**Step 1: Understand the Assignment**

* **Module: Information Security (402IT)**
* **Tasks: There are three tasks:**
  1. **Information Security Risk Assessment (40%)**
  2. **Penetration Testing and Reporting (40%)**
  3. **Security Policies Development (20%)**

**Ensure your submission adheres to the provided guidelines and includes:**

* **Proper formatting and APA7 referencing.**
* **Appendices for supporting documents like reports.**

**Step 2: Task 1 - Risk Assessment (40%)**

1. **Introduction:**
   * **Define information security and its importance.**
   * **Highlight best practices and industry standards (e.g., ISO/IEC 27001, NIST SP 800-30).**
2. **Risk Identification:**
   * **Identify assets in the hospital case study (hardware, software, data).**
   * **Create an Asset Register with descriptions, locations, and values.**
   * **Identify vulnerabilities for each asset.**
3. **Risk Analysis and Evaluation:**
   * **Use a standard method (e.g., NIST, ISO 27005) to analyze and evaluate risks.**
   * **Provide examples of threats, impacts, and likelihood.**
   * **Summarize findings in a table or matrix.**

**Deliverable: A technical report summarizing the findings and including the Asset Register in an appendix.**

**Step 3: Task 2 - Penetration Testing (40%)**

1. **Setup:**
   * **Use tools like Kali.**
   * **Simulate hospital systems (e.g., windows servers, legacy Windows XP).**
2. **Penetration Testing (20%):**
   * **Perform scans (e.g., Nmap, Nessus) to identify vulnerabilities.**
   * **Exploit vulnerabilities (safely and legally within the virtual environment).**
   * **Phishing attack**
   * **Sql injection**
   * **Open Vas report**
3. **Report (20%):**
   * **Follow a standard format (e.g., OWASP Testing Guide).**
   * **Include:**
     + **Methodology**
     + **Findings (vulnerabilities, exploits)**
     + **Remediation recommendations.**

**Deliverable: A detailed penetration test report included as an appendix.**

**Step 4: Task 3 - Security Policies (20%)**

1. **Access Control Policy (10%):**
   * **Define roles and permissions.**
   * **Use examples (e.g., role-based access control for patient data).**
2. **Acceptable Use Policy (10%):**
   * **Outline guidelines for IT resource use.**
   * **Address internet, email, and device usage.**
3. **Impact Explanation:**
   * **Discuss how the policies support confidentiality, integrity, and availability.**

**Deliverable: Policies presented clearly in the main report.**

**Step 5: Compile and Format the Report**

1. **Structure:**
   * **Cover Page: Include module details and your information.**
   * **Table of Contents: Organize tasks and appendices.**
   * **Main Sections:**
     + **Task 1: Risk Assessment**
     + **Task 2: Penetration Testing**
     + **Task 3: Security Policies**
   * **Appendices: Asset Register, Penetration Test Report.**
2. **Formatting:**
   * **Use Calibri/Arial, 12 pt font, 1.5 line spacing.**
   * **Use APA7 for references and citations.**