

Required Source Information and Tools

To complete the project, you need the following:

Course textbook

Access to the Internet

Microsoft Word and Microsoft PowerPoint, or compatible editing and presentation software

Learning Objectives and Outcomes

By the end of this project, you will know how to:

Describe an appropriate data classification scheme for a given scenario.

Evaluate and select a risk assessment methodology.

Create a gap analysis plan.

Explain how to assess risks, threats, and vulnerabilities.

Evaluate potential outcomes of a malware attack and exposure of confidential information.

Evaluate information systems security countermeasures.

Analyse the purposes of system hardening.

Evaluate information systems security activities in terms of business success.

Project Scenarios

Each group will choose one scenario. You will be working on this scenario for the remaining of the module

1. E-Commerce Platform (TechTraders Ltd.)

TechTraders Ltd. is an online retail store that sells consumer goods such as electronics, clothing, and home essentials. They operate through a website and mobile app, providing users with the ability to browse products, make purchases, and interact with customer service.

2. Healthcare Management System (MediCare Solutions)

MediCare Solutions is a healthcare provider, such as a hospital or clinic, that uses an integrated Electronic Health Records (EHR) system. They store patient medical histories, appointment details, lab results, prescriptions, and treatment plans.

3. Financial Management System (FinSecure Bank)

FinSecure Bank is a financial institution, such as a bank or investment firm, that offers an online platform for managing accounts, processing transactions, providing loans, and managing investments.

4. Learning Management System (EduFlex school)

EduFlex school is a school that uses an online Learning Management System (LMS) to manage courses, track student progress, and deliver educational materials.

5. Public Booking System (GovBook Services)

GovBook Services is a government agency that operates a public booking system allowing citizens to book appointments for various public services, such as passport applications, driving license renewals, social services, and public health consultations.

Deliverables

The project is divided into several parts. Details for each deliverable can be found in this document. Due dates for each part are listed in the course Syllabus.

- Week 1. Developing an Information Security Management Plan
- Week 2. Analysing Security Needs
- Week 3. Debating Ethical Dilemmas in Information Security
- Week 4. Strategic Planning for Security Governance
- Week 5. Evaluating Different Security Management Models
- Week 6. Creating a Contingency Plan
- Week 7. Conducting Risk Assessment
- Week 8. Security Technologies- Firewalls and VPNs**
- Week 9. Cryptography protection
- Week 10. Security Maintenance

Objective: Conducting Risk Assessment

Risk management work phase (1 hour)

Each group must:

a) Choose Suitable Firewall Types

1. Evaluate different Firewall types (e.g., Packet-Filtering Firewalls, Stateful Inspection Firewalls, Proxy Firewalls, Next-Generation Firewalls (NGFWs)).
2. Determine the most appropriate firewall type(s) for your system, considering factors such as:
 - Sensitivity of data being processed
 - Threat landscape and risk exposure
 - System architecture (e.g., cloud-based, on-premises, hybrid)
 - Compliance requirements
3. Justify why the chosen firewall is best suited for your system.
4. Research a specific firewall product that meets the type you identified.

Consider factors such as:

- Vendor reputation and support
- Features and functionalities
- Cost and scalability
- Integration with existing security infrastructure

b) Choose Suitable VPN Types

1. Assess different VPN types (e.g., Site-to-Site VPN, Remote Access VPN, SSL VPN, IPSec VPN).
2. Determine the most appropriate VPN solution for your system, considering:
 - Who needs remote access (e.g., employees, contractors, customers)
 - Level of encryption and security required
 - System integration with existing security infrastructure
 - Compliance and data privacy regulations

c) Justify why the selected VPN type is the best fit for your system.

d) Monitoring and Maintenance: Identify how firewall logs and VPN access logs will be monitored and reviewed for security compliance

Presentation (10 minutes each)

Each group will briefly present their findings, explaining:

- Key network security requirements based on last week's risk assessment.
- Chosen firewall type and justification.
- Researched firewall product and why it meets the needs.
- Chosen VPN type and justification.

Class Discussion (30 minutes)

The remaining of the session is focused on the assignment and how you should align this week activity with the assignment tasks.