

**Name: Anis Ur Rehman**

**ID : 23031710**

**Date of submission: 22/Nov/24**

**[LO2] Systematic application of the tools, methods and procedures (theoretical and methodological) used within the cyber security arena under the context of a risk and threat assessment**

**These are bellow few steps in which fulfill the requirements of the task:**

**1. Tools**

Tools are essential for systematic identification and assessment of risks and threats.

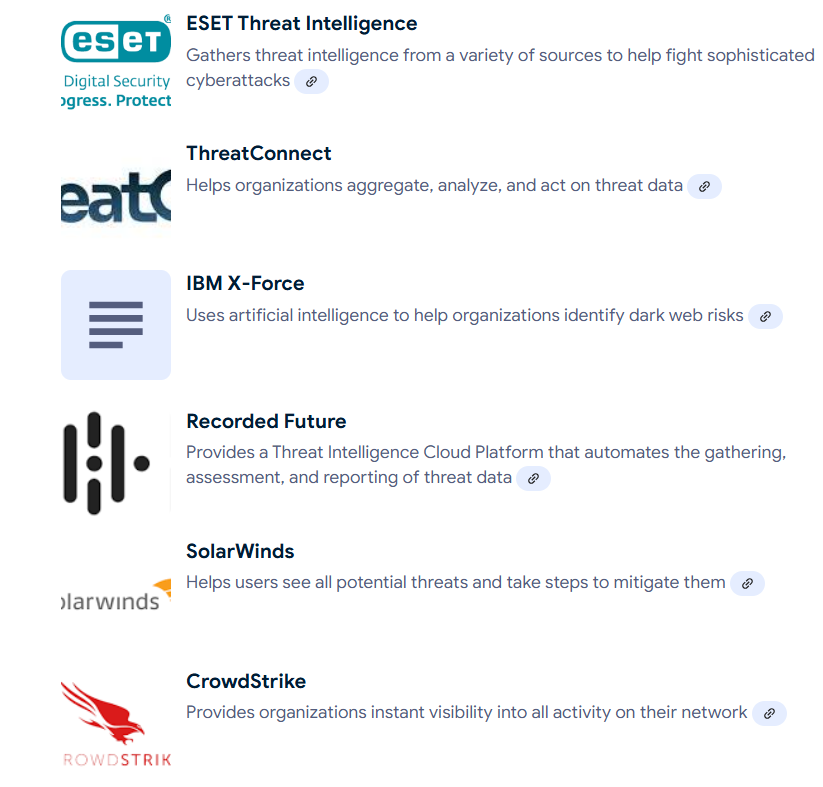
**Vulnerability scanners:** Tools such as Nmap, Nessus, and OpenVAS identify potential vulnerabilities in systems and networks.

**Penetration testing frameworks:** Tools such as Metasploit and Burp Suite are used to simulate attacks and assess system resilience.

**Risk assessment platforms:** Tools such as RiskWatch and GRC (Governance, Risk, and Compliance) software help map risks to organizational priorities.

**Threat intelligence platforms:** Tools such as IBM X-Force, Recorded Future, and AlienVault collect threat intelligence in real time and proactively identify risks.

Also some more in the bellow picture:



**2. Methodology**

Methodologies determine how tools and procedures are applied:

**Risk Assessment Framework:**

* NIST Risk Management Framework (RMF): Guides organizations in categorizing systems, selecting controls, and monitoring risk.
* ISO/IEC 27002: Provides a structured approach to information security risk management.

**Threat Modeling:** Analyzes potential threats and vulnerabilities through techniques such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service(DOS), Privilege Escalation).

**Kill Chain Analysis:**

* Maps an attacker's steps from reconnaissance to execution, enabling defenders to predict and mitigate attacks.
* **OWASP Risk Assessment Methodology:** Focuses on assessing web application vulnerabilities and ranking them by severity and probability.

Refrence link: https://owasp.org/www-community/OWASP\_Risk\_Rating\_Methodology

**3. Procedures of the:**

Step-by-step procedures ensure consistent application of tools and techniques.

**i. Inventory:**

Identify critical assets (hardware, software, data) and their vulnerabilities.

**ii. Threat Identification:**

Use tools and intelligence platforms to identify potential threat actors, such as insiders, external hackers, and advanced persistent threats (APTs).

**iii. Risk Analysis:**

Evaluate risk by combining probability and impact assessment.

Tools such as the Common Vulnerability Scoring System (CVSS) are often used in this step.

**iv. Prioritize:**

Apply frameworks such as the Pareto principle or risk matrix to focus resources on high-risk areas.

**v. Implement controls:**

Use preventive, detective, and corrective controls to mitigate identified risks.

**Vi. Monitor and reassess:**

* Continuously monitor for threats using a Security Information and Event Management (SIEM) solution such as Splunk or QRadar.
* Periodic reassessment ensures adaptive security.

**Example: Applications in IoT Security**

**Tools:** Use IoT Inspector or Wireshark for network packet analysis.

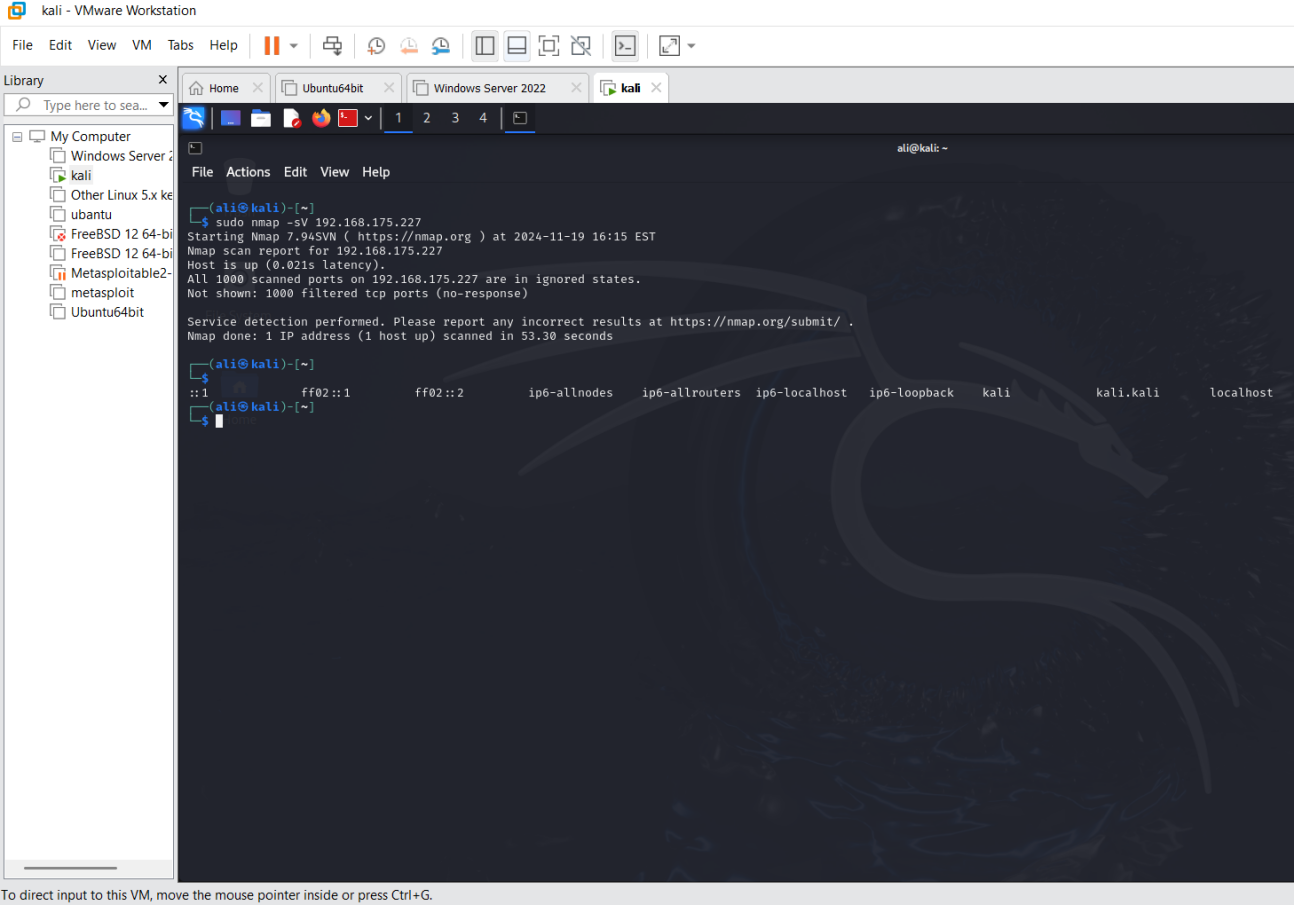
Methodology: Apply threat modeling (STRIDE) to identify vulnerabilities in IoT communication protocols.

**Methodology:**

Identify IoT devices on your network.

Perform a vulnerability scan using Nmap.

Analyze captured packets for anomalies.



**[LO3] Demonstrate the ability to critically demonstrate self-direction and creativity in managing the security of an information environment at the strategic, tactical and operational levels, effectively developing information security policies;**

Developing a comprehensive information security policy is essential to effectively manage the security of information environment at the strategic, tactical, and operational levels. This process includes several important steps to ensure that the policy is not only effective, but also aligned with organization's goals and responsive to emerging threats:

**Define Scope and Purpose.**

**Establish Clear Boundaries:** The first step in creating an information security policy is to define its scope and purpose. This includes identifying the information assets, systems, networks, and personnel that are covered by the policy. A clearly defined scope helps all involved parties understand the purpose and limitations of the policy12.

**Align with business objectives:** Policy objectives should be specific, measurable, achievable, relevant, and time-bound (SMART). Aligning these objectives with broader business goals helps ensure that policies support corporate strategy1.

**Conduct a risk assessment:**

**Identify threats and vulnerabilities:** A thorough risk assessment is essential to understand potential threats to an organization's information environment. This process includes evaluating existing systems and identifying vulnerabilities that could be exploited by an attacker24.

**Gap analysis:** Conduct a gap analysis to determine what security measures are currently in place and where improvements are needed. This analysis helps identify areas where additional controls or policies are needed2.

**Policy Development:**

**Key or Vital Components:** An effective information security policy should contain several key elements:

**Purpose:** Articulate why the policy exists.

**Scope:** Specify in detail what the policy covers.

**Roles and Responsibilities:** Define who is responsible for implementing and monitoring the policy.

**Procedures:** Outline specific steps for compliance and enforcement35.

**Incorporate Compliance Standards:** Ensure that your policies address relevant laws, regulations, and ethical standards for your industry. This may include frameworks such as HIPAA, PCI DSS, and SOC 235.

**Implementation and Maintenance:**

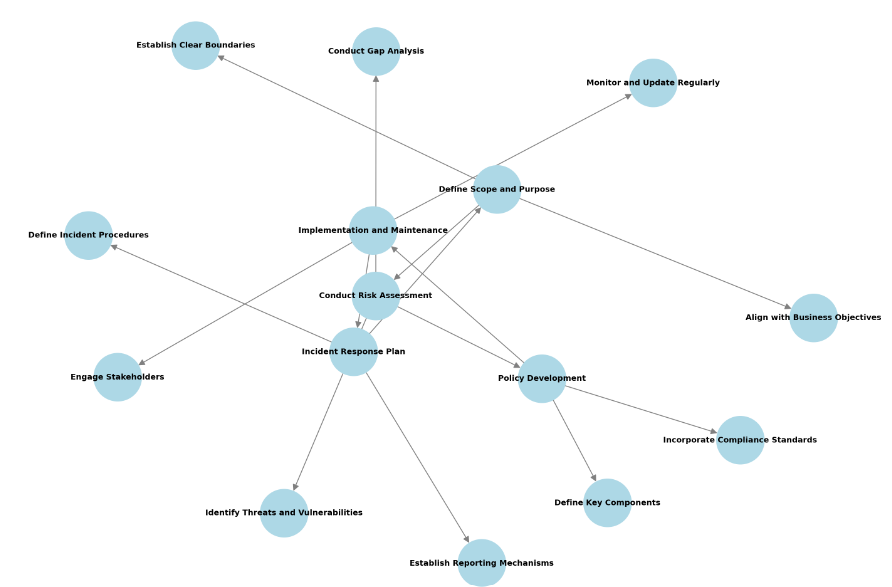
**Stakeholder Engagement:** Involve key stakeholders during both the development and implementation phases. Insights can help improve the relevance and effectiveness of your policies. Regular training can promote a safety-conscious culture within your organization24.

**Regularly Monitor and Update:** The information security landscape is constantly evolving. Therefore, it is important to regularly review and update policies to adapt to new threats and changes in business operations. Establishing a policy review routine ensures continued relevance and compliance13.

**Incident Response Plan:**

**Define Security Incident Procedures:** Add clear procedures for responding to security incidents such as data breaches and cyber attacks. This should include reporting mechanisms, investigation protocols and corrective actions.

**information Security Policy Management Process:**



**[LO4] Demonstrate the ability to take initiative to autonomously conduct and manage a risk assessment of a complex and unpredictable environment;**

**1. Understand the environment and context**

**Gather information:** Identify and collect relevant data about the environment, stakeholders, and operational objectives.

**Analyze complexity:** Assess factors such as uncertainty, interdependencies, and variability that contribute to the unpredictability of the environment.

**2. Determine the scope of the risk assessment.**

* Clarify goals and boundaries.
* Identify key assets, processes, or systems that need to be protected.
* Prioritize based on the potential impact of risks.

**3. Identify Risks**

* Use a structured approach to uncover potential risks. For example:
* Brainstorming sessions.
* Review historical data and trends.
* Collaborate with experts and stakeholders.
* Consider different risk categories (financial, operational, environmental, technical, etc.).

**4. Analyze and Assess Risks**

**Assess Probability and Impact:**

* Use qualitative or quantitative methods to assess the likelihood and potential impact of each risk.
* Prioritize Risks:
* Rank risks by severity to allocate resources effectively.

**5. Develop a risk mitigation strategy**.

* Create a plan of action to address high priority risks.
* Avoid: Modify plans to eliminate risk.
* Reduce: Implement controls to minimize impact.
* Transfer: Outsource risk or insure against risk.
* Accept: Monitor and prepare for risks that are deemed acceptable.

**6. Implement and Monitor**

* Implement a risk mitigation plan with clear roles, responsibilities, and timelines.
* Establish a monitoring system to track risk indicators and detect emerging threats.

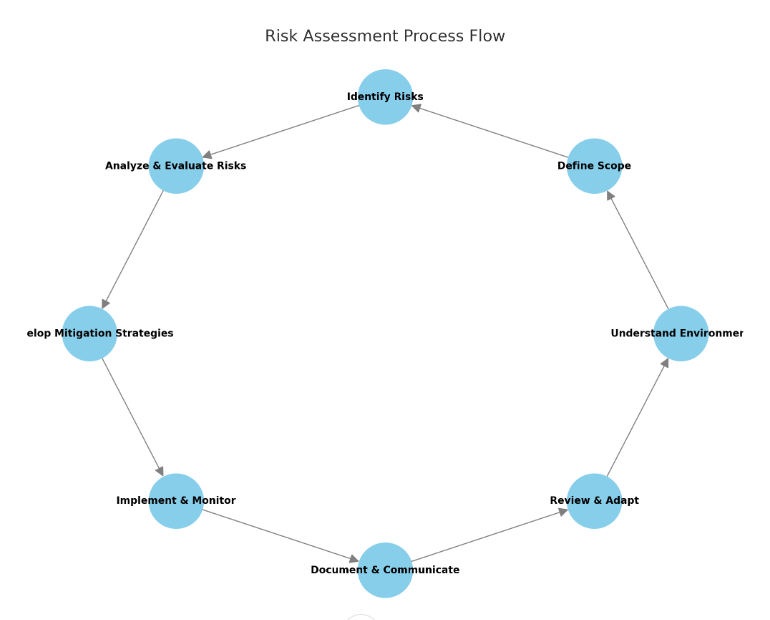
**7. Document and Communicate.**

* Record the risk assessment process, results, and decisions.
* Share information with relevant stakeholders to ensure alignment and accountability.

**8. Review and Adjust**

* Continually monitor changes in the environment.
* Regularly review and update risk assessments to reflect new challenges and insights.

**Risk Assessment Process Flow Chart:**



**[LO5] Demonstrate the ability to take a systematic approach of creatively applying security standards to unfamiliar contexts for solving problems.**

**1. Understand the context.**

**Analyze the unknown environment:**

* Identify key characteristics, stakeholders, assets, and potential vulnerabilities.

**Clarify the objective:**

* Define what the security standard needs to accomplish in this specific situation (confidentiality, integrity, availability, security, etc.).

 The CIA triad

**2. Review relevant security standards.**

**Identify applicable frameworks:**

Consider standards such as ISO 27001, NIST, GDPR, or industry-specific standards.

**Identify core principles:**

Understand the basic elements of the standard (risk management, access control, encryption, incident response, etc.).

**3. Assess gaps and challenges:**

* Assess how unfamiliar contexts differ from standard use cases.
* Identify constraints such as resource limitations, special environmental factors, cultural aspects, etc.

**4. Adapt and Apply Standards Creatively.**

**Tailor your implementation:**

* Adapt your security measures to the situation without losing sight of the core principles.

**Innovate within the framework:**

* Combine standards and unconventional methods to address unique challenges (e.g., use non-traditional encryption tools for resource-constrained systems).

**5. Design Systemic Solutions.**

**Integrate security standards:**

* Create a coherent solution that maps standard requirements to the unique characteristics of the context.

**Test and Iterate:**

* Validate your solution in simulations or pilots and refine based on the results.

**6. Document and Justify Decisions.**

* Maintain detailed records of how standards were interpreted and applied.
* Justify adjustments to ensure transparency and traceability.

**7. Evaluate and Monitor Implementation.**

* Continually evaluate the effectiveness of the solution through audits, feedback and monitoring.
* Adapt to new threats and changes in an unfamiliar environment.

**Use Case**

**Scenario:**

A rural clinic with limited internet connectivity and no IT staff needs to protect patient records.

Application:

1. **Understand the context:**

Analyze the clinic's workflow and technical limitations.

**II. Select a standard:**

Use HIPAA and ISO 27001 as a guide.

**III. Identify the gaps:**

Access to cloud-based solutions is limited.

**IV.Creative Customization:**

Implement offline encryption for patient records and use manual logging for access control.

**V. Design Solution:**

Train staff on basic security measures.

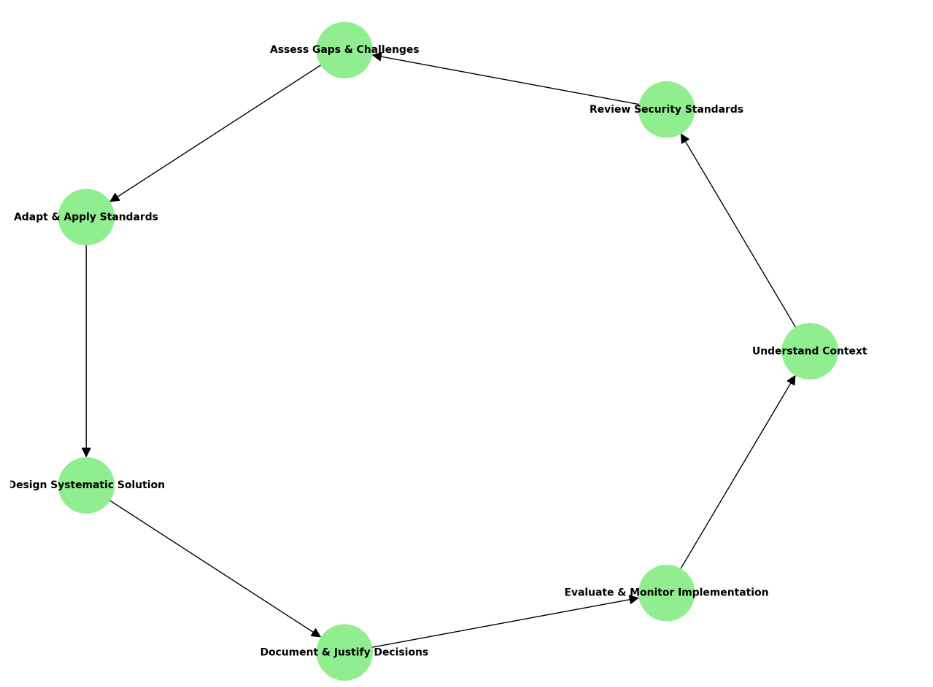
**VI. Documentation:**

Record decisions and justify the use of encryption over manual alternatives.

**VII. Evaluation:**

Monitor compliance and effectiveness over time

**Systematic Approach to applying Security standards graph:**



1. **Synnovis Context and Operations:**

Overview of the Synnovis

Synnovis is a pathology partnership providing diagnostic services essential to patient care. It operate collaboratively works with Guy's and St Thomas' NHS Foundation Trust, King's College Hospital NHS Trust and SYNLAB. Synnovis supports healthcare providers with diagnostic solutions and focuses on delivering timely and accurate medical results such as: B. Blood tests and biopsies that are essential to patient treatment.

**Vital Operations:**

1. **Medical diagnostics:**

* Processing millions of pathology tests annually.
* Supporting healthcare professionals with accurate test results.
* Electronic delivery of diagnostic reports to NHS partners and other stakeholders.

1. **Information Management:**

* Manages Electronic Health Records (EHR) containing confidential patient information.
* Processes diagnostic service requests and distributes results via networked IT systems.

**iii. Stakeholders:**

* NHS hospitals, GPs, laboratories, regulators, patients.
* External partners such as the National Cyber Security Centre (NCSC) and private contractors supporting the IT infrastructure.

**Dependence on IT systems:** Synobis relies heavily on its IT ecosystem to:

* Ensure 24/7 availability of key diagnostic services;
* Maintain secure, efficient and accurate data storage and processing;
* Enable rapid communication between hospitals, laboratories and doctors.

**Impact of the ransomware attack (June 2024):**

* Service interruption: Diagnostic processes at GP practices and hospitals were affected, requiring manual operations in some areas.
* Data breach: Sensitive patient information was stolen and shared, exposing the company to legal and reputational risks.
* Operational Recovery: Gradual restoration of IT services, with some capabilities expected to be fully operational by Fall 2024.

**2. Threat Landscape and Challenges**

Synnovis operates in the highly regulated and sensitive healthcare sector, making it a target for cyber threats. Below is an analysis of the threat landscape and operational challenges:

**Threat Landscape:**

1. **Cyber Threats:**

* **Ransomware attacks**: encrypt systems and demand a payment for the decryption key. The June 2024 attack is an example of this threat.
* **Data Breach:** unauthorized access to sensitive patient records, possible GDPR violation.
* I**nsider threats:** Malicious or accidental employee actions leading to data leaks or system vulnerabilities.
* **Phishing attacks**: Cyber criminals take advantage of employee negligence to gain access to critical systems.

1. **Regulatory threats:**

* Failure to comply with GDPR and NHS specific data protection requirements can result in significant fines.High profile data breaches have led to
* increased scrutiny from the Information Commissioner's Office (ICO) and the media.

**iii. Technological threats:**

* Vulnerabilities in outdated IT systems or unpatched software.
* Weak access controls or ineffective password policies.

**iv. Third-party risks:**

* Dependence on contracted partners for IT infrastructure can lead to security gaps.
* Supply chain risks, especially if providers aim for indirect access to Synnovis' systems.

**Operational challenges:**

1. **Service continuity:**

* Disruptions to diagnostic services are impacting hospitals and GP practices, delaying patient treatment.
* Reliance on manual processes during IT outages reduces efficiency and increases error rates.

**ii. Data sensitivity:**

* Patient files contain highly sensitive information, making them attractive to attackers.
* Unauthorized access can lead to legal consequences and loss of trust between parties.

**iii. Resource limitations:**

* Limited budgets for cybersecurity improvements delay critical upgrades.
* There is a shortage of qualified personnel to effectively manage and mitigate cyber risks.

**iv. Complex IT ecosystem:**

* Managing networked systems across multiple NHS partners and laboratories increases vulnerability to cyber attacks.
* Seamlessly integrating recovered systems after an attack is a logistical challenge.

**v. Public and stakeholder trust:**

* Negative media coverage following a breach could damage the organization's reputation.
* Stakeholders such as patients and healthcare providers may lose confidence in Synovis's ability to protect their data.

**3. List of Assumptions**

The following assumptions (including fictitious data) are developed to support this **t I.**

1. **Operational Assumptions and Policy Dev:**

* Synnovis handles and work on 10 million diagnostic tests data annaully.

The company operates three major data centers with significant IT infrastructure.

* Approximately 80% of diagnostic workflows are automated, with the remainder relying on manual intervention.

**ii. Cybersecurity Assumptions:**

* A ransomware attack in June 2024 affected 60% of IT systems, including patient data databases and communication interfaces.
* backup systems were partially encrypted, delaying full system restore.
* Multi-factor authentication (MFA) was not uniformly applied to all access points.

**iii. Organizational Assumptions:**

* Synnovis employs 1,000 people, 30% of whom work remotely.
* Employee cybersecurity awareness training is conducted annually but does not meet best practices in scope or depth.

**iv. Risk and Threat Assumptions:**

* The ransomware attack originated from a phishing campaign targeting employees.
* Primary vulnerabilities include outdated operating systems and lack of endpoint security tools on workstations.
* Threat actors used stolen credentials to bypass weak password policies.

**v. Regulatory Assumptions:**

* Synnovis must meet the following requirements:
* GDPR to protect patient data.
* ISO 27001/27002 for information security management.
* Information Commissioner's Office (ICO) specific requirements.

All the above policy rule is according to the ISO 27001/27002

**vi. Stakeholders and socio-cultural assumptions:**

* Stakeholders expect diagnostic services to be available 24/7.
* Public trust in Synnovis depends on transparent communication and rapid response following security incidents.