact of a cyber-attack.

### 3.2.2 Incident

- Refers to a specific cybersecurity event or breach, such as a data leak or ransomware attack.
- Requires prompt response, containment, and eradication to minimize damage.
- Involves incident response planning, communication, and post-incident analysis to improve future response.

### 3.2.3 Safety Culture

- Refers to an organization's shared values, attitudes, and behaviors that prioritize cybersecurity and risk management.
- Involves fostering a culture of accountability, transparency, and continuous improvement.
- Encourages employees to report incidents and near-misses without fear of retribution.

## 3.3 Links between Risk, Incident, and Safety Culture:

- Risk management informs incident response planning by identifying potential threats and vulnerabilities.
- Incident response improves risk management by providing lessons learned and feedback for improvement.
- Safety Culture supports risk management and incident response by promoting a proactive and accountable approach to cybersecurity.
- A Strong Safety Culture encourages employees to report incidents and near-misses, enabling swift response and continuous improvement.
- Effective risk management and incident response reinforce a positive Safety Culture by demonstrating an organization's commitment to cybersecurity and employee trust.
- Cybersecurity incidents can impact an organization's reputation and trust among customers, partners, and stakeholders, highlighting the importance of a strong Safety Culture.
- Continuous monitoring and assessment of risks and incidents help identify areas for improvement in the Safety Culture.

## 3.4 Diagram illustrating the links between Risk, Incident, and Safety Culture in the workplace in the context of cyber security

Here's a diagram illustrating the links between Risk, Incident, and Safety Culture in the workplace in the context of Cybersecurity:

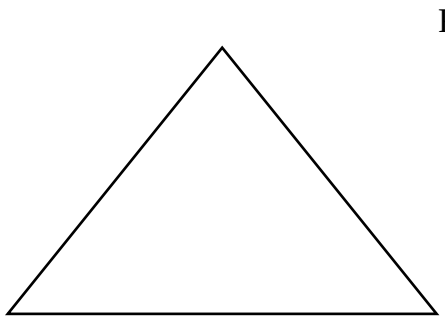



**Figure 1.2:** Relationship between Risk, Incident and Safety Culture

Relationship:

1) Risk ⟺ Incident

❖ Risk if not mitigated often leads to security incidents (Cyber-attacks, data breaches).
❖ Also, incidents can reveal new risks or vulnerabilities.

2) Incident ⟺ safety culture.

❖ Incident tends to weaken or strengthen safety culture.
❖ A strong safety culture can improve incident response and minimize damage.

3) Safety culture ⟺ Risk.

❖ Positive safety culture reduces risk
❖ Identifying and managing risks can foster a culture of pro-activeness and accountable approach to cyber security thereby maintaining a good safety culture.

### ❖ Deductions from dynamics of the triangle.

i. Base of the triangle (Risk, incident) where Risk and incident correspond directly to each other.
ii. Apex (Safety culture)

A significant measure of safety culture can influence and mitigate Risk and incident from occurring.
In summary:

- Risk management informs incident response planning
- Incident response improves risk management by providing lessons learned
- Safety Culture supports risk management and incident response by promoting a proactive and accountable approach to cybersecurity
- A Strong Safety Culture encourages employees to report incidents and near-misses, enabling swift response and continuous improvement

By understanding these links, organizations can create a robust cybersecurity posture that integrates risk management, incident response, and safety culture to protect their digital assets and reputation.

## 4.0 Self-Assessment Exercise(s)

1. What is the relationship between risk incidents and safety culture?

**Answer**
Promoting a robustly safe culture is significant to managing risks, thereby responding strongly to incidents. Hence the three (3) are interconnected.

2. Why is constant monitoring and risk assessment important in an organization?

**Answer**
It is important because it helps identify areas for improvement in the safety culture.

## 5.0 Conclusion

You have learnt from this unit that by understanding these links, organizations can create a robust cybersecurity posture that integrates risk management, incident response, and safety culture to protect their digital assets and reputation.

## 6.0 Summary

- Risk management informs incident response planning
- Incident response improves risk management by providing lessons learned
- Safety Culture supports risk management and incident response by promoting a proactive and accountable approach to cybersecurity
- A strong Safety Culture encourages employees to report incidents and near-misses, enabling swift response and continuous improvement

By understanding these links, organizations can create a robust cybersecurity posture that integrates risk management, incident response, and safety culture to protect their digital assets and reputation. In the next unit, you will be introduce to how to identify, classify and implement key risk management issue.

## 7.0 References/Further Readings

Alsmadi, I. (2023). Cyber Operational Planning. In I. Alsmadi, The NICE Cyber Security Framework (pp. 131–178). Springer International Publishing. https://doi.org/10.1007/978-3-031-21651-0_7.

# UNIT 4 KEY RISK MANAGEMENT IMPLEMENTATION ISSUES.

**Contents**



## 1.0 Introduction

You will learn from this unit how to identify, classify, and implement key risk management issues.

After studying this unit, you will be able to conceptualize risk management issues.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Identify, understand risk management implementation issues.
- Assess endless key risk management implementation issues in a structured approached.

## 3.0 Main Content

Key risk management implementation issues in cybersecurity refer to the common challenges and obstacles that organizations face when

implementing effective risk management practices to mitigate cyber threats.

## 3.1 Key risk management implementation issues in cybersecurity

1. Lack of Clear Ownership: Unclear responsibility for risk management leads to confusion and ineffective implementation.
2. Insufficient Resources: Inadequate funding, personnel, and technology hinder risk management efforts.
3. Limited Risk Awareness: Poor understanding of cybersecurity risks among stakeholders and employees.
4. Inadequate Risk Assessment: Incomplete or inaccurate risk assessments lead to ineffective mitigation strategies.
5. Inefficient Risk Prioritization: Failure to prioritize risks based on likelihood and impact leads to wasted resources.
6. Inadequate Risk Mitigation: Ineffective or incomplete implementation of risk mitigation controls.
7. Lack of Continuous Monitoring: Failure to continuously monitor and review risk levels and controls.
8. Inadequate Incident Response: Poor incident response planning and execution exacerbate cybersecurity incidents.
9. Insufficient Training and Awareness: Lack of regular training and awareness programs for employees.
10. Inadequate Third-Party Risk Management: Failure to assess and mitigate risks associated with third-party vendors and services.
11. Lack of Integration with Existing Processes: Risk management not integrated with existing security processes and procedures.
12. Inadequate Risk Reporting: Poor reporting of risk levels and incident response to stakeholders.
13. Lack of Flexibility: Inability to adapt risk management strategies to evolving threats and technologies.
14. Overreliance on Technology: Excessive reliance on technology without proper human oversight and intervention.
15. Inadequate Board-Level Support: Lack of support and engagement from senior management and the board of directors.

Addressing these implementation issues is crucial to effective risk management in cybersecurity.

## 3.2 Addressing Key Risk Management Implementation Issues in Cyber-Security

Addressing key risk management implementation issues in cyber security requires a structured approach.

Here are some steps to help overcome these challenges:

1. Establish a clear risk management framework and policies.
2. Conduct regular risk assessments and prioritize threats.
3. Allocate sufficient resources and budget for risk mitigation.
4. Foster effective communication and collaboration between teams.
5. Implement robust risk mitigation and control measures.
6. Provide regular cybersecurity awareness and training.
7. Stay up-to-date with evolving threats and technologies through continuous monitoring and learning.
8. Develop and regularly test incident response plans.
9. Establish effective risk metrics and reporting processes.
10. Integrate risk management into existing processes and culture.

Additionally:

1. Engage leadership and stakeholders to champion risk management.
2. Utilize industry frameworks and standards (e.g., NIST, ISO 27001).
3. Continuously monitor and evaluate the risk landscape.
4. Implement a threat intelligence program.
5. Foster a culture of cybersecurity awareness and responsibility.

By addressing these implementation issues, organizations can strengthen their cyber risk management capabilities and reduce the likelihood and impact of cyber-attacks.

## 4.0 Self-Assessment Exercise(s)

1. Explain in simple terms risk management implementation issues in cybersecurity.

**Answer**
This refers to the common challenges and obstacles that are often faced by organizations in implementing effective risk management practices in a bid to mitigate cyber threats.

2. State the vision and mission of the national cybersecurity policy.

**Answer**
The vision is to build a secure and resilient cyberspace for citizens, businesses, and government while protecting user privacy.

The mission is to protect information and infrastructure in cyberspace, develop capabilities to prevent and respond to cyber threats, and minimize damage from cyber incidents through a combination of structures people processes, technology, and cooperation.

## 5.0 Conclusion

You have learnt from this unit, how to identify, classify and implement key risk management issues.
You are also able to conceptualize risk management issues.

## 6.0 Summary

At the end of this unit, you have learnt to identify and explore risk management implementation issues. You have also learnt to access key risk management issues in a structured approach.

## 7.0 References/Further Readings

Alamdari, A. M., Jabarzadeh, Y., Adams, B., Samson, D., & Khanmohammadi, S. (2023). An analytic network process model to prioritize supply chain risks in green residential megaprojects. Operations Management Research, 16(1), 141–163. https://doi.org/10.1007/s12063-022-00288-2

Alsmadi, I. (2023). Cyber Operational Planning. In I. Alsmadi, The NICE Cyber Security Framework (pp. 131–178). Springer International Publishing. https://doi.org/10.1007/978-3-031-21651-0_7

Salah, B., Alnahhal, M., & Ali, M. (2023). Risk prioritization using a modified FMEA analysis in industry 4.0. Journal of Engineering Research, 11(4), 460–468. https://www.sciencedirect.com/science/article/pii/S2307187723001645

# MODULE 2: PRACTICAL RISK ASSESSMENT DEMONSTRATION

## Module Introduction

Risk assessment in the context of cybersecurity entails rolling out steps for identifying, analyzing, and evaluating risk in a bid to ensure that the cybersecurity controls chosen are proportionally appropriate to the risks faced by an organization. Risk assessment is significant in informing one's cyber security choices to minimize the waste of resources - time, effort, and money.

The Module attempts to take a swipe at Risk assessment demonstration, Risk control options, Risk prioritization and decision-making, and Risk assessment strategies.

Unit 1: Risk Assessment Demonstration
Unit 2: Risk Control Options.
Unit 3: Risk Prioritization and Decision Making.
Unit 4: Risk Assessment Strategies

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

## UNIT 1: RISK ASSESSMENT DEMONSTRATION

## Contents

## 1.0 Introduction

You will learn from this unit the concept of risk assessment and how to demonstrate and conduct risk assessment. After standing the unit, you will be equipped with the skills to define, identify, evaluate, and prioritize risks within an organization. You will also have the requisite background knowledge for demonstrating how to carry out risk assessment.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Appraise that risks are ongoing, while vulnerabilities are temporary and ideally remediated to remove associated risks.

## 3.0 Main Content

The practical risk assessment demonstration in cybersecurity involves a systematic process to identify, evaluate, and prioritize cybersecurity risks within an organization's systems. Here are the key steps for a practical risk assessment demonstration in cybersecurity: (Bartusiak et al., 2023).

**Define the Context**: Begin by defining the scope of the risk assessment, including critical systems, networks, and data, while considering regulatory requirements and industry standards

**Compile Information Assets Inventory**: Create a comprehensive inventory of information assets, categorize them based on their significance and sensitivity to business operations, and understand their interconnections within the organization

**Analyze Threats**: Understand potential attackers' motives and methods to refine defenses effectively. This step empowers organizations to enhance their cybersecurity posture by addressing specific threats proactively

### 3.1 Identify Cybersecurity Risks

Use threat modelling techniques to identify potential threats and attack vectors that could target critical assets. This step aids in understanding

the tactics, techniques, and procedures commonly employed by threat actors. By mapping out potential threats, organizations can better prepare for and defend against various cyberattack methods.

## 3.2 Perform Vulnerability Assessment

Conduct vulnerability scans and assessments to detect weaknesses in systems, applications, and networks. Once identified, patch or mitigate these vulnerabilities to lower the probability of successful attacks. Regular vulnerability assessments ensure that potential entry points for attackers are promptly addressed, enhancing overall security posture.

## 3.3 Develop Risk Scenarios

Create cyber risk scenarios that outline specific threats and their potential impact on critical assets. Analyze the likelihood and consequences of these scenarios to prioritize risk mitigation efforts. By developing detailed risk scenarios, organizations can focus their resources on the most significant threats, ensuring that critical vulnerabilities are addressed first.

## 3.4 Understand Risks vs. Vulnerabilities:

Differentiate between risks and vulnerabilities/issues. Risks are ongoing, while vulnerabilities are temporary and ideally remediated to remove associated risks. Periodic vulnerability assessments are crucial for improving IT security posture

## 3.5 Engage External Experts

Consider engaging external security experts or firms to conduct independent assessments for a fresh perspective and additional insights into cybersecurity risks

By following these steps and incorporating best practices from the sources provided, organizations can effectively demonstrate a practical risk assessment in cybersecurity. This approach helps in identifying, assessing, and mitigating risks to protect critical assets and maintain a strong cybersecurity posture.

## 4.0 Self-Assessment Exercise(s)

1. What is a risk assessment demonstration in cybersecurity?

**Answer**
Risk assessment demonstration involves a systematic process to identify, evaluate and optimize cybersecurity risks within an organization's systems.

2. Why perform vulnerability assessment?

**Answer**
The main reason is to scan and assess systems applications and networks to detect weaknesses in order to lower the probability of successful attacks.

## 5.0 Conclusion

You have learnt from this unit, the concept of risk assessment and how to demonstrate and conduct a risk assessment. You have also been equipped with skills to define, identify, evaluate, and prioritize risks within an organization.

## 6.0 Summary

At the end of this unit, you have learnt how to appraise risks, and vulnerabilities and how to minimize risk. In the next unit, you will be introduced to the concept of risk control in cyber security and how to apply options as a proactive measure to minimize risks and reduce the likelihood of adverse events.

## 7.0 References/Further Readings

Bartusiak, A., Kühne, M., Nitschke, O., Lässig, J., Nicolai, S., & Bretschneider, P. (2023). First step into automation of security assessment of critical infrastructures. Sustainable Energy, Grids and Networks, 36, 101139. https://www.sciencedirect.com/science/article/pii/S2352467723001479

# UNIT 2: RISK CONTROL OPTIONS

## Contents



## 1.0 Introduction

You will learn from this unit the concept of risk control in cybersecurity and how to apply risk options as a proactive measure to minimizing risks and reduce the likelihood of adverse events.

After studying the unit, you will be equipped with the skills of establishing contingency plans to respond to unforeseen events.
You will also have the requisite background knowledge for building techniques for creating contingency plans in the midst of unforeseen events.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Appraise the necessity of personal protective equipment (PPE) which translates to using risk control technologies and tools for extra defence such as regulating antivirus and antimalware software**.**

## 3.0 Main Content

Risk control involves systematic and proactive measures to minimize, mitigate, or manage various risks. The primary goal is to reduce the likelihood of adverse events and limit their impact. This includes

identifying potential risks, implementing preventive measures, and establishing contingency plans to respond to unforeseen events. (Alsmadi, 2023).

## 3.1 Steps of Risk Control Hierarchy in Cybersecurity

Level 1: Eliminating the Risk

The highest level of protection is risk elimination. This involves identifying and assessing vulnerabilities and threats within the organization's digital infrastructure and systems. Effective measures to eliminate these risks include:

- Closing unnecessary network ports and services.
- Decommissioning or replacing unsupported legacy systems.
- Educating employees on cybersecurity best practices to reduce human error.

Level 2: Substituting the Risk

When risk elimination is not feasible, the next step is risk substitution. This involves replacing a high-risk element with a lower-risk alternative, such as:

- Substituting vulnerable software with more secure alternatives.
- Implementing multi-factor authentication (MFA) instead of relying solely on passwords.

Level 3: Isolating the Risk

Risk isolation involves separating critical systems and data from potential threats, which can be achieved through:

- Network segmentation to isolate sensitive data and systems.
- Implementing firewalls and intrusion detection/prevention systems to create barriers between internal systems and external threats.

Level 4: Engineering Controls

Engineering controls focus on integrating security features into the digital infrastructure. These controls target the source of cyber threats and can include:

- Encrypting sensitive data to prevent unauthorized access.

- Regularly patching and updating software and systems to address vulnerabilities.
- Using network monitoring tools to detect and respond to cyber threats in real-time.

Level 5: Administrative Controls

Administrative controls involve policies, procedures, and training to enhance cybersecurity practices, such as:

- Developing and enforcing IT security policies outlining acceptable use and security protocols.
- Conducting regular cybersecurity training and awareness programs for employees.
- Creating an incident response plan to guide actions in the event of a security breach.

Level 6: Personal Protective Equipment (PPE)

In cybersecurity, PPE translates to using risk control technologies and tools for additional defence, including:

- Deploying antivirus and anti-malware software to protect against known threats.
- Implementing intrusion detection systems to monitor network traffic for suspicious activities.

By following this hierarchy, organizations can systematically assess and address cyber threats, strengthening their cybersecurity posture and reducing the likelihood and impact of cyberattacks.

## 4.0 Self-Assessment Exercise(s)

1. What is the primary goal of applying risk control in cybersecurity?

Answer
Basically, applying risk control helps to reduce the probability of adverse events and limit their impact; this includes identifying potential risks, implementing preventive measures and establishing contingency plans to respond to unforeseen events.

2. State the six (6) steps of risk control in cybersecurity.

Answer
Level 1: Eliminating the risk
Level 2: Risk substitution
Level 3: Isolating the risk
Level 4: Engineering controls
Level 5: Administration controls
Level 6: Personal Protective Equipment (PPE)

## 5.0 Conclusion

You have learnt from this unit the concept of risk control in cyber security and how best to apply risk options as a proactive measure in mitigating risks in a bid to reduce the likelihood of adversity. You have also been equipped with the skills of establishing contingency plans to respond to unforeseen events.

## 6.0 Summary

At the end of this unit, you have learnt to appraise the necessity of personal protective equipment (PPE) which translate to using risk control technologies and tools for extra defence such as regulating anti-virus and anti-malware software. In the next unit you will be introduced to the concept of risk prioritization in the phase of decision making and how to set priorities based on the likelihood of a risk occurring and its potential impact.

## 7.0 References/Further Readings

Bartusiak, A., Kühne, M., Nitschke, O., Lässig, J., Nicolai, S., & Bretschneider, P. (2023). First step into automation of security assessment of critical infrastructures. Sustainable Energy, Grids and Networks, 36, 101139. https://www.sciencedirect.com/science/article/pii/S2352467723001479

# UNIT 3: RISK PRIORITIZATION AND DECISION-MAKING

## Contents



## 1.0 Introduction

You will learn from this unit the concept of risk prioritization in the face of decision-making and how to set priorities based on the likelihood of a risk occurring and its potential impact.

After studying the unit, you will be equipped with the basic skills of making and setting priorities based on the likelihood of occurrence of risking events, looking at the seismic activity history; for example, earthquake, whose occurrence is low, and making it have a lower priority than critical assets such as data centers and the probability of a cyberattack which are of top priority.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Appraise the need for prioritizing risks on the basis of risk classification – tolerable risk, low risk and medium risk.

## 3.0 Main Content

Risk prioritization involves identifying and addressing the most critical risks first. Priorities should be set based on the likelihood of a risk occurring and its potential impact. For example, while an earthquake might have a high impact, its likelihood in a location with no seismic activity history is low, making it a lower priority. Conversely, if your

critical assets are data centers, the likelihood and impact of a cyberattack are high, making it a top priority. (Salah et al., 2023).

## 3.1 Levels of Risk Prioritization

- Tolerable Risk: Insignificant risks with very low chances of harm.
- Low Risk: Minor risks with negligible chances of negative consequences.
- Medium Risk: Moderate risks that could cause significant harm but are not serious threats.
- High Risk: Critical risks that could severely affect a project's success and have significant adverse repercussions.
- Intolerable Risk: Catastrophic risks that cause significant system loss, necessitating the termination of procedures, systems, or productivity.

Prioritizing risks forms the basis for resource allocation, ensuring that mission-critical needs are addressed and resources are maximized.

## 4.0 Self-Assessment Exercise(s)

1. What is the rationale behind risk assessment?

**Answer**
The rationale for risk assessment is mainly to identify which assets are most vulnerable to cyber risks.

2. State five (5) strategies in handling risk assessment strategies in cybersecurity.

**Answer**

i. Identify and prioritize risk
ii. Identify the most critical information technology assets.
iii. Carryout threat analysis.
iv. Vulnerability assessment.
v. Risk response planning.

## 5.0 Conclusion

You have been equipped with the basic skills of making and setting priorities based on the likelihood of occurrence of risky events, looking at the seismic activity history. For instance, earthquakes, which are low and making have a lower priority than critical assets such as data centers, and the probability of the cyber-attack which are of top priority.

## 6.0 Summary

At the end of this unit, you have conceptualized the need for prioritizing risks based on risk classification- tolerable risk, low risk, and medium risk. In the next unit, you will be introduced to methods of conducting risk assessment.

## 7.0 References/Further Readings

Salah, B., Alnahhal, M., & Ali, M. (2023). Risk prioritization using a modified FMEA analysis in Industry 4.0. Journal of Engineering Research, 11(4), 460–468. https://www.sciencedirect.com/science/article/pii/S2307187723001645

# UNIT 4: RISK ASSESSMENT STRATEGIES.

## Contents



## 1.0 Introduction

You will learn from this unit how to conduct risk assessments. After studying this unit you will be able to manage, and mitigate cyber risks by completing a cybersecurity risk assessment in an organization.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Conduct a cyber-risk assessment, following the effective strategies to mitigate the risk of a cyber-attack.

## 3.0 Main Content

Given that nearly all organizations have internet connectivity and IT infrastructure, they are all at risk of cyberattacks. To manage this risk, organizations need to complete a cybersecurity risk assessment. (Alamdari et al., 2023).

### 3.1 Effective risk assessment strategies

This process identifies which assets are most vulnerable to cyber risks. Effective strategies include:

- Identify and Prioritize Risks: Begin by identifying and prioritizing risks to organizational operations, assets, individuals, and other entities resulting from the use of information systems
- Asset Identification: Identify the most critical information technology assets within your organization
- Threat Analysis: Recognize potential threats to your assets, including malware, cyber-attacks, or human errors, and evaluate the vulnerabilities in your systems
- Risk Estimation and Evaluation: Estimate the level of potential impact of each identified threat and evaluate the likelihood of exploitation
- Vulnerability Assessment: Identify internal and external vulnerabilities and assess the impact of these vulnerabilities are exploited
- Risk Response Planning: Develop IT security controls and data security strategies for risk remediation based on the identified risks
- Continuous Monitoring: Implement continuous monitoring of systems to detect and respond to suspicious activities in real time.
- Incident Response Planning: Develop an Incident Response Plan (IRP) outlining roles, responsibilities, and steps to manage cyber incidents effectively
- Layered Security Approach: Implement multiple layers of security, including firewalls, intrusion detection systems, access controls, and endpoint protection, to enhance defense mechanisms.

Regular Risk Assessments: Conduct comprehensive enterprise security risk assessments at least annually or when significant changes occur in the business or IT environment

## 4.0 Self-Assessment Exercise(s)

1. Define risk assessment in cybersecurity.

**Answer**
This is the process of trying to manage and forestall risks by completing a cybersecurity assessment, identifying which assets are most vulnerable to cyber risk.

2. State and briefly explain three (3) strategies used for risk assessment in an organization.

**Answer**

i. Identifying and prioritizing risks: this has to do with identifying and prioritizing organizational operations, assets, individuals and other entities resulting from the use of information systems.
ii. Assets identification: this has to do with the identification of the most critical information technology assets within your organization.
iii. Threat analysis: this has to do with recognizing potential threats to your assets, including malware, cyber-attacks in an bid to evaluate the vulnerabilities in your systems.

## 5.0 Conclusion

You have learnt from this unit how to conduct risk assessment. In the same unit you have learnt to manage, mitigate cyber risks by completing the cyber security risk assessment in an organisation

## 6.0 Summary

At the end of this unit you already know how to conduct a cyber-risk assessment following the effective strategies to mitigate the cyber-attack.

## 7.0 References/Further Readings

Alamdari, A. M., Jabarzadeh, Y., Adams, B., Samson, D., & Khanmohammadi, S. (2023). An analytic network process model to prioritize supply chain risks in green residential megaprojects. Operations Management Research, 16(1), 141–163. https://doi.org/10.1007/s12063-022-00288

# MODULE 3: INCIDENT INVESTIGATION BASICS AND TERMINOLOGY

## Module Introduction

Oftentimes, cyber incident reports act as tools in helping organizations learn more about incidents to build and improve their risk management strategy.

Essentially, awareness is raised about new and emerging cyber threats, attack patterns, cracks in already existing security infrastructure, and other malicious tendencies.

The Module explores some useful concepts such as the basics of incident investigation, interviewing and facts-gathering techniques, and Root cause analysis.

This module is classified into the following four (4) units:

Unit 1: Incident Investigation.
Unit 2: Process of Incident Investigation.
Unit 3: Interviewing and Facts Gathering Techniques.
Unit 4: Root Cause Analysis. (RCA)

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

## UNIT 1: INCIDENT INVESTIGATION

## Contents

7.0 References/Further Readings

## 1.0 Introduction

You will learn from this unit how to investigate an incident, and the basics and terminologies involved in the context of cyber security; after studying this unit, you will be able to learn technologies of incident investigation from the basics of incident detection, incident recognition, and incident management process.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Conduct incident investigation in the context of cybersecurity ranging from incident detection, incident recognition and incident management.

## 3.0 Main Content

### 3.1 Incident Investigation Basics

#### 3.1.1 Incident Detection

The act of identifying the cause of an investigation to be a confirmed malicious activity by a threat actor. This involves escalating an alert to an incident, which is then investigated to determine whether it is a false positive or a genuine incident

#### 3.1.2 Incident Recognition

The act of recognizing an incident, which is triggered by an event or a set of correlated events that indicate suspicious activity. This can be escalated to an incident if the activity is confirmed as malicious

#### 3.1.3 Incident Management Process

The process of managing an incident from detection to resolution. This includes incident handling, incident response, and incident resolution.

## 3.2 Incident Terminologies

Some Incident Terminologies Include:

1. **Alert**: One or more events that correlate to a programmed alarm rule within a Security Information and Event Management (SIEM) system. Alerts are investigated to determine whether they are false positives or genuine incidents
2. **False Positive**: An alert that is investigated and found not to be a genuine incident. False positives are typically resolved through the incident management process
3. **Incident**: A confirmed malicious activity by a threat actor. Incidents are investigated and managed through the incident management process
4. **Threat Actor**: An individual or group that carries out malicious activities, such as cyber attacks
5. **Cyber Insider Threats**: Threats that come from within an organization, including employees, former employees, contractors, vendors, and suppliers. Insider threats can be due to negligence, malicious intent, or infiltration
6. **Cyber Kill Chain**: A model that outlines the different stages of a cyber attack, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions and objectives
7. **Cybersecurity**: The processes and strategies employed to safeguard and secure assets used to carry information within an organization from being stolen or attacked
8. **Data Breach**: An incident where a hacker successfully exploits a vulnerability in a network or device, gaining unauthorized access to its files and data.
9. **Data Integrity**: The maintenance and assurance of data quality, ensuring its accuracy and consistency throughout its entire lifecycle.
10. **Sandbox**: An isolated environment within a network that mimics end-user operating environments, allowing for the safe execution of suspicious code without risking harm to the host device or network.
11. **Security Incident Response**: A planned approach to addressing and managing the aftermath of a cyber-attack or network security breach, to minimize damage and reduce disaster recovery time through predefined procedures.
12. **Security Operations Center (SOC)**: A dedicated facility where enterprise information systems are continuously monitored, assessed, and defended by SOC analysts.

13. **Security Policy**: A statement outlining how an organization expects its staff to behave and its systems to operate to maintain security.
14. **Security Posture**: The overall state of an organization's systems in terms of security, including its preparedness to respond to a security incident.
15. **Security Information and Event Management (SIEM)**: A system that aggregates log and event data from various sources, providing real-time monitoring and incident detection.

## 4.0 Self-Assessment Exercise(s)

1. What is incident investigation in cybersecurity?

**Answer**
This entails carrying out analysis, responding to a cyber-attack including breach, malfunction in a bid to determine the carrier, extend and impact of an cyber incident.

2. What are the three (3) basic elements of incident investigation?

**Answer**
The three (3) elements are:

i. Incident detection: - Identifying the cause of an investigation to be a confirmed malicious activity by a threat actor.
ii. Incident recognition: - recognizing an incident, which is triggered by an event or a set of correlated events that indicate suspicious activity.
iii. Incident management process: - Managing an incident from detection to resolution

## 5.0 Conclusion

In this unit, you have learned how to investigate an incident, and the basics and terminologies involved in the context of cyber security. You have also learnt about technologies of incident investigation from the basics, incident detection, incident recognition, and incident management process

## 6.0 Summary

In this unit, you have learnt to conduct incident investigations in the context of cybersecurity ranging from incident detection, incident recognition, and incident management. In the next unit, you will learn to conceptualize incident investigation in cybersecurity

## 7.0 References/Further Readings

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Computers & Security, 135, 103525. https://www.sciencedirect.com/science/article/pii/S0167404823004352

Romaniuk, S. N., & Hattiangady, P. (n.d.). Cybercrime, National Security, and Internet Governance. In The Handbook of Homeland Security (pp. 211–230). CRC Press. Retrieved June 29, 2024, from https://www.taylorfrancis.com/chapters/edit/10.4324/9781315144511-34/cybercrime-national-security-internet-governance-scott-romaniuk-priyanka-hattiangady

# UNIT 2: PROCESS OF INCIDENT INVESTIGATION

## Contents



## 1.0 Introduction

You will learn from this unit to conceptualize incident investigation and how it is being conducted in cybersecurity. After studying this unit, you will be able to carry out the process of incident investigation using key steps.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

Carryout the process of incident investigation using the key steps

## 3. Main Content

### 3.1 Key steps of incident investigation

The process of incident investigation in cybersecurity involves several key steps to identify, contain, and resolve security incidents effectively. Here are the key steps:

### 3.1.1 Identification

**Speed is of the essence**: Identify the incident as quickly as possible to minimize the damage and prevent further exploitation

**Automated detection tools**: Utilize automated threat detection tools to issue alerts when suspicious activity is detected

**Human detection**: Employees or IT teams may also identify incidents through manual monitoring or reporting suspicious activity.

### 3.1.2 Initial Investigation

**Preliminary investigation**: Conduct a preliminary investigation to identify all systems and services affected by the incident, and document any sensitive information compromised

**Interviews and evidence gathering**: Interview personnel who discovered the breach and gather relevant evidence to understand the scope of the incident

**Notification of authorities**: Notify law enforcement and regulatory bodies as necessary

### 3.1.3 Immediate Action

**Isolation of affected areas**: Isolate the affected areas to prevent further contamination of evidence and to gather relevant information

**Containment and eradication**: Contain and eradicate the threat to prevent further damage

### 3.1.4 Analysis

**Data analysis**: Analyze the gathered data to understand how the incident occurred, what information was compromised, and how long it was compromised

**Root cause analysis**: Identify the root cause of the incident to prevent similar incidents in the future

### 3.1.5 Remediation Planning

**Remediation planning**: Develop a comprehensive plan to remediate the incident, including steps to prevent similar incidents and estimates for the time required to complete remediation tasks

**Prioritization and resource allocation**: Prioritize remediation tasks and allocate resources accordingly

### 3.1.6 Post-Incident Activities

**Debriefing and lessons learned**: Conduct debriefing sessions to reflect on the incident, assess the extent of the attack, and identify areas for improvement

**Notification and communication**: Notify stakeholders and communicate the incident and its resolution to maintain transparency and trust

**Incident reporting**: Document the incident and its resolution in a cybersecurity incident report, outlining the steps taken to mitigate the incident and prevent future occurrences

These steps form the core of the incident investigation process in cybersecurity, ensuring that incidents are identified and resolved efficiently to minimize damage and maintain the security and integrity of digital assets.

## 4.0 Self-Assessment Exercise(s)

1. What is incident investigation in cybersecurity?

This simply involves the process of rolling out all the key steps of digging into a cyber-incident cause, and extent of impact with the aim of proffering solutions.

2. State five (5) steps of incident investigation in cybersecurity.

**Answer**

i. Automated detection tools
ii. Interviews and evidence
iii. Fact Gathering
iv. Isolation of affected areas
v. Root cause analysis

## 5.0 Conclusion

You have learnt from this unit to carry out incident investigations in cybersecurity. You have also learnt how to carry out an incident investigation using key steps

## 6.0 Summary

At the end of this unit, you have learnt to carry out the process of incident investigation using the key steps.

In the next unit, you learn the process of interviewing and fact-gathering techniques and the vital role they will play in cybersecurity investigations, incident response and risk assessments.

## 7.0 References/Further Readings

Robinson, O. C. (2023). Probing in qualitative research interviews: Theory and practice. Qualitative Research in Psychology, 20(3), 382–397. https://doi.org/10.1080/14780887.2023.2238625

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, 132, 103309. https://www.sciencedirect.com/science/article/pii/S0167404823002195

# UNIT 3: INTERVIEWING AND FACTS GATHERING TECHNIQUES.

**Contents**



## 1.0 Introduction

You will learn from this unit how interviewing and fact-gathering techniques play a vital role in cybersecurity investigations, incident response, and risk assessments. You will also learn some commonly used techniques.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Demonstrate interviewing and fact-gathering techniques in carrying out investigations regarding incidents in cybersecurity.

## 3.0 Main Content

### 3.1 Interviewing and Fact-Gathering Techniques

Interviewing and fact gathering techniques play a crucial role in cybersecurity investigations, incident response, and risk assessments. Here are some commonly used techniques:

1. Structured Interviews: Conducting interviews with stakeholders, system administrators, and other relevant personnel using predefined questions to gather specific information about security incidents, system configurations, access controls, and other relevant details.

2. Open-Ended Interviews: Allowing interviewees to provide narrative responses, which can uncover unexpected information or details that might not have been captured by structured questions (Robinson, 2023). This technique can be useful for understanding the context of security incidents or exploring areas where little information is available.
3. Forensic Interviews: Conducting interviews with individuals involved in security incidents in a manner that preserves the integrity of potential evidence for forensic analysis. These interviews often follow specific protocols to ensure that the information obtained can be used in legal proceedings if necessary.
4. Document Review: Examining documentation such as incident reports, system logs, network diagrams, security policies, and procedures to gather information about security incidents, vulnerabilities, and control measures in place.
5. Observation: Observing system behavior, network traffic, and user activities in real-time or through system logs and monitoring tools to identify potential security issues or anomalies.
6. Surveys and Questionnaires: Distribute surveys or questionnaires to employees, customers, or other relevant stakeholders to gather information about security awareness, training needs, and perceptions of security risks.
7. Threat Intelligence Gathering: Collecting information from various sources such as threat intelligence feeds, security advisories, and online forums to identify emerging threats, vulnerabilities, and attack trends that may pose a risk to the organization.
8. Social Engineering Testing: Simulating social engineering attacks such as phishing emails, pretexting calls, or physical security breaches to assess the effectiveness of security awareness training and identify areas for improvement.
9. Vulnerability Scanning and Penetration Testing: Using automated tools and manual techniques to identify vulnerabilities in systems and networks, and to assess the effectiveness of security controls in place.
10. Collaborative Workshops and Brainstorming Sessions: Bringing together stakeholders from different departments or teams to discuss security risks, potential threats, and mitigation strategies in a collaborative environment.

## 4.0 Self-Assessment Exercise(s)

1. What do you understand by a forensic interview?

**Answer**

This has to do with conducting interviews with individuals involved in security incidents in a manner that preserves the integrity of potential evidence for forensic analysis.

2. Define vulnerability scanning and penetration restoring.

**Answer**

This entails using automated tools and manual techniques to identify vulnerabilities in systems and networks and assess the effectiveness of security controls.

## 5.0 Conclusion

You have learnt from this unit how interviewing and fact-finding techniques play a vital role in cybersecurity investigations, incident response, and risk assessments. You were also exposed to some commonly used techniques

## 6.0 Summary

At the end of this unit, you have learnt how to demonstrate interviewing and fact-finding techniques in investigating incidents in cybersecurity.
In the next unit, you will learn how to use standard techniques to carry out Root Cause Analysis in cyber security

## 7.0 References/Further Readings

Robinson, O. C. (2023). Probing in qualitative research interviews: Theory and practice. *Qualitative Research in Psychology*, *20*(3), 382–397. https://doi.org/10.1080/14780887.2023.2238625

# UNIT 4: ROOT CAUSE ANALYSIS. (RCA)

## Contents



## 1.0 Introduction

You will learn from this unit how to use standard techniques to carry out root cause analysis in cybersecurity. After studying this unit, you will be able to identify the root cause of any cyber incident.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:
Identify the root cause of an incident using a basic framework.

## 3.0 Main Content

### 3.1 Root Cause Analysis in Cybersecurity

Root cause analysis (RCA) is the methodology used to identify the origin of a problem, with the aim of implementing measures to prevent recurrence(Lakbala et al., 2024). RCA operates on the principle that addressing the root cause of an issue is more effective than merely treating its symptoms.

## *3.2* Identifying a Root Cause

There is no universal method for pinpointing a problem's root cause; the process can differ across industries and organizations. In software projects, RCA is typically carried out by a specialized team familiar with the issue, led by an RCA manager(Liepelt et al., 2023). This function often aligns with "incident response," where root cause analyses are conducted as part of a post-incident review.

A basic framework for RCA includes the following steps:

- **Identify the Problem**: Start by defining a clear problem statement and identifying symptoms, such as a machinery malfunction, a failed process, or human error. Isolate suspected contributing factors to contain the problem while investigating the root cause.
- **Collect Data**: Gather comprehensive data, including incident reports, evidence (screenshots, logs), and interviews with involved personnel. This data helps establish the sequence of events, identifying adverse events leading to the problem, involved systems, the duration of the issue, and its overall impact.
- **Determine Root Cause**: The RCA team conducts brainstorming sessions using tools like Fishbone diagrams and Pareto charts to uncover the root cause. These sessions, moderated by the RCA manager, should be collaborative and free from blame.
- **Implement the Solution**: Based on the identified root cause, determine the best solution and plan its implementation. Monitor the effectiveness of the solution, a process formally known as Root Cause Corrective Action.
- **Document Actions**: Document the problem and its resolution to prevent recurrence. Include recommendations for physical or process improvements and preventive measures in the documentation.

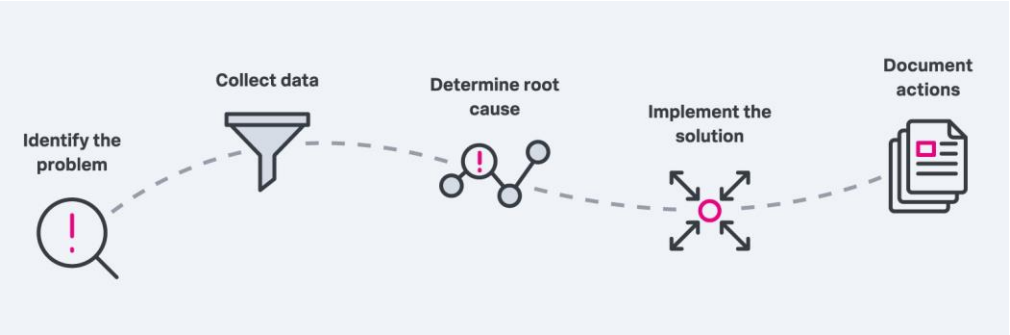



**Figure 3.1:** Key Steps for Root Cause Analysis

## 3.3 Key Steps for Root Cause Analysis

Root cause analysis often follows the Six Sigma approach to quality management, which aims to improve business processes by identifying defects, understanding their causes, and enhancing processes to reduce variability and increase consistency. The Six Sigma DMAIC framework—Define, Measure, Analyze, Improve, Control—guides this process.

In the "Analyze" phase, Six Sigma employs five types of analyses: source, process, data, resource, and communication analysis. Source analysis, in particular, uses a three-step RCA process:

- **Open Step**: Brainstorm all potential explanations for the problem using techniques like the cause-and-effect Fishbone diagram.
- **Narrow Step**: Refine the list of possible explanations.
- **Close Step**: Validate the narrowed list of potential causes.

Six Sigma applies to improving IT operations and software development processes, helping to identify reasons for system failures, high defect rates, missed deadlines, and other issues affecting product quality, system performance, and customer satisfaction.

## 3.4 Core Principles of Root Cause Analysis

Effective RCA is guided by several core principles:

- **Focus on the Root Cause**: The main goal is to identify and correct the underlying cause to prevent recurrence, although addressing symptoms can provide short-term relief.
- **Systematic Investigation**: RCA requires a structured approach and appropriate procedures to yield accurate results.
- **Multiple Root Causes**: Most problems have more than one root cause.
- **Relationship Establishment**: The analysis must establish a connection between the problem, its root cause, and contributing factors using a timeline or sequence of events.
- **Blameless Approach**: RCA should focus on how and why the problem occurred, avoiding blame to encourage full participation.
- **Evidence-Based Conclusions**: Root cause conclusions must be supported by factual evidence, not opinions or guesses.
- **Multiple Solutions**: A single root cause can suggest multiple solutions.

- **Efficient and Cost-Effective Solutions**: Solutions should aim to prevent recurrence in the most efficient way and at the lowest cost.

RCA is a comprehensive problem-solving approach that seeks to uncover the root cause and provide sufficient context to suggest effective corrective actions

## 4.0 Self-Assessment Exercise(s)

1. What is Root Cause Analysis (RCA)?

This is the methodology used to identify the origin of a problem (cyber incident), and to implement measures to prevent recurrence. Operating on the root of an issue is more effective than simply focusing on its symptoms.

2. State four (4) steps of conducting RCA.

**Answer**

The steps are:

i. Identification of the problem
ii. Collection of data
iii. Determine the root cause
iv. Implement the solution

## 5.0 Conclusion

You have learnt from this unit how to use standard techniques in carrying out Root Cause Analysis. You have also learnt to identify a Root Cause of any cyber incident.

## 6.0 Summary

At the end of this unit, you have learnt to identify the root cause of an incident using the basic framework. You also learnt various steps in conducting root cause analysis.

## 7.0 References/Further Readings

Lakbala, P., Bordbar, N., & Fakhri, Y. (2024). Root cause analysis and strategies for reducing falls among inpatients in healthcare facilities: A narrative review. Health Science Reports, 7(7), e2216. https://doi.org/10.1002/hsr2.2216

Liepelt, S., Sundal, H., & Kirchhoff, R. (2023). Team experiences of the root cause analysis process after a sentinel event: A qualitative case study. BMC Health Services Research, 23(1), 1224. https://doi.org/10.1186/s12913-023-10178-3

# MODULE 4 PRACTICAL INCIDENT INVESTIGATION EXECUTION.

## Module Introduction

Essentially, carrying out Incident investigation entails ascertaining and recognizing that a security incident has taken place. It involves the use of intrusion detection systems, data leakages prevention software and firewalls. The use of these tools can significantly help in monitoring and notifying the security team about any suspicious activity. The Module explores case study on incident investigation, incident report writing and presentation.

This module is classified into the following four (4) units:

Unit 1: Incident Investigation execution.
Unit 2: Case Study on Incident Investigation.
Unit 3: Incident Investigation, Report Writing and Presentation.
Unit 4: Practical Integration of Risk Management and Incident.

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit.

## UNIT 1: INCIDENT INVESTIGATION EXECUTION.

## Contents



## 1.0 Introduction

You will learn from this unit how to carry out incident investigation cybersecurity. After studying this unit, you will be able to master the systematic approach to identifying containing, and resolving cybersecurity incidents.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Conduct practical incident investigation execution in cybersecurity using a systematic approach to identifying, containing and resolving cybersecurity incidents.

## 3.0 Main Content

### 3.1 Incident Investigation execution.

Practical incident investigation execution in cybersecurity involves a systematic approach to identifying, containing, and resolving cybersecurity incidents. Here's a detailed explanation of the steps involved:

### 1. Preparation:

a. Establish an incident response plan and team
b. Define incident classification and prioritization criteria
c. Set up incident response tools and technologies (e.g., SIEM, IR platforms)

### 2. Identification:

a. Monitor systems and networks for suspicious activity
b. Use threat intelligence and analytics to identify potential incidents
c. Receive and respond to incident reports from users and systems

### 3. Initial Response (IR):

a. Activate the incident response plan and team
b. Assign an incident responder to lead the investigation
c. Provide initial guidance and support to affected parties

4. Incident Containment:

a. Isolate affected systems or networks to prevent further damage
b. Implement temporary fixes or workarounds to mitigate the impact

## 5. Evidence Collection:

a. Gather logs, network captures, and system images
b. Collect and preserve physical evidence (e.g., devices, media)
c. Use forensic tools and techniques to analyze evidence

## 6. Incident Analysis:

a. Analyze evidence to determine incident scope, cause, and impact
b. Identify affected systems, data, and users
c. Determine incident severity and priority

## 7. Incident Eradication:

a. Remove malware, backdoors, or other malicious artifacts
b. Implement permanent fixes or patches
c. Restore systems and data to a known good state

## 8. Incident Recovery:

a. Restore systems and data to production
b. Verify incident resolution and system integrity
c. Document incident closure

9. Incident Reporting:

a. Document incident details, including root cause, impact, and response actions
b. Report incidents to stakeholders, regulatory bodies, and law enforcement (as required)

10. Incident Review:

a. Conduct post-incident reviews to identify lessons learnt and areas for improvement
b. Refine incident response processes and procedures
c. Provide training and awareness programs for incident responders and stakeholders

## 3.2 Practical tips:

i. Establish a clear incident response plan and team
ii. Use automation and orchestration tools to streamline incident response
iii. Continuously monitor and improve incident response processes

iv. Communicate effectively with stakeholders and teams
v. Prioritize incident containment and eradication
vi. Document everything!

By following this structured approach, organizations can effectively execute incident investigations, minimize damage, and improve overall cybersecurity resilience.

## 4.0 Self-Assessment Exercise(s)

1. Outline the steps involved in incident investigation.

i. Preparation: - Establish an incident response plan
ii. Identification: - Monitor systems and networks for suspicious activity.
iii. iii. Initial Response (IR): - Activate the incident response plan and team.
iv. iv. Incident containment isolates affected systems networks to prevent more damage.
v. Evidence collection: gather logs, network captures, and system images.
vi. Incident analysis: analyze evidence to determine incident scope
vii. Incident Reporting: - Document incident details, including root cause, impact, and response actions.

## 5.0 Conclusion

You have learnt from this unit how to conduct incident investigations in cybersecurity.

You have also learnt the systematic approach of identifying, containing, and resolving cybersecurity incidents.

## 6.0 Summary

At the end of this unit, you have learnt to conduct practical incident investigation execution in cyber security using a systematic approach to identifying, containing, and resolving cybersecurity incidents.
In the next unit, you will learn how to conceptualize a case study on an incident investigation in cybersecurity.

## 7.0 References/Further Readings

Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., & Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. Computers & Security, 128, 103139. https://www.sciencedirect.com/science/article/pii/S0167404823000494

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Computers & Security, 135, 103525. https://www.sciencedirect.com/science/article/pii/S0167404823004352

# UNIT 2: CASE STUDY ON INCIDENT INVESTIGATION.

## Contents



## 1.0 Introduction

You will learn from this unit how to conceptualize a case study on incident investigation in the context of cybersecurity and using a large e-commerce company that experienced a security breach (That has to do with the theft of sensitive customer data including credit card members)

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Conduct incident investigation in cybersecurity using any selected case study.

## 3.0 Main Content

### 3.1 Case Study on Incident Investigation

Case Study: Incident Investigation in Cyber Security
Background:

A large e-commerce company, XYZ Inc., experienced a security breach resulting in the theft of sensitive customer data, including credit card numbers and personal information. (Kafi & Akter, 2023).
Incident Response:

- Detection: XYZ Inc.'s security team detected unusual network activity and received reports of suspicious emails from customers.
- Initial Response: The incident response team was activated, and an investigation began.
- Containment: Affected systems were isolated, and temporary fixes were implemented to prevent further data exfiltration.
- Evidence Collection: Logs, network captures, and system images were collected and analyzed using forensic tools.
- Analysis: Investigation revealed a phishing attack had compromised an employee's account, leading to malware deployment and data theft.
- Eradication: Malware was removed, and affected systems were restored to a known good state.
- Recovery: Customer data was restored from backups, and affected customers were notified.
- Reporting: The incident was reported to regulatory bodies and law enforcement.

## 3.2 Lessons Learned:

- Phishing attacks can have severe consequences.
- Regular security awareness training is essential for employees.
- Incident response plans must be regularly tested and refined.
- Customer data must be prioritized and protected.

## 3.3 Recommendations

1. Implement advanced threat detection and prevention tools.
2. Conduct regular security audits and vulnerability assessments.
3. Enhance incident response plan and team training.
4. Invest in customer data protection and encryption technologies.

By following a structured incident investigation process, XYZ Inc. was able to quickly identify the root cause of the breach, contain and eradicate the threat, and recover from the incident. The lessons learned and recommendations from this incident will help improve the company's overall cybersecurity posture and protect against future threats.

## 3.4 Additional case studies on incident investigation in cyber security

- Microsoft Incident Response Ransomware Case Study: This case study describes how Microsoft's incident response team investigated a ransomware incident.
- Cyber Security Incident Response Case Study by FRSecure: This case study examines a ransomware attack on a client's servers and backups.
- A Case Study of the Capital One Data Breach: This case study examines the Capital One data breach, in which a hacker accessed and stole the sensitive information of millions of people.
- International Case Report On Cyber Security Incidents: This case study examines the DigiNotar case, in which a cyber-attack resulted in the theft of sensitive information.
- The Stanford University Ransomware Attack: This case study examines a ransomware attack on Stanford University's computer systems.

## 4.0 Self-Assessment Exercise(s)

1. State three (3) recommendations that could come up after the conduct of a cyber incident investigation in an organization.

**Answer**

Three (3) possible recommendations could be;

i. Implement advanced threat detection and prevention tools
ii. Conduct regular security audits and vulnerability assessments iii. Enhance incident response plan and team training

2. Illustrate three (3) case studies on incident investigation in cybersecurity.

**Answer**

a. Microsoft Incident Response Ransomware Case Study: which describes how Microsoft’s incident response team investigated a ransomware incident.
b. Cybersecurity Incident Response Case Study by FIR Secure. This case study examines a ransomware attack on a client’s servers and backups.

c. International Case Report on Cybersecurity Incidents: This case study examines the DigiNotar case, in which a cyber-attack resulted in the theft of sensitive information.

## 5.0 Conclusion

You have learnt from this unit how to conceptualize case study on incident investigation on the contest of cybersecurity and using a large e-commerce company which experienced a security breach.

## 6.0 Summary

At the end of this unit you have learnt to conduct incident investigation in cybersecurity using a selected case study. Illustrations were also on three case studies such as Microsoft Incident Ransomware, Cybersecurity Incident Response Case Study by FIR Secure. In the next unit you will learn how to conduct incident investigation, report writing and presentation in cybersecurity.

## 7.0 References/Further Readings

Alsmadi, I. (2023). Cyber Operational Planning. In I. Alsmadi, The NICE Cyber Security Framework (pp. 131–178). Springer International Publishing. https://doi.org/10.1007/978-3-031-21651-0_7

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15–26. https://www.academia.edu/download/106082632/1188.pdf

# UNIT 3: INCIDENT INVESTIGATION, REPORT WRITING AND PRESENTATION.

## Contents



## 1.0 Introduction

You will learn from this unit how to conduct incident investigations, report writing, and presentation in cybersecurity.

After studying this unit you will be able to understand the basic rationale behind an incident investigation report and presentation being to document the findings, analysis, and conclusions of a cybersecurity incident investigation.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of the unit, you will be able to;

- Conduct incident investigation report writing and presentation, report writing and presentation in cyber security.

## 3.0 Main Content

## 3.1 Incident Investigation, Report Writing, and Presentation.

Incident investigation report writing in the context of cyber security refers to the process of documenting and reporting on the findings and results of a cyber-security incident investigation. (Patterson et al., 2023). The report provides a detailed account of the incident, including:

1. Incident description and scope
2. Investigation methodology and procedures
3. Findings and analysis (e.g., root cause, vulnerabilities, attacker TTPs, IOCs)
4. Impact and damage assessment
5. Recommendations for incident prevention and mitigation
6. Action plan and next steps
7. Appendices (supporting documents, logs, images, etc.)

The report aims to:

1. Provide a clear understanding of the incident and its impact
2. Identify vulnerabilities and weaknesses
3. Document incident response and containment efforts
4. Support incident prevention and mitigation
5. Enhance incident response capabilities and planning
6. Meet compliance and regulatory requirements

Effective incident investigation report writing in cyber security is crucial for:

1. Documenting incident details and findings
2. Communicating incident impact and recommendations
3. Supporting incident response and improvement
4. Demonstrating compliance and due care
5. Enhancing cyber security posture and resilience.

## 3.2 Purpose:

The purpose of an incident investigation report in cyber security is to document the findings, analysis, and conclusions of a cyber-security incident investigation, providing a clear and concise account of the incident, its impact, and the recommendations for improvement. (Mouratidis et al., 2023).

Structure:

1. Executive Summary: Brief overview of the incident, investigation, and key findings.

2. Incident Description: Detailed description of the incident, including:

- Date and time of incident
- Type of incident (e.g., malware, data breach, denial-of-service)
- Affected systems, networks, and data
- Known or suspected attackers

3. Investigation Methodology: Explanation of the investigation process, including:

- Tools and techniques used (e.g., forensic analysis, network logs)
- Data collection and analysis methods
- Interviews and statements from relevant parties

4. Findings: Presentation of the evidence and analysis, including:

- Root cause of the incident
- Incident severity and impact
- Affected data and systems
- Vulnerabilities exploited
- Malicious activity and indicators of compromise (IOCs)

5. Analysis: Interpretation of the findings, including:

- Identification of vulnerabilities and weaknesses
- Determination of incident severity and impact
- Analysis of attacker tactics, techniques, and procedures (TTPs)

6. Recommendations: Actionable suggestions for incident prevention, mitigation, and improvement, including:

- Security controls and countermeasures
- Incident response plan improvements
- Vulnerability remediation and patch management
- Security awareness training

7. Conclusion: Summary of the investigation, findings, and recommendations.

8. Appendices: Supporting documents, logs, images, and other relevant materials.

Content:

- Clearly define the incident and its scope

- Provide a timeline of events
- Identify affected systems, data, and personnel
- Document evidence collection and analysis
- Include interviews and statements from relevant parties
- Detail incident containment and eradication efforts
- Provide recommendations for incident prevention and mitigation
- Include a plan for implementing recommendations

## 3.3 Best Practices:

- Use a standardized report template
- Ensure clarity, concision, and objectivity
- Include visual aids (e.g., diagrams, flowcharts)
- Use proper grammar, spelling, and punctuation
- Review and edit the report carefully
- Ensure report confidentiality and access control
- Use incident response and reporting frameworks (e.g., NIST, SANS)

By following this structure and content guide, incident investigation reports in cyber security can effectively communicate the findings and recommendations of an incident investigation, supporting continuous improvement and incident prevention.

## 4.0 Self-Assessment Exercise(s)

1. Define incident investigation report writing in cybersecurity.

**Answer**

Incident investigation report writing in cybersecurity refers to the process of documenting and reporting on the findings and results of a cybersecurity incident investigation.

2. State the elements of a good incident investigation report writing and presentation.

**Answer**

The elements of a good incident investigation report writing are as follows:

i. Incident description and scope

ii. Investigation methodology and procedures
iii. Findings and analysis (e.g. root cause, vulnerabilities, attacker TTPs, IOCs)
iv. Impact and damage assessment
v. Recommendations for prevention and mitigation.

## 5.0 Conclusion

You have learnt from this unit how to conduct incident investigations, report writing, and presentation. You have also learnt in this unit about the rationale behind incident investigation reports and presentations – to document the findings, analysis, and conclusion of a cyber-security incident investigation.

## 6.0 Summary

At the end of this unit, you have learnt to conduct incident investigation, report writing, and presentation in cybersecurity; in addition, illustrations were made on the various elements of a good incident investigation report.

In the next unit, you will be introduced to risk management and incident reporting.

## 7.0 References/Further Readings

Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., & Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. Computers & Security, 128, 103139. https://www.sciencedirect.com/science/article/pii/S0167404823000494

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, 132, 103309. https://www.sciencedirect.com/science/article/pii/S0167404823002195

# UNIT 4: PRACTICAL INTEGRATION OF RISK MANAGEMENT AND INCIDENT.

## Contents



## 1.0 Introduction

You will learn in this unit how to conceptualize risk management and incident reporting as a systematic approach to identifying assessing and mitigating potential cyber-security threats.

After studying this unit, you will be able to conceptualize incident response in cybersecurity as a structured approach to managing cybersecurity.

## 2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to; carry out risk management and incident reporting with a view to integrating the two.

## 3.0 Main Content

## 3.1 Incident Investigation, Report Writing and Presentation.

Risk Management in Cyber Security:

Risk management is a systematic approach to identifying, assessing, and mitigating potential cybersecurity threats. It involves:

- Risk Identification: Identifying potential threats and vulnerabilities in the organization's systems, data, and infrastructure.
- Risk Assessment: Evaluating the likelihood and potential impact of identified risks.
- Risk Prioritization: Prioritizing risks based on their likelihood and potential impact.
- Risk Mitigation: Implementing controls and measures to mitigate or reduce risks
- Risk Monitoring: Continuously monitoring and reviewing risk levels and controls.

## 3.2 Incident Response in Cyber Security:

Incident response is a structured approach to responding to and managing cybersecurity incidents. It involves:

- Incident Detection: Identifying potential security incidents.
- Incident Reporting: Reporting incidents to the appropriate teams and stakeholders.
- Incident Response Activation: Activating the incident response plan and team.
- Incident Containment: Containing the incident to prevent further damage.
- Incident Eradication: Removing the root cause of the incident.
- Incident Recovery: Restoring systems and data to a known good state.
- Incident Post-Incident Activities: Conducting post-incident reviews and activities to improve incident response.

## 3.3 Key Components of Incident Response:

- Incident Response Plan (IRP): A documented plan outlining incident response procedures.
- Incident Response Team (IRT): A team of trained individuals responsible for responding to incidents.
- Incident Response Procedures: Documented procedures for containing, eradicating, and recovering from incidents.

- Communication Plan: A plan for communicating with stakeholders during an incident.
- Training and Exercises: Regular training and exercises to ensure incident response readiness.

Effective risk management and incident response are critical components of a comprehensive cybersecurity program. By identifying and mitigating potential risks, organizations can reduce the likelihood and impact of security incidents. In the event of an incident, a well-planned and executed incident response can minimize damage and ensure quick recovery. (Mathew, 2024).

## 3.4 Practical Integration of Risk Management and Incident Reporting.

Practical integration of risk management and incident response in cybersecurity involves combining these two essential functions to enhance an organization's overall cybersecurity posture. Here's a detailed explanation:

Risk Management:

i. Identifies potential threats and vulnerabilities
ii. Assesses the likelihood and impact of potential incidents
iii. Prioritizes and mitigates risks

Incident Response:

i. Responds to and manages cybersecurity incidents
ii. Contains and eradicates threats
iii. Restores systems and data

Integration:

i. Risk management informs incident response by identifying high-risk areas and potential incident scenarios
ii. Incident response provides feedback to risk management on the effectiveness of controls and potential new risks
iii. Jointly, they:

✓ Develop incident response plans tailored to specific risks
✓ Conduct simulations and exercises to test plans and identify vulnerabilities
✓ Continuously monitor and review incident response effectiveness
✓ Update risk assessments based on incident response experiences

Benefits:

i. Enhanced preparedness for potential incidents
ii. Improved incident response effectiveness
iii. Reduced risk of security breaches
iv. Increased collaboration and information sharing between teams
v. More accurate risk assessments and incident response planning

Tools and Techniques:

i. Risk management frameworks (e.g., NIST Risk Management Framework)
ii. Incident response frameworks (e.g., NIST 800-61)
iii. Threat intelligence platforms
iv. Vulnerability management tools
v. Incident response platforms
vi. Simulation and exercise tools (e.g., tabletop exercises, simulation software)

By integrating risk management and incident response, organizations can proactively identify and mitigate potential threats, enhance their incident response capabilities, and reduce the risk of cybersecurity breaches.

## 4.0 Self-Assessment Exercise(s)

1. What are the basic components of incident response in cybersecurity?

**Answer**

i. Incident Detection: Identifying potential security incidents.
ii. Incident Reporting: Reporting incidents to the appropriate teams and stakeholders.
iii. Incident Response Activation: Activating the incident response plan and team. iv. Incident Containment: containing the incident to prevent further damage.
v. Incident Recovering: Restoring systems and data to a known good state.

2. What is the major goal of integrating risk management and incident response?

**Answer**

The goal is to proactively identify and mitigate potential threats, enhance their incident response capabilities and reduce the risk of cybersecurity breaches.

## 5.0 Conclusion

You have learnt from this unit about risk management and incident reporting as a systematic approach to identifying, assessing and mitigating potential cybersecurity threat. Moreover, you were able to conceptualize incident response as a structured approach to managing cyber security.

## 6.0 Summary

At the end of this unit you have learnt how to carryout risk management and incident reporting with a view to integrating the two.

## 7.0 References/Further Readings

Mathew, A. J. (2024). Unscripted Practices for Uncertain Events: Organizational Problems in Cybersecurity Incident Management. Science, Technology, & Human Values, 01622439241240411. https://doi.