PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

2026

Data Security and Compliance (FT-ACCA5034)

School of Applied Computing

IBRAHIM YAHIA MOHAMED
School of Applied Computing
1/6/2026

Assignment Title: Data Security and Compliance
Module Code: ACCA5034

Contents

Task 1: Researching in Data Security and Compliance **5**

1.0. Introduction **5**

1.1. Overview 5

1.2. Understanding Principles of Data Security 5

1.3. Common Threats and Vulnerabilities 1

1.4. Frameworks and Security Standards ..... **Error! Bookmark not defined.**

2.0 Data Compliance Regulations and Understanding of their rules **1**

2.1. GDPR has seven key principles. 1

2.3. The aims of research 1

2.4. Legal Requirements of Compliance Framework 1

2.5. Legal and Ethical Compliance 0

3.0. Case Scenario Analysis: Meta Cambridge Analytica Scandal **0**

3.1 Background 0

3.2. Cause of the Breach 1

3.3. Consequences and Compliance Failures 1

3.4. Lessons Learned 1

4.0 Risk Management **1**

4.1. Responsibilities in Data Security: 1

4.2. Data ownership consent: 1

4.3. Ethical Use of Personal Sensitive Data: 1

4.4. Enforcement Actions: 2

5.0. Emerging Trends in Data Security and Compliance **2**

5.1. Zero Trust Security Model challenges: 2

5.2. Cloud Security: 2

5.3. Data Encryption: 2

5.4. Artificial Intelligence: 2

5.5. Threats Detection: 2

6. What is the Active Directory Systems? **1**

6.0. Importance of Active Directory Enumeration Role in Management and Security Auditing 1

6.1. Inventory management: 1

6.2. Security Auditing: 1

6.3. Compliance: 1
6.4. Need for Authorised Administrators. 1
6.5. Standards and Regulations ..... **Error! Bookmark not defined.**
6.6. Tools for Active Directory Enumeration and Analysis 1
Task 2- Case Scenario: Zero Trust Aligned Security Programme for Resilient Intellect Ltd..... 4
1. 4
1. Overview of Resilient Intellect Ltd 4
1.2. Overview Diagram..... 4
1.3. EU expansion and regulatory landscape..... 0
1.4. Objectives of the security programme 0
2.0 Strategic Design of the Information Security Unit..... 1
2.1. The Zero Trust Principles..... 0
2.2. Strategic, forward looking architecture 0
3.0 Organisational Structure..... 1
3.1. Policies and Procedures 1
3.2. Secure Deployment and SaaS Configuration Standards Purpose 1
3.3. BYOD Stand for Bring Your Own Device Policy for Hybrid Workforce Security..... 1
4. Compliance Framework 1
4.0. DORA operational resilience requirements 1
4.1. Governance and Strategy..... 1
4.2 Security strategy and business goals 0
4.3 Governance and measurement 0
5.0. Risk Management 0
5.1. Four types of risk management techniques as you can see below. 1
5.2. Three Primary Aspects of Risk Management..... 0
5.3. Software supply chain threats for example poisoned AI models 0
5.4. Case studies of real-world threats example. 0
5.6. Key supply chain security gaps in open-source AI models..... 0
5.4. Cloud Misconfigurations Mitigation Strategies 0
5.4.1 Mitigation Strategies..... 1
5.4.2 Challenges in Detecting AI threats is difficult 1
5.7. Discussion..... 1
5.8. Recommendations 1
5.8.1 full maintenance program includes: 1
5.8.2 The external factors:..... 1
5.8.3 The internal factors: 1

5.9. Protection Mechanisms Recommended Security 1
6.0. Controls Cloud Security Posture Management 1
6.1. Security Information and Event Management (SIEM) 1
6.2 MFA Stand for Phishing Resistant Multi Factor Authentication 1
Conclusion 1
Future Considerations 1
References IEEE Style 0
References 0

Task 1: Researching in Data Security and Compliance

1.0. Introduction

The data security is about protecting digital information, while compliance ensures organisations handle it responsibly and legally. Together, they are building trust, reduce risks, and prevent costly legal or financial consequences [1].

1.1. Overview

What is data security? Data security is the protection of information that is maintained in database against unauthorized access, modification or destruction. As we know data is a valuable asset and protecting it from internal or external sources helps an organization to avoid financial loss, reputational harm, consumer trust degradation and brand erosion. Using encryption method, one can achieve data security. Data integrity, it is the mechanism that is applied to ensure that data in the database is correct and consistent. Data integrity is important as it guarantees the search ability and traceability of data. Data performance and stability also increase when one ensures effective data accuracy and data protection. [2]

1.2. Understanding Principles of Data Security

The definition and Core principles of data security revolve around the CIA Triad, and stand for Confidentiality, Integrity, and Availability these core principles are the basic foundation of cybersecurity. Involves encryption, authentication, authorisation and auditing. [3]

Figure 1 CIA Triad, and stand for Confidentiality, Integrity, and Availability

The figure shown as Confidentiality keeps information private by using access controls, encryption, and data masking.

Integrity ensures data remains accurate and unchanged through hashing, digital signatures, and audits.

The availability is meaning that data and systems are always accessible with backups, redundancy, and failover systems.

1.3. Common Threats and Vulnerabilities

Organisations face threats such as malware, phishing, DDoS attacks, ransomware, and insider misuse. Vulnerabilities arise from misconfigurations, outdated software, weak passwords, and lack of encryption.

2.0 Data Compliance Regulations and Understanding of their rules

The General Data Protection Regulation. It is an European Union law that took effect on May 25, 2018. GDPR controls how we can use, process, and store user data. It regulates how the personal data of individuals is processed and transferred. It applies to all organizations in Europe and those providing goods and services to Europe. The General Data Protection Regulation (2016) governs data privacy across the EU, enforcing principles like consent, transparency, and the right to be forgotten. [4] [5]

2.1. GDPR has seven key principles.

- First, Lawfulness, transparency, and fairness.
- Second, only using data for specific lawful purpose that it was obtained.
- Third, only acquire data that we strictly need.
- Fourth, ensure any data we possess is accurate.
- Fifth, storage limitations.
- Sixth, Confidentiality of data integrity
- Seventh, accountability. Society is now more data-driven. Therefore, there are rise in cyberattacks and data breaches.

Hence, the need of the GDPR to make organisation accountable for the safety and security of data they have acquired. GDPR has become so important. HIPAA and for, the Health Insurance Portability and Accountability Act in the United States, requiring covered entities to implement administrative, physical, and technical safeguards.

PCI DSS sand for the Payment Card Industry Data Security Standard form the backbone of modern compliance strategies and secures payment card data through encryption, firewalls, and access control measures. [6]

2.3. The aims of research

It analyses a real-world case study, the Equifax data breach, to identify key lessons learned.

ISO/IEC 27001 stands for the International Organization for Standardization and the International Electrotechnical Commission standard 27001. This standard provides a framework for compliance and continuous monitoring by outlining best practices for implementing and maintaining an Information Security Management System (ISMS). In addition, the National Institute of Standards and Technology (NIST) offers a framework for identifying, managing, and mitigating information security risks.

2.4. Legal Requirements of Compliance Framework

The compliance Frameworks and legal regulations set the rules for how organisations should protect data and stay accountable within their businesses. They create consistent security standards across industries, help keep personal and sensitive information safe, and protect businesses from fines and reputational damage and establish standards for securing sensitive, information across different industries and regions. [7] [5]

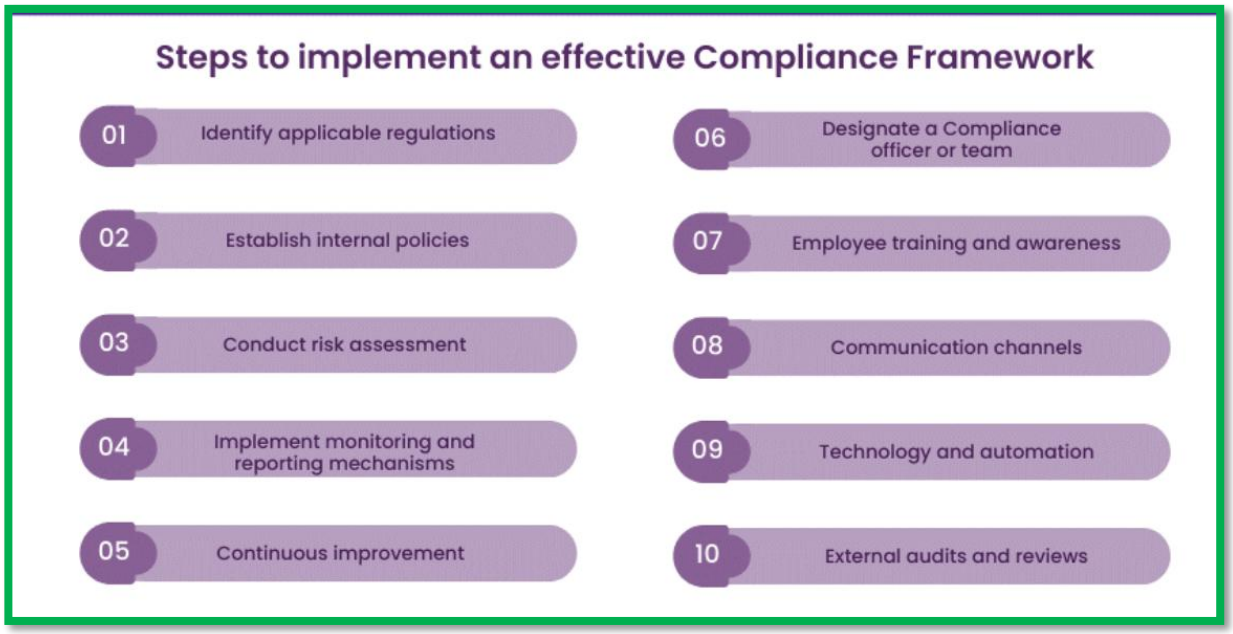
Figure 2 Global data regulation frameworks

Below figure show the global regulations data protection framework with more details and establishing standard for securing and key principles.

Regulation	Region	Focus	Key Principles
GDPR	European Union	Protects personal data and privacy of EU citizens.	Lawfulness, fairness, transparency. Data minimization and purpose limitation. Rights to access, rectify, erase, and port data.
HIPAA	United States	Safeguards medical information	Privacy rule, security rule and breach notification rule.
PCI DSS	Global industry	Secures credit/ debit card transactions	Build and maintain secure networks Protect cardholder data Monitor and test networks Maintain an information security policy.
ISO/IEC 27001	International	Information Security management Systems	Risk assessment and treatment. Security continuous improvement cycle.
NIST CSF	United States	Cybersecurity frameworks and standards	Identify, Protect, Detect, Respond, Recover.
NIST SP 800-53	United States	Frameworks	Federal agencies and organisations seeking best practices.

Figure 3 Implement an effective compliance framework

Below figure shows steps by step guidance to implement an effective compliance framework [8]



2.5. Legal and Ethical Compliance

The importance of Legal and Ethical Compliance they are reduces financial and reputational risks. Builds customer trust and ensures legal protection against potential violations or misuse of AI systems. Also, ensuring the organisation operates responsibly and transparently. [9]

- Legal Protection is avoiding fines and legal penalties.
- Reputation Management is demonstrating responsibility to customers.
- Business Continuity is ensuring resilience against cyber threats.
- Global Trade Enablement is compliance with international standards builds trust in cross border operations.

3.0. Case Scenario Analysis: Meta Cambridge Analytica Scandal

3.1 Background

Meta paid $725 million to settle the Cambridge Analytica scandal. Millions of users' data were misused without consent. This situation raised important privacy and accountability concerns. [10]

3.2. Cause of the Breach

Cause**:** Meta Improper sharing of user data through third-party apps.

3.3. Consequences and Compliance Failures

Impact: Data from millions users exploited for political purposes.

3.4. Lessons Learned

Lesson: Highlighted compliance gaps in data governance and privacy oversight.

4.0 Risk Management

The organisations must adopt a risk management framework to identify, assess and mitigate threats. This includes:

- Determining potential vulnerabilities that mean risk identification.
- Measuring the likelihood and impact of risks assessment.
- Applying security controls for example firewalls, encryption, MFA, all that mean risk mitigation.
- Continuously evaluating risk in a changing threat landscape, monitoring and review.

4.1. Responsibilities in Data Security:

These organisations are typically at a higher level in responsible for keeping data safe from unauthorized access and being transparent about how it's used.

Two other key roles are the data controller and the data processor. The data controller manages how the data will be used, while the data processor actually handles that data.

The data controller can often give instructions to the data processor on how to use the data. For instance, when is come to the payroll department might serve as the data controller, while a payroll company acts as the data processor.

As the data processor, the payroll company will access user information and bank details to process payroll weekly. The payroll department must ensure everyone gets paid and directs the payroll company on how to handle the payroll process.

4.2. Ownership consent:

The data owner is responsible for data quality, fully access permissions, and use policies. The personal data ownership or individual is key to consent management because it defines who controls personal information. Clear individual ensures valid consent, legal compliance, transparency, and trust while preventing data misuse of especially in AI and technology.

4.3. The Ethical Use of Personal Sensitive Data:

Using sharing of sensitive data means protecting privacy data, manages how the data will be used, while the data processor actually handles that data and research. It requires informed consent, transparency,

anonymisation, and strong security. The personal data should only be shared when necessary and used fairly to benefit everyone without causing harm or discrimination.

4.4. Enforcement Actions:

The enforcement actions are first steps that government agencies take to make sure laws and regulations are followed. Enforcement actions are steps regulators take like warnings, fines, or shutdowns to ensure laws are followed, prevent violations, and maintain fairness and public trust.

5.0. Emerging Trends in Data Security and Compliance

5.1. Zero Trust Security Model challenges:

The Zero Trust Model Challenges is verifying every access request for better protection.

5.2. Cloud Security:

The cloud security is focusing on protecting data stored online

5.3. Data Encryption:

The data encryption is keeping data unreadable to unauthorised users.

5.4. Artificial Intelligence:

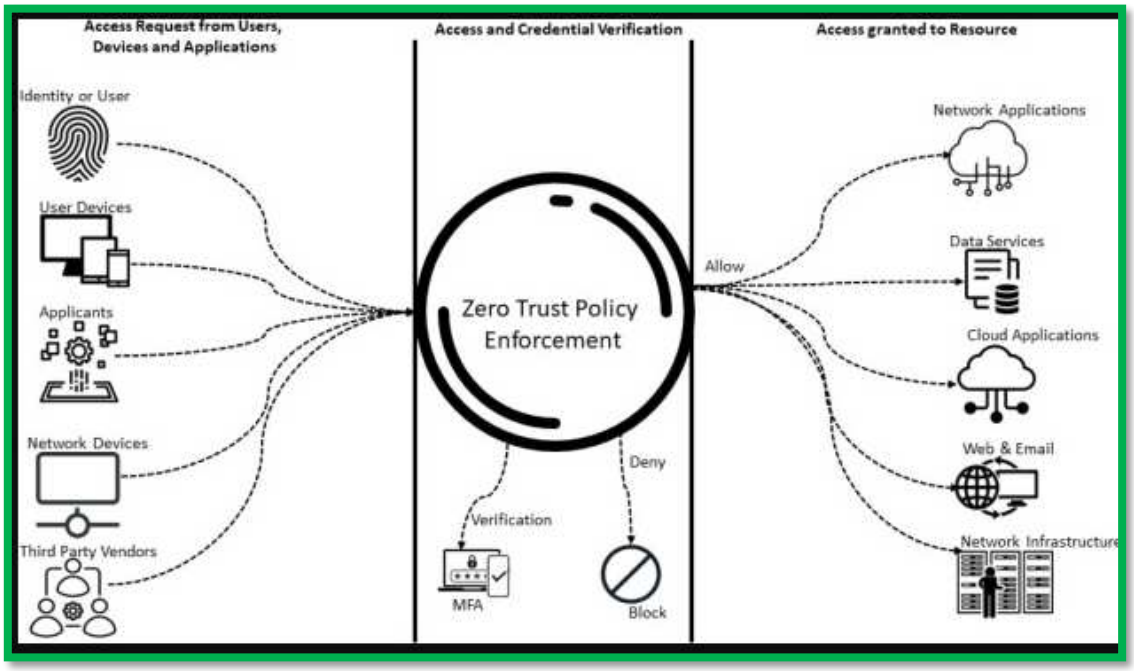
Artificial Intelligence (AI) is helping detect and stop cyber threats.

5.5. Threats Detection:

Threat Detection users real time monitoring to identify attacks early. [11]

Figure 4 Zero Trust Policy Enforcement

As while the figure below screenshot showing the importance of Zero Trust Policy Enforcement.



6. What is the Active Directory Systems?

Active Directory is a system in windows Server used to manage users, computers, and services. Also is central to managing users, computers, and services in Windows Server environments. As the systems is growing more complex, regularly reviewing AD's contents is crucial for maintaining security, efficiency, and compliance. [12]

6.0. Importance of Active Directory Enumeration Role in Management and Security Auditing.

As organisations depending on it for identity and security, for protecting the network. And the is part of the Microsoft Windows Server environment and offers a centralized system for managing users, computers, and services. The As organisations depend on AD for identity management, security checks, and access control, understanding its contents becomes very important. [13]

Gathering detailed information about AD objects, such as users, groups, computers, and permissions. The collecting comprehensive data of Active Directory's objects, is including users, groups, computers, and their permissions, is known as enumeration for a number of reasons:

6.1. Inventory management:

It helps admins to keep tabs on all the stuff on the network, which makes their day-to-day jobs easier.

6.2. The Security Auditing:

Regular updating and enumeration allows for the identification of misconfigurations, such as excessive permissions or outdated accounts, which can lead to security breaches.

6.3. The Compliance:

The regulations, such as ISO 27001, GDPR, and HIPAA, mandate the implementation of access controls and regular security audits. Enumeration supports compliance efforts by ensuring that proper access controls are enforced and monitored.

6.4. Need for Authorised Administrators.

The need of authorised network security administrators must have the capability to enumerate Active Directory to effectively manage and secure the environment and enumeration can help to identify: [14]

- Privileges Mismanagement its meant detecting users with

unnecessary elevated privileges.

- Inactive Accounts: Identifying accounts that have not been used for an extended period, which may pose a security risk.
- Group Memberships: Understanding group memberships helps in identifying potential lateral movement opportunities within the network.

Active Directory admin, managing multiple domains, plus offers everything you need to streamline your daily tasks. Below is the screenshot as evidenced.

Figure 5 All in one Active Directory management tool

Figure show an active Directory admin, managing multiple domains, offers everything need to streamline daily tasks.

Figure 6 Seamless integration for unified

Figure 6 show AD management, below is the screenshot as evidenced

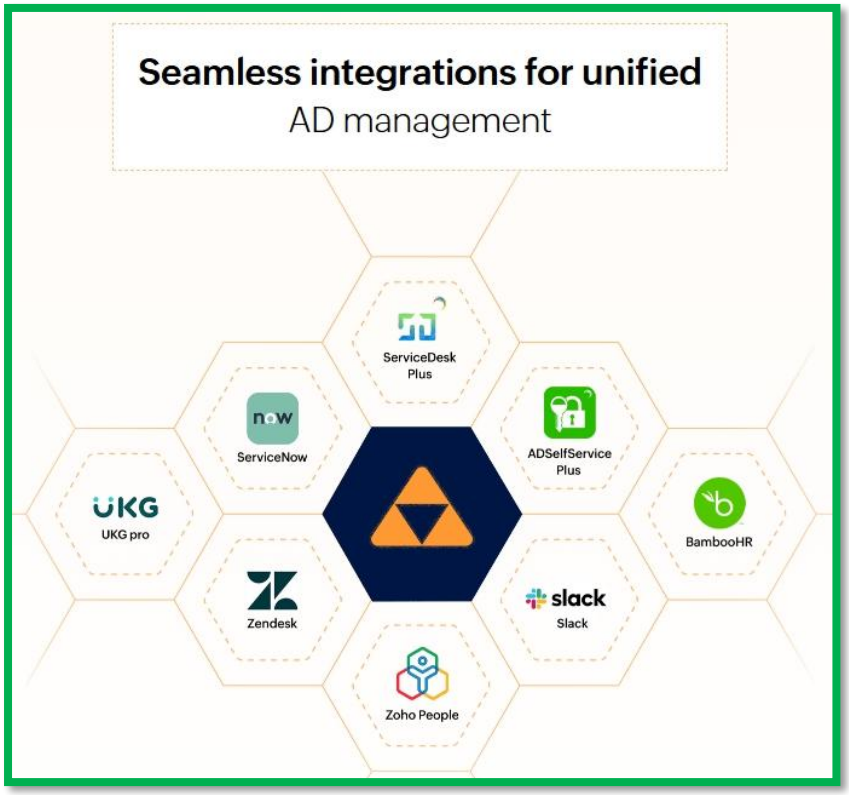


Figure 7 default protected accounts and groups

The following figure 7 is the table list the default protected accounts and groups in Active Directory. [15]

Windows 2000 <SP4	Windows 2000 SP4 -Windows Server 2003	Windows Server 2003 SP1+	Windows Server 2008 -Windows Server 2012
Administrators	Account Operators	Account Operators	Account Operators
	Administrator	Administrator	Administrator
	Administrators	Administrators	Administrators
Domain Admins	Backup Operators	Backup Operators	Backup Operators
	Cert Publishers		
	Domain Admins	Domain Admins	Domain Admins
Enterprise Admins	Domain Controllers	Domain Controllers	Domain Controllers
	Enterprise Admins	Enterprise Admins	Enterprise Admins
	Krbtgt	Krbtgt	Krbtgt
	Print Operators	Print Operators	Print Operators
			Read-only Domain Controllers
	Replicator	Replicator	Replicator
Schema Admins	Schema Admins		Schema Admins

6.6. Tools for Active Directory Enumeration and Analysis

A commonly used for Active Directory enumeration is Nmap.

How Nmap works?
The Network Mapper, is an open-source tool for network discovery and security checking. It runs different types of scans to find active devices, open ports, and the services on those ports.

6.7. Services and Protocols

Nmap uses several protocols, mainly TCP/IP, to connect and collect information about the network. This helps administrators map devices, spot vulnerabilities, and study network behaviour. Below is to be installing. [16] [17]

Figure 8 License terms before installing Nmap

Before installing Nmap agreement after review the license Agreement then click the Agree.

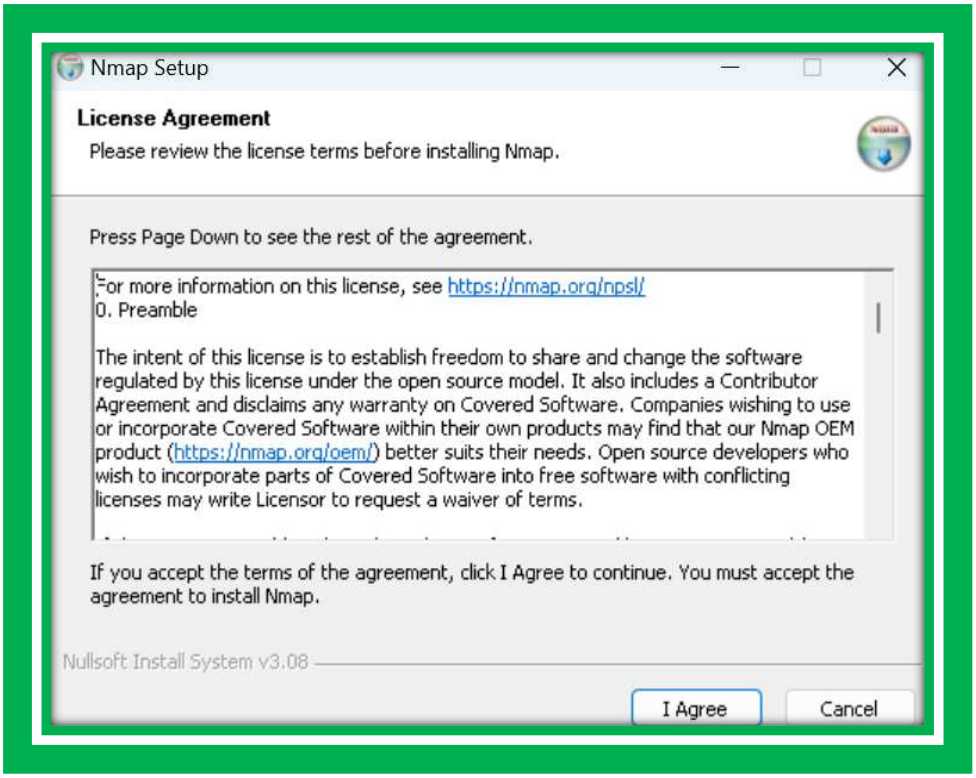


Figure 9 Choose components which features

Choose Components which features of Nmap that need to install.

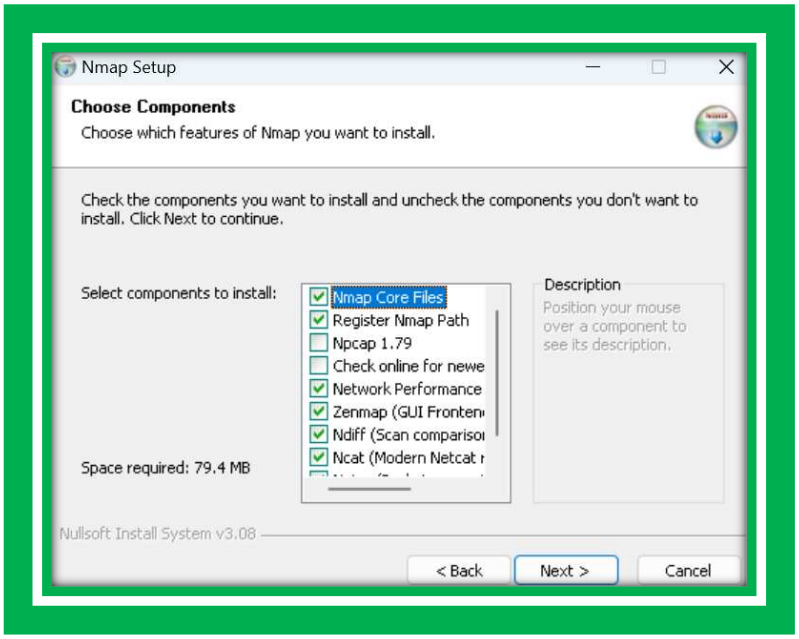


Figure 10 features of Nmap

These figure show selects components to install and then click next to continue.

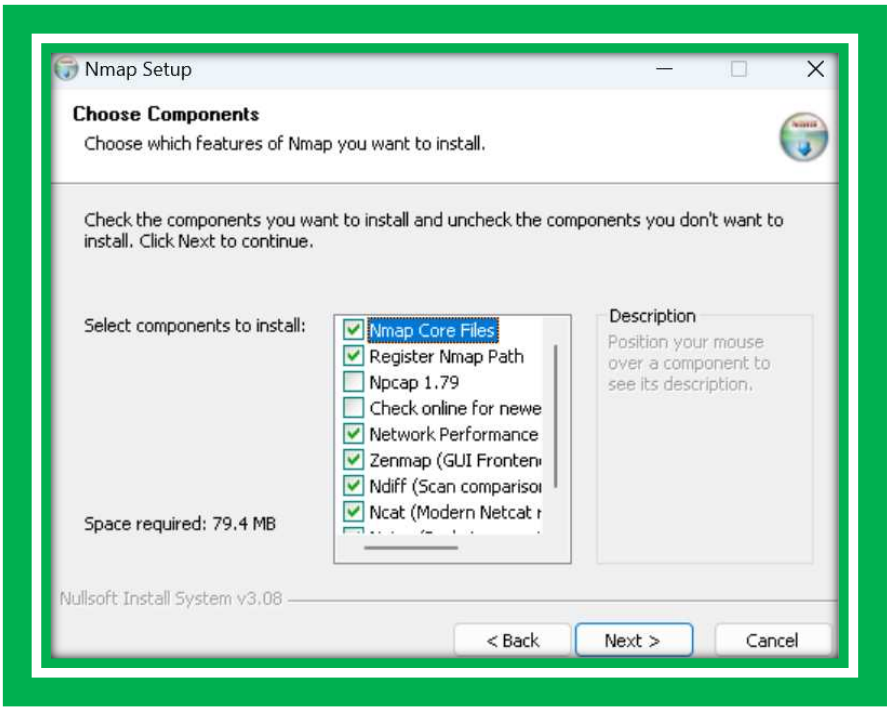


Figure 11 Zenmap scan tools

Figure 11 Zen map scan tools show where can put target to scan and the output host details.

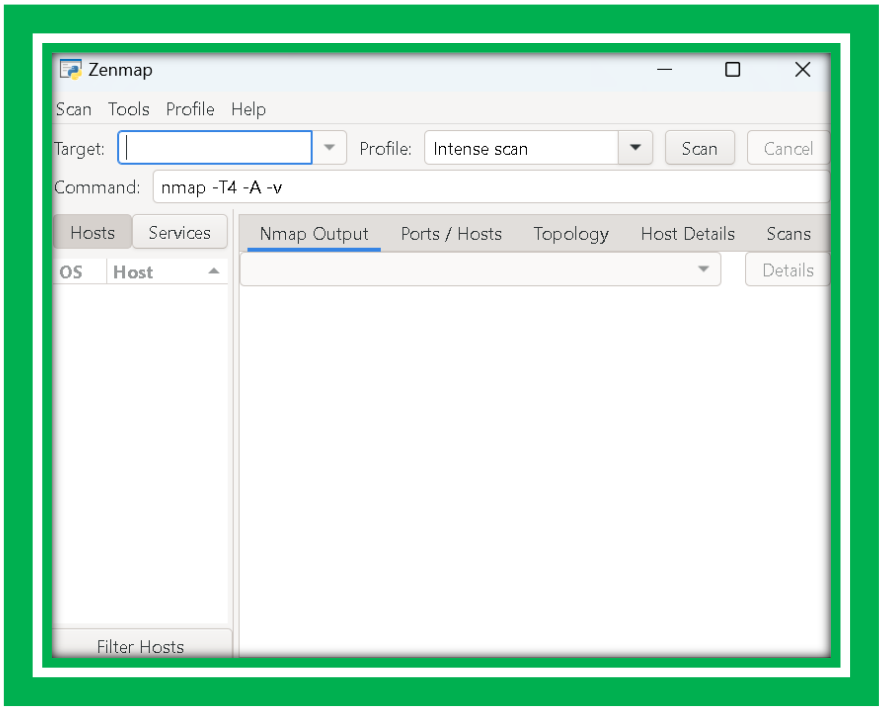
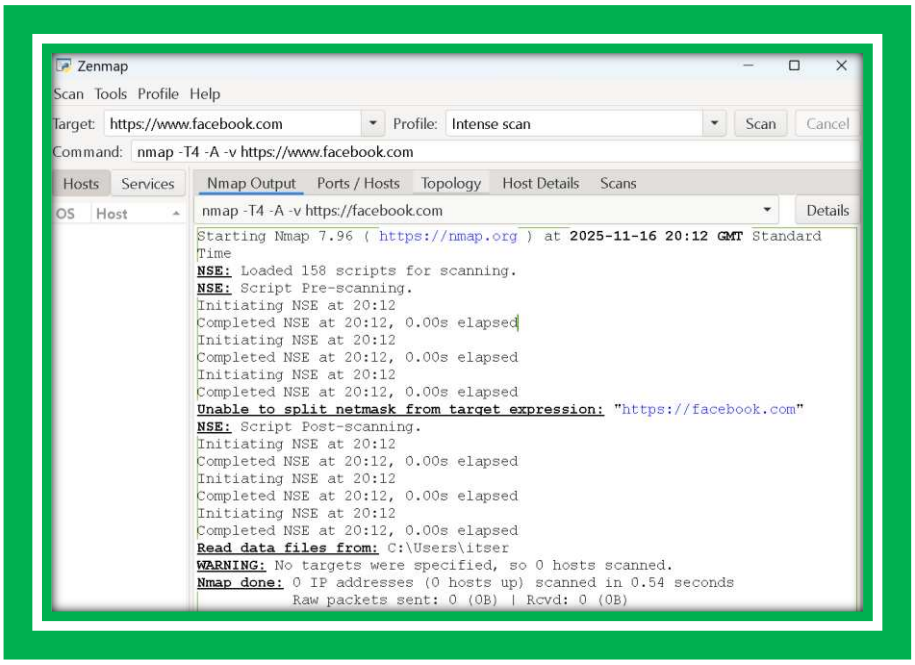


Figure 12 Zenmap output details

Output details the target was Facebook as below can be seen IP address and host name.



Task 2- The Case Scenario of Zero Trust Aligned Security Programme for Resilient Intellect Ltd

1.

1. Overview of Resilient Intellect Ltd

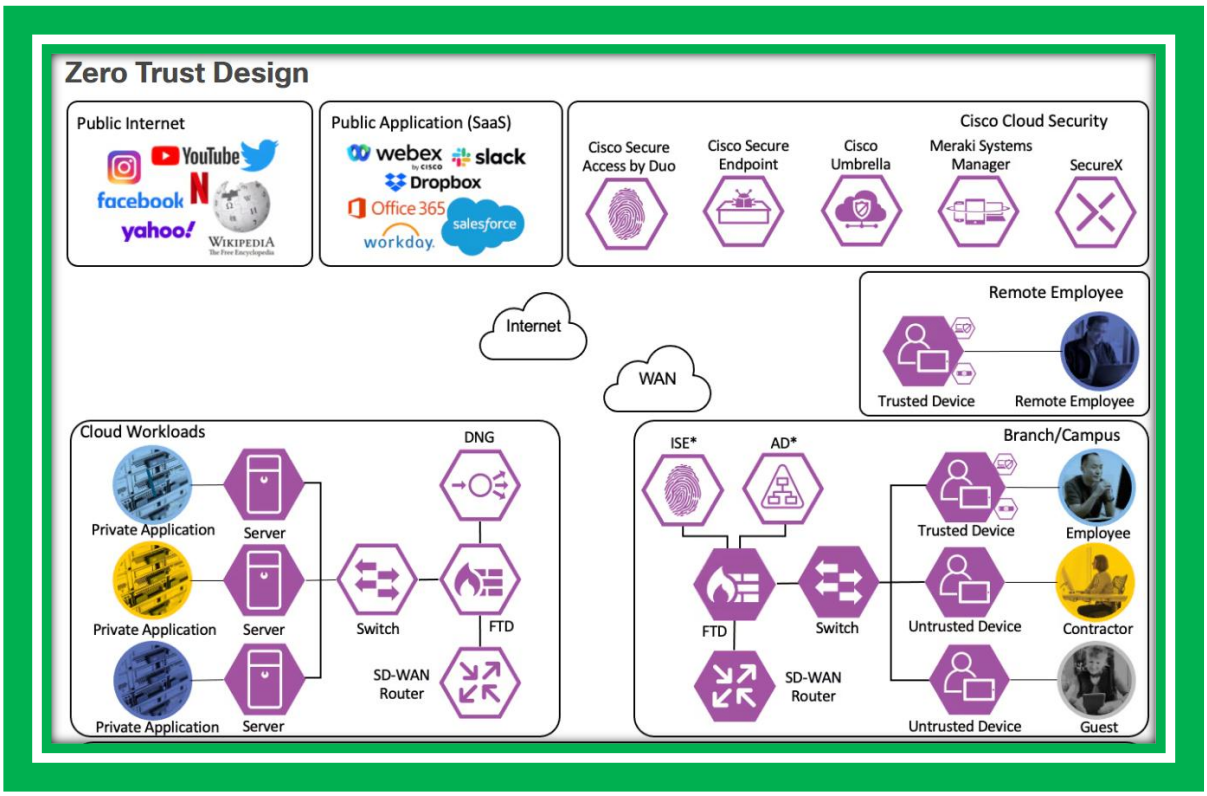
The Resilient Intellect Ltd is a rapidly expanding technology and data analytics company specializing in AI-powered business solutions. As the company enters the European Union market, it gains access to new growth opportunities while also facing increased responsibilities around cybersecurity, data privacy, and regulatory compliance. [18]

1.2. Overview Diagram

The combined overview diagram, is integrates the Zero Trust architecture and Information Security Unit (ISU) structure into one clear, executive level view showing how security and governance align.

Figure 13 Zero Trust Design

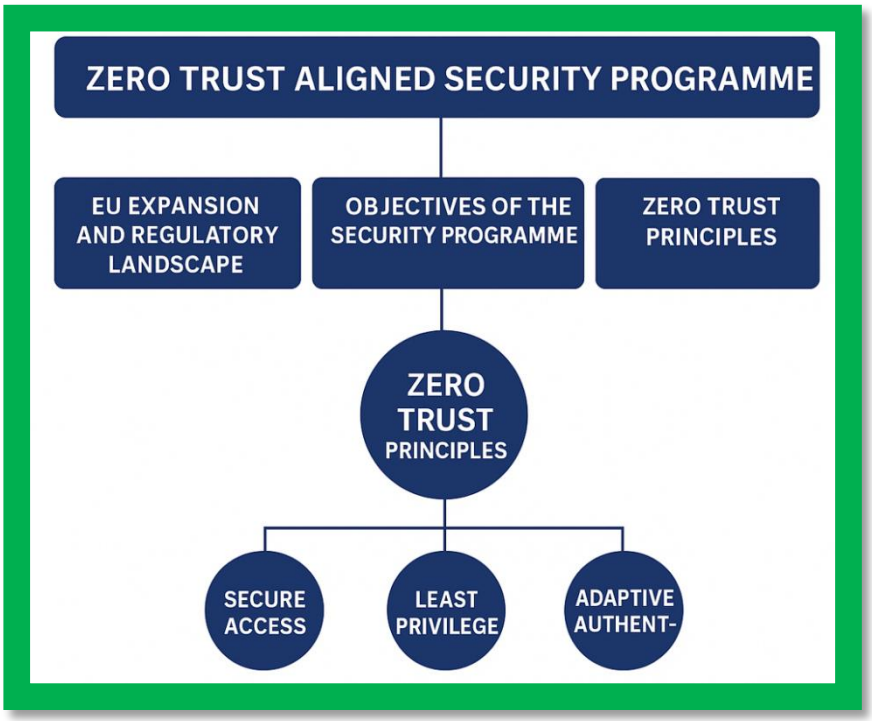
Below is the screenshot of figure Zero Trust Design for the evident. [19]



As seen above figure 13 design diagram show how users, devices, applications, and data connected through ongoing verification and policy enforcement, not a trusted internal network, public internet, Cisco Cloud Security, cloud workloads and remote employee.

Figure 14 Zero Trust Aligned Security Programme

These below figures discover how a data first approach to security. Zero Trust architecture is the essential guide to Zero Trust and learn how implement Zero Trust security with expert guidance



.

1.3. EU expansion and regulatory landscape

Operating in the European Union means following strict data protection rules like the GDPR and local cybersecurity laws. The company must handle data responsibly covering transfers, consent, and breach reporting to stay compliant, maintain trust, and avoid penalties.

1.4. Objectives of the security programme

The objectives of the Security Programme within the Zero Trust Aligned Security Programme is designed to:

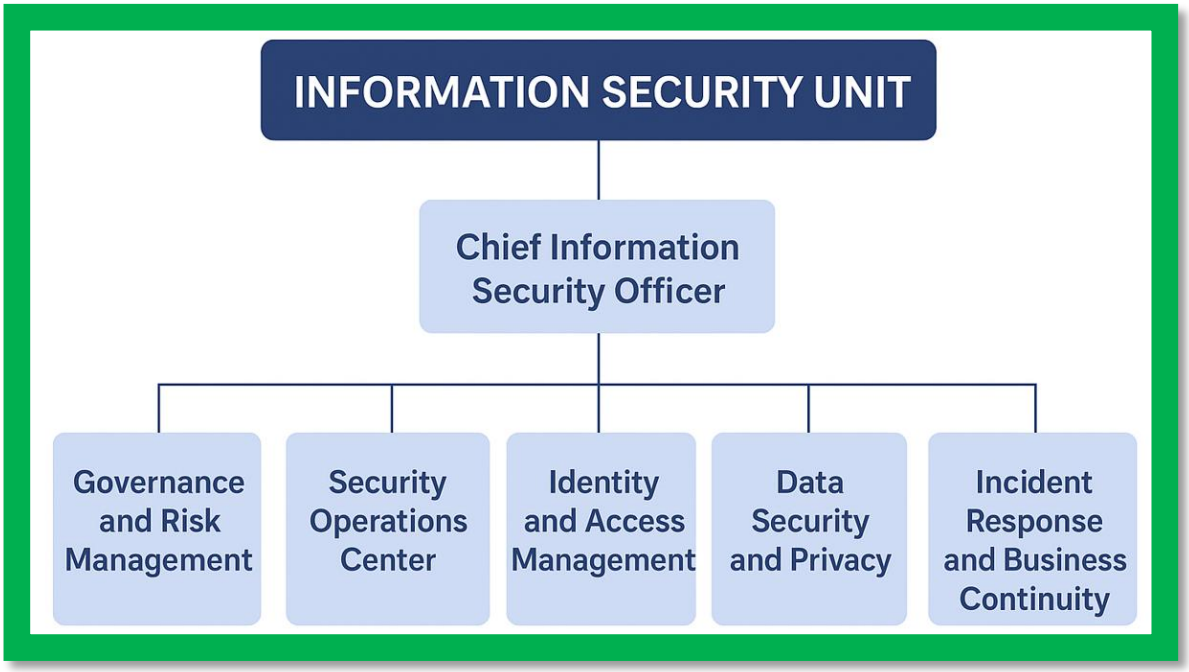
- Boost cybersecurity and minimize breach risks.
- Ensure compliance with EU data protection rules.
- Safeguard sensitive company and customer data.
- Encourage proactive, continuous security monitoring.
- Enable secure, sustainable growth in the EU.

2.0 The Strategic Design of the Information Security Unit

The Information Security Unit (ISU) will focus on Governance, Risk, Compliance, Security Operations, and Incident Response. Led by the Chief Information Security Officer (CISO), it will develop policies, train staff, manage third-party risks, and implement Zero Trust principles with continuous monitoring, reporting directly to executive leadership for accountability.

Below is the screenshot Figure 16 Information Security Unit for the evident.

Figure 15 Information Security Unit



The above figure ISU which is supports Resilient Intellect Ltd.'s and Zero Trust programme by overseeing governance, risk, compliance, and security operations. Led by the CISO, which is enforces security policies, manages risk, and ensures ongoings' monitoring through a coordinated team of security roles aligned with business and regulatory needs.

2.1. The Zero Trust Principles

The security program will use a Zero Trust architecture based on these main principles:

- Make sure each user and device must be authenticated and authorised before accessing the system.
- Given limit user permissions only to what is necessary for their job.
- Secure zones to contain possible breaches.
- Ongoing check user behaviour, device health, and network activity for unusual activity.
- Centralize identity control and use multi-factor authentication (MFA).
- When it is moving to prevent unauthorised disclosure and protect data both when it is stored.

Figure 16 Zero Trust Architecture

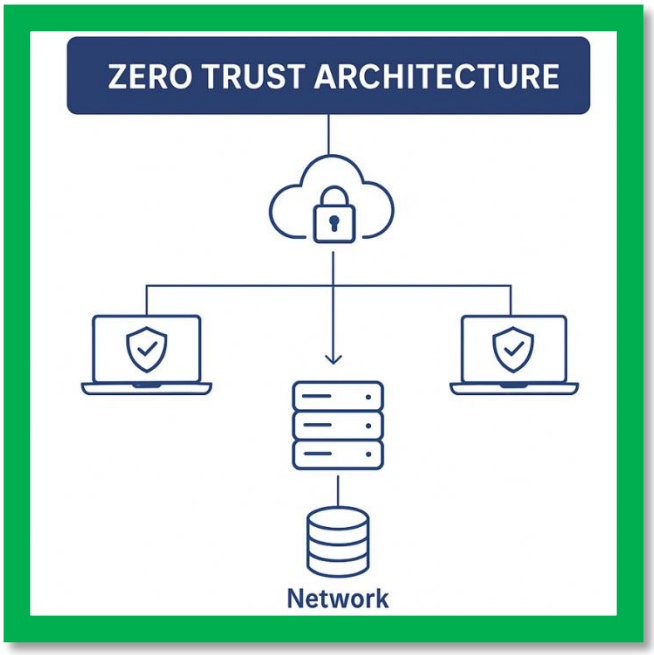
2.2. Strategic, forward looking architecture

Resilient Intellect Ltd is Security Architecture built on Zero Trust principles, the architecture will be adaptive, intelligent, and in line with ISO/IEC 27001 and NIST standards.

Key Features [20]**.** [21]**.** [18]

- Cloud is the based tools for scalable, reliable protection.
- Machine learning to detect threats and predict risks.
- Integrated cloud networking and security for secure access anywhere.
- Stronger user verification and session control.
- Regions under GDPR and data kept within approved EU.
- Tracking and reporting automated, real-time compliance.

Below figure shows the Zero Trust Architecture's screenshot diagram for the evident.



As seen figure 17 above shows that the Zero Trust Exchange uses identity based controls to securely broker segmented access between users, workloads, third parties, and locations without granting broad network access. This outlines key zero trust principles verify every user and device, apply least privilege access, segment networks to limit breaches, ongoing monitoring's activity, enforce MFA with centralized identity management, and protect data at rest and in transit.

3.0 Organisational Structure

Proposed structure with cloud security architect and development, security and operations, Lead. Role definitions and integration into the security programme, the key roles include:

- Chief Information Security Officer
- Governance, Risk and compliance lead.
- Cloud Security Architect.
- Development, Security and Operations Lead
- Security operations Centre Analysis

3.1. The Policies and Procedures AI Ethics and Usage Policy

Purpose:

The purpose is to ensure that all artificial intelligence systems are used in a responsible, secure, and

ethically sound manner, and that they meet regulatory requirements.

The Key Guidelines and Structure:

- Using methods like hash checks and documentation of their source and all AI models must be verified for integrity.
- Unapproved or unverified open-source are not allowed in production environments.
- Each model's history, updates, and versions and maintain detailed documentation that tracks.
- Identify bias, fairness issues, and potential security vulnerabilities and conduct regular testing.
- Using encryption and protect training data The Enforcing role the based access controls and.

3.2. Secure Deployment and SaaS Configuration Standards Purpose

To ensure that Software-as-a-Service (SaaS) platforms are deployed and managed securely across the organisation. [22]. [20]

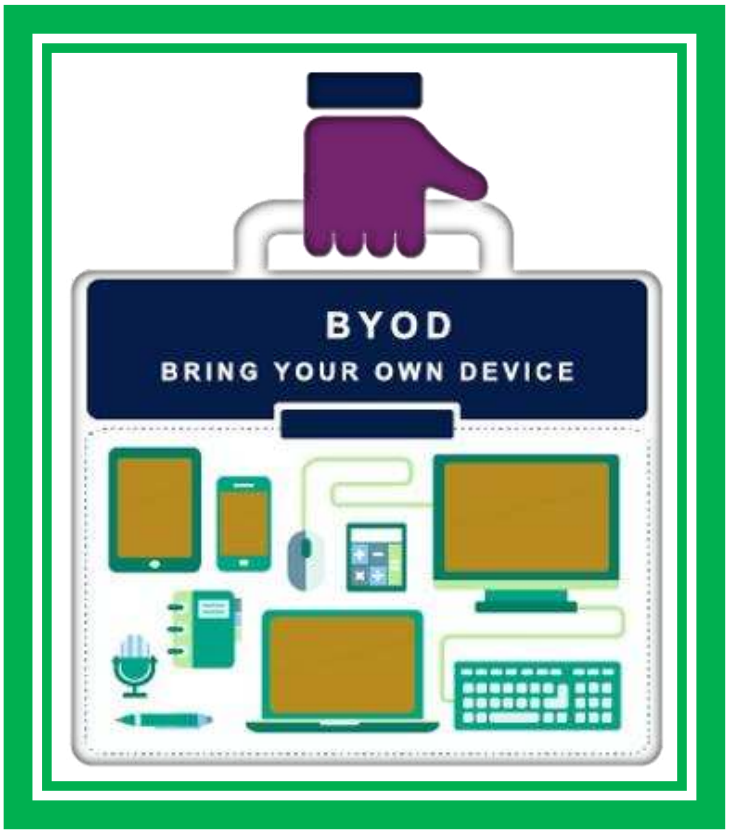
Key Guidelines:

- Configuration all SaaS services according to CIS Benchmarks and Zero Trust security principles.
- Apply the principle of least privilege to all user accounts and require multi-factor authentication (MFA), single sign-on (SSO) using identity federation.
- Security Information and Event Management (SIEM) system for continuous monitoring and centralize all SaaS activity logs in the organisations.
- Ensure compliance Using CASB stand for Cloud Access Security Brokers to detect and control unauthorized SaaS usage.
- Make sure every three months to confirm that security controls remain effective.

3.3. BYOD Stand for Bring Your Own Device Policy for Hybrid Workforce Security

Employees who use their own devices for work must ensure those devices meet company Mobile Device Management (MDM) requirements, including up-to-date patches, full encryption, and active endpoint protection. [23]

Figure 17 Bring Your Own Device Policy



All the organisation will implement Zero Trust network access instead of traditional VPNs to provide more secure, identity-based connections.

To protect privacy, corporate and personal data will be kept separate using secure container technology.

If a device is lost or stolen, IT will have the ability to perform a remote wipe to safeguard company information.

All users must enable phishing-resistant multi-factor authentication (MFA) to verify identity and prevent unauthorised access.

If they are, employees should make sure devices used for work conform to company-issued Mobile Device Management (MDM) policies: such as having the latest patch levels, full encryption and endpoint protection.

Zero Trust network for access will be the technology Zero Trust replaces traditional VPNs with more secure, identity-based connections.

Secure container technology will be utilized to keep corporate and personal data separated and ensure privacy.

IT will be able to do everything from a remote wipe in case of lost or stolen device.

4. Compliance Framework

4.0. DORA operational resilience requirements

Digital Operational Resilience Act (DORA) to ensures clear operational resilience that meets EU digital sovereignty expectations. [24]

Figure 18 Compliance Framework

Regulation	Key Requirement	Alignment Action
DOR	Operation Resilience	Ensure resilience through continuity plans, third-party risk management, and threat testing
DORA	Incident Reporting	Requires reporting breaches within one hour.
NIS2	Security and Reporting	Requires 24/7 response and breach reporting within 24-72 hours.
NIS2	Governance and Accountability	Assigns executive accountability and ongoing risk monitoring.

Figure 18 above shows a regulation compliance framework, and the keys alignment action. As a Compliance Framework is a structured system and guidelines to meet regulations that organisations and government use to ensure they meet the rules and regulations that apply to their industry to protect data, and manage risks. Common frameworks.

4.1. Governance and Strategy

Adoption of NIST Cybersecurity Framework (CSF). Core Functions: Identify, Protect, Detect, Respond and Recover. [25]

Figure 19 Governance and Strategy

Figure below shows the function, objective example initiatives in business alignment.

Function	Objective	Example Initiative	Business Alignment
Identify	Asset and risk visibility	Implement cloud security management and asset inventory	Supports compliance readiness and IT governance
Protect	Strengthen defences	Zero Trust Network Segmentation, EDR	Ensures uptime of critical digital services
Detect	Early detection	SOC with UEBA & AI-driven anomaly detection	Minimises operational disruption
Respond	Effective containment	IR playbooks for AI systems and cloud	Meets DORA/NIS2 response timeline
Recover	Business continuity	Immutable backups tested	Protects business reputation timelines

Figure 19 shows how governance, policies, and strategic planning provide leadership, direction, and accountability for implementing Zero Trust security. Policies convert these objectives into clear rules for access control, data protection, and risk management across the organisation.

4.2 Security strategy and business goals

The business goals are strong security strategy management should follow with a company's overall objectives. As we know the protecting data and systems isn't just a technical task it supports business continuity, protects reputation, ensures regulatory compliance, and enables growth. When security initiatives are tied to business goals, they can help the organisation operate safely while pursuing its mission.

4.3 Governance and measurement

The clear policies, defined are responsibilities, and regular audits ensure security measures are effective and aligned with business goals. Risk assessments, and reporting monitor compliance and performance that can ensure security measures are implemented, risk are managed and the organisation stays with its goals and regulations.

5.0. Risk Management

It identifies key threats and vulnerabilities, assesses their impact, and ranks actions to protect data, ensure safety, and keep the business running.

Here below are the figure 20 for high level risk assessment tables: [26] [27]

Figure 20 Risk Management

Figure 21 Risk Management above which explains how organisations identify, access, and mitigate risks to protect data and maintain business continuity.

Figure 21 Risk area and description

Risk Area	Description	Likelihood	Impact	Mitigation
Poisoned AI Models	Compromised or manipulated training datasets	Medium	High	Model provenance tracking, data validation pipelines
Vulnerable Dependencies (Software Supply Chain)	Open-source components with CVEs	High	High	SBOM (Software Bill of Materials), automated dependency scanning
Cloud Misconfigurations	Publicly exposed storage buckets or IAM roles	Medium	High	CSPM tools, automated remediation, continuous compliance scanning
Insider Threats	Privileged user abuse	Medium	High	UEBA, just-in-time access, privileged access monitoring

5.1. Four types of risk management techniques as you can see below.

These four techniques work together to help organisations make informed decisions about how to handle different risks based on cost, impact, and business requirements. *Figure 22 Type of risk management techniques*

5.2. Three Primary Aspects of Risk Management

- First one is Risk Identification is Finding possible threats and weaknesses in systems or data.
- Secondly is Risk Assessment is Examining how likely those risks are and their potential impact.
- Thirdly is Risk Mitigation is Using controls, policies, and tools to lower or remove risks.

Together, these steps enable proactive risk management, safeguard organisational assets, and support compliance with business and regulatory requirements.

5.3. Software supply chain threats for example poisoned AI models

The software supply chain threats are attacks where hackers compromise shared components to spread malicious code or poisoned models. [28] [29]

- Data poisoning is where attackers corrupt training datasets.
- Model tampering is where backdoored models are uploaded to trusted platforms.
- Invisible backdoors are which active only under specific triggers and evade traditional detection methods. [30]

5.4. Case studies of real-world threats example.

The Case studies show real-world threats AI and software risk, from poisoned models and prompt injection to supply chain compromises and dependency hijacking. [31]

Figure 23 show real-world threats AI and software risk, from poisoned models

Incident name	Year	Attack vector	Impact	Source
Malicious models on Hugging Face	2024	Malicious payloads in model cards and metadata	Compromised developer environments via Hugging Face	JFrog Security
Prompt injection attacks on LLMs	2023–24	Crafted user inputs override model behavior	Leaked prompts, API abuse, and misaligned outputs	arXiv
AML.CS0028: AI Model Tampering via Supply Chain Attack	2023	Supply chain compromise	AI models poisoned by exploiting vulnerabilities in cloud-based container registries, leading to backdoored models being distributed through trusted channels	MITRE ATLAS
PyTorch dependency hijack (torchtriton)	2022	Typosquatting and dependency confusion in PyPI	System fingerprinting and data exfiltration	PyTorch

Figure 23 above shows real-world AI and software security threats, emphasizing how poisoned or compromised models and training data pose serious risks to system reliability and security, differing only in level of detail and emphasis.

5.6. Key supply chain security gaps in open-source AI models.

The key issues include the security gap, impact and consequence. These weak provenance, missing model signing, and poor checksum enforcement let poisoned AI models spread undetected. [32] Below the figure for security gaps in open-source AI models.

Figure 24 . Key supply chain security gaps in open-source AI models

Security gap	Impact	Consequence
Lack of provenance and transparency	• Unknown training sources and contributors • No audit trail for model origins	• Trust is assumed rather than verified • Attackers can easily insert poisoned or backdoored models
No standardized model signing	• Models are rarely signed and checksums are rarely enforced • Signature does not always cover weights or dependencies	• Tampering during distribution or pull request merges often go unnoticed
Insecure dependency chains	• Widespread use of unvetted PyPI/NPM/conda packages • Prone to typosquatting and dependency confusion	• One rogue dependency (e.g., torchtriton) can breach the full pipeline
No trigger-behavior testing	• Testing focuses on accuracy rather than adversarial or edge-case behavior	• Backdoors remain hidden unless specifically triggered
Blind trust in pretrained models	• Pretrained models are widely reused with minimal inspection • Transfer learning can propagate hidden threats	• Inherited risks are magnified across ecosystems

following figure 24 shows how AI supply chains face serious security risks, hidden backdoors can evade testing and enable attacks, tampered model distribution can alter weights without detection, dependency attacks can introduce upstream compromises, and weak adversarial testing leaves safety vulnerabilities unaddressed.

5.4. Cloud Misconfigurations Mitigation Strategies

The cloud misconfiguration is one of the biggest causes of security breaches in Infrastructure as a Service (IaaS), Platform as a Service

(PaaS), and Software as a Service (SaaS) environment. Misconfigurations occur when cloud resources such as storage buckets, virtual machines, Identity and Access Management (IAM) roles, firewalls, or databases are deployed with insecure or incorrect settings. Below is the comprehensive mitigation strategies to prevent cloud misconfigurations

.

Figure 25 these measures to help ensure a secure and resilient cloud environment.

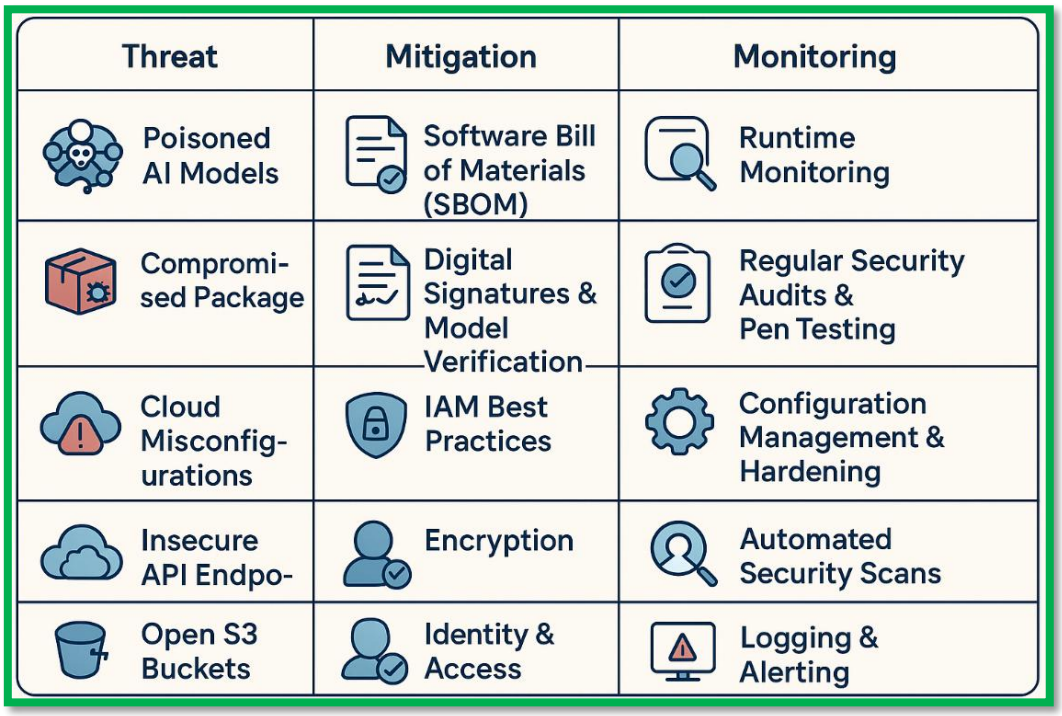


Figure above shown the Cloud Misconfigurations Mitigation Strategies face major security threats such as poisoned AI models, compromised packages, misconfigurations, insecure Application Programming Interface (APIs), and exposed storage buckets. These risks can be reduced by using Software Bills of Materials, digital signature verification, strong Identity and Access Management (IAM) practices, encryption, and strict access controls. With alerts essential like ongoing monitoring through audits, configuration management,

automated scans, and logging. These Cloud Misconfigurations Mitigation Strategies measures help to ensure a secure and maintaining resilient cloud environment.

5.4.1 Mitigation Strategies

The version of the mitigation strategies:

Use trusted sources, Scan models for anomalies, track provenance, monitor deployed systems, and apply strict DevSecOps checks.

5.4.2 Challenges in Detecting AI threats is difficult

Several challenges make these threats hard to spot for a few reasons, such as:

Opaque model structures, Unclear outputs, Missing provenance, no ground truth, Limited adversarial testing, knowledge and experience, and lack of expertise and best practices. [32]

5.5.Contingency Planning

Ransomware Scenario AI training data and source code. Recovery Objectives and procedures.

5.6. Disaster Recovery (DR) Plan:

5.6.1. Detection and Containment is the SOC isolates affected VMs and repositories. Block malicious IPs via EDR & firewall orchestration.

5.6.2. Communication, Notify EU regulators per DORA/NIS2 timelines (24–72 hours). Activate crisis communication team.

5.6.3. Recovery, restore from immutable, offline backups (stored in separate cloud region). Validate integrity using cryptographic checksums.

5.6.4. Post-Incident Review, Root cause analysis, playbook refinement, and cyber insurance claim initiation. Conduct red-team validation before resuming operations.

5.7. Discussion

The need for ongoing maintenance of the information security program is not static. Threats evolve, systems change, new vulnerabilities emerge, and staff affects security awareness. Ongoing maintenance ensures that polices, controls, and defences stay effective over time.

5.8. Recommendations

The list of recommendations security management models, is the security management models provide structured guidance for organising and maintaining an information security program, including: [33]

- Security Management Model (SMM) outlines how

organisations should maintain their information ongoing security maintenance model.

- ISO/IEC 27000 series international standards for creating and managing an information security management system.
- NIST SP 800 is United State guidelines that provide detailed information for cybersecurity and risk management.
- COBIT is IT governance framework manging to ensure security and alignment with business goals.

5.8.1 full maintenance program includes:

The continuous maintenance and monitoring, regular assessments, policy reviews, incident response updates, remediation planning. This goal is keeping the security posture aligned with business needs and emerging risks. The key factors involved in the external and external environment:

5.8.2 The external factors:

Attack trends, new vulnerabilities, regulatory changes and vendor advisories.

5.8.3 The internal factors:

System configurations, access logs, users' behaviour, and policy compliance, controls, detect functionality and example technology.

Figure 26 Internal System configurations

following figure show interna compliance, with example controls System configuration technology's related controls and

Control	Function	Example Technology
CSPM (Cloud Security Posture Management)	Detect and remediate cloud misconfigurations	Wiz, Prism a Cloud, Orca Security
SIEM with UEBA	Correlate and analyse logs with AI-driven behaviour analytics	Microsoft Sentinel, Splunk, IBM Radar
EDR/XDR with Automated Response	Endpoint threat detection and isolation	Crowd Strike Falcon, Sentinel One, Microsoft Defender XDR
Phishing-Resistant MFA	Prevent credential theft	FIDO2/U2F hardware keys
ZTNA (Zero Trust Network Access)	Secure access without VPNs	Scalar, Cloud flare Access
DLP & CASB Integration	Protect data in motion and at rest	Netscape, Force point
Immutable Backups	Ransomware resilience	AWS S3 Object Lock, Rubric, Vee am

settings, functionality access detection tools.
activity, user behaviours, and policy

5.9. Protection Mechanisms Recommended Security

To maintain a strong cybersecurity, the organizations should implement multiple layers of protection that can safeguard data, systems, and users. Here is some key recommended controls.

Explain how planning, risk assessment, vulnerability, and remediation works together to support ongoing information security maintenance?

Planning establishes security goals and defines the resources required to meet them. The risk assessment identifies potential threats and ranks them by likelihood and impact. The vulnerability assessment pinpoints weaknesses within systems, processes, or configurations. The remediation addresses are resolving the issues discovered during the assessments. These all steps ensure the security program adapts to evolving threats and maintains strong, up to date protection.

6.0. Controls Cloud Security Posture Management

This tools can help organizations to manage their cloud environments. So they can automatically find misconfigurations, ensure compliance with security standards, and show visibility across multiple cloud platforms. This keeps cloud services secure, compliant, and strong against changing threats. [34]

6.1. The Security Information and Event Management

SIEM, is a system that collects and examines security data from various parts of an organisation, including the network, servers, and applications. It helps detect suspicious activities in real time and supports incident response. It improves visibility, boosts threat detection, and ensures compliance with security regulations.

6.2 MFA Stand for Phishing Resistant Multi Factor Authentication

Is resistant to phishing Beyond of using passwords, and phishing-resistant multi-factor authentication (MFA) adds a crucial layer of security. Therefor users must use secure authentication factors, like hardware tokens or biometrics, to confirm their identity using this method. These factors are impervious to attempts at credential theft and phishing. [35] [36] [37].

Conclusion

Data security and compliance are essential for protecting sensitive information and maintaining trust. Organisations must use strong frameworks, continuous risk assessment, and secure technologies to prevent breaches and meet legal requirements. As threats evolve especially in cloud and AI systems Zero Trust, ongoing monitoring, and modern security tools help keep systems resilient. They ensure that information remains

safe, reliable, and legally handled. This research shows how frameworks like General Data Protection Regulation ,Digital Operational Resilience Act, International Organization for Standardization 27001and National Institute of Standards and Technology Cybersecurity Framework help organisations protect sensitive data while staying accountable and transparent. Also, real-world examples, such as the Cambridge Analytica scandal, illustrate that weak governance, poor access control, and lack of oversight can lead to serious consequences. The risk assessment, managing vulnerabilities, and timely fixes. The strong security measures like Cloud Security Posture Management, Security Information and Event Management, and phishing-resistant Multi-Factor Authentication are essential for creating a safe and reliable digital environment. Organisations can reduce risks and maintain compliance with data protection standards laws. These practices, businesses can stay secure, compliant, and prepared for future challenges.

The tasks one research shows the compliance frameworks like GDPR, ISO/IEC 27001, and the NIST Cybersecurity Framework how they play a critical role in protecting sensitive information and promoting accountability within organizations in the real world. These standards can helps reduce regulatory risks and also builds greater trust among stakeholders.

The Zero Trust model helps and guided by the idea of never trust, always verify offers a strong defence against complex cyber threats. In another side for Resilient Intellect Ltd, applying Zero Trust principles through identity management, least of privilege access, and ongoing monitoring strengthens both compliance efforts and day security. This layered approach today helps the organization stay flexible and prepared as threats evolve, while still meeting regulatory requirements.

Future Considerations

The cyber threats grow more advanced, organisations should:

- Use AI-powered tools threat detection for faster responses.
- Strengthen Zero-Trust security across all systems.
- Automate policy enforcement in hybrid and multi-cloud environments.
- Ongoing train employees to stay alert to new risks.

By adopting and following these strategies, businesses can build a resilient and adaptive cybersecurity framework ready for the future.

References IEEE Style

References

[1] H. J. M. Michael E. Whitman, 2022. [Online]. Available: https://faculty.cengage.com/works/9780357506431. [Accessed 12 10 2025].

[2] rudderstack, “rudderstack,” 07 05 2025. [Online]. Available: https://www.rudderstack.com/blog/data-security-compliance/. [Accessed 10 10 2025].

[3] “Dataprotection,” [Online]. Available: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection. [Accessed 15 10 2025].

[4] “Data protection,” [Online]. Available: https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation. [Accessed 8 10 2025].

[5] M. K. Malik, 23 03 2025. [Online]. Available: https://www.linkedin.com/pulse/ultimate-guide-cybersecurity-laws-policies-gdpr-iso-27001-malik-8e1af/. [Accessed 17 11 2025].

[6] dataprotection, “dataprotection,” [Online]. Available: https://www.dataprotection.ie/en/individuals/data-protection-basics/definition-key-terms. [Accessed 20 11 2025].

[7] “Cyber Security,” 10 06 2025. [Online]. Available: https://www.tekclarion.com/cyber-security/compliance-standards/#gdpr-hipaa-pcidss-and-sox. [Accessed 17 11 2025].

[8] “theknowledgeacademy,” 10 11 2025. [Online]. Available: https://www.theknowledgeacademy.com/blog/compliance-framework/. [Accessed 19 11 2025].

[9] D. Rockett, Technical Marketing Content, 07 05 2025. [Online]. Available: https://www.rudderstack.com/blog/data-security-compliance/. [Accessed 01 11 2025].

[10] S. McCallum, “BBC,” 23 12 2022. [Online]. Available: https://www.bbc.co.uk/news/technology-64075067. [Accessed 06 11 2025].

[11] E. B.V., “sciencedirect,” 27 10 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524001689. [Accessed 08 11 2025].

[12] A. Protect, “Airbus Protect,” 04 04 2023. [Online]. Available: https://www.protect.airbus.com/blog/active-directory-a-canary-under-your-hat/. [Accessed 21 11 2025].

[13] 03 11 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. [Accessed 21 11 2025].

[14] [Online]. Available: https://www.gov.uk/guidance/being-an-authorised-corporate-service-provider. [Accessed 21 11 2025].

[15] 12 05 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/reducing-the-active-directory-attack-surface?source=recommendations. [Accessed 21 11 2025].

[16] 2015. [Online]. Available: https://nmap.org/download#windows. [Accessed 21 11 2025].

[17] "Nmap," 2015. [Online]. Available: https://nmap.org/download.html. [Accessed 21 11 2025].

[18] M. A. Tour, "learn.microsoft.com," 27 06 2025. [Online]. Available: https://learn.microsoft.com/en-us/security/zero-trust/deploy/networks. [Accessed 29 11 2025].

[19] "Cisco Zero Trust Framework," 09 03 2023. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-network-cloud-dg.html. [Accessed 29 11 2025].

[20] "www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice," 28 11 2025. [Online]. Available: https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice. [Accessed 30 11 2025].

[21] 07 06 2025. [Online]. Available: https://www.ncsc.gov.uk/collection/cloud/using-cloud-services-securely/using-saas-securely. [Accessed 30 11 2025].

[22] C. s. professionals, 07 06 2023. [Online]. Available: https://www.ncsc.gov.uk/collection/cloud/using-cloud-services-securely/using-saas-securely. [Accessed 30 11 2025].

[23] 13 05 2025. [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device. [Accessed 13 10 2025].

[24] D. O. R. Act, 17 06 2025. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. [Accessed 15 11 2025].

[25] C. F. v2.0, 26 02 2025. [Online]. Available: https://csf.tools/reference/nist-cybersecurity-framework/v2-0/. [Accessed 13 11 2025].

[26] Hyperproo, "Hyperproo," 05 02 2025. [Online]. Available: https://hyperproof.io/resource/risk-management-techniques/. [Accessed 22 11 2025].

[27] metricstream, "metricstream," 2025. [Online]. Available: https://www.metricstream.com/learn/risk-identification.html#section-3. [Accessed 14 10 2025].

[28] C. Owen-Jackson. [Online]. Available: https://www.ibm.com/think/insights/cyber-criminals-compromising-ai-software-supply-chains. [Accessed 26 11 2025].

[29] A. K. S. a. S. Zeadally, 27 05 2025. [Online]. Available: https://cacm.acm.org/research/malicious-ai-models-undermine-software-supply-chain-security/. [Accessed 25 11 2025].

[30] 25 07 2025. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-trust-in-open-source-ai-the-hidden-supply-chain-risk-no-one-is-watching. [Accessed 15 11 2025].

[31] A. V. a. D. Patel, 25 07 2025. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-trust-in-open-source-ai-the-hidden-supply-chain-risk-no-one-is-watching. [Accessed 29 11 2025].

[32] A. V. a. D. Patel, 25 07 2025. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-trust-in-open-source-ai-the-hidden-supply-chain-risk-no-one-is-watching. [Accessed 30 11 2025].

[33] S. Barker, 16 11 2025. [Online]. Available: https://hightable.io/iso-27001-annex-a-5-27-learning-from-information-security-incidents/. [Accessed 28 11 2025].

[34] 19 10 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management. [Accessed 22 11 2025].

[35] 11 2023. [Online]. Available: https://www.cyber.gov.au/business-government/protecting-devices-systems/hardening-systems-applications/system-hardening/implementing-multi-factor-authentication. [Accessed 22 10 2025].

[36] 27 11 2023. [Online]. Available: https://www.cyber.gov.au/business-government/protecting-devices-systems/hardening-systems-applications/system-hardening/implementing-multi-factor-authentication. [Accessed 22 11 2025].

[37] F. C. H. Ryan Rowcliffe, 16 11 2024. [Online]. Available: https://securityboulevard.com/2024/09/what-is-phishing-resistant-mfa-and-how-does-it-work/. [Accessed 23 11 2025].

[38] H. J. M. Michael E. Whitman, 2022. [Online]. Available: https://faculty.cengage.com/works/9780357506431. [Accessed 12 10 2025].