

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. Threat modelling and vulnerability assessment
- Week 9. Securing the perimeter

Objective: Design a Disaster recovery plan and a Business Continuity plan

Analyse Your Scenario

1. Identify potential disasters or events (natural or man-made) that could impact your organisation.
2. Highlight critical business functions and assets essential for continuity and recovery.

Designing the Business Continuity Plan (BCP)

1. *Form the BC Team:*

- Define roles and responsibilities within your scenario organization.
- Assign personnel for plan development, testing, and maintenance.

2. *Outline BC Strategies:*

- **Exclusive-Use Options:** Decide on hot, warm, or cold sites.
- **Shared-Use Options:** Explore timeshares, service bureaus, or mutual agreements.
- **Specialised Options:** Consider mobile sites or external resources.

3. *Develop the BC Policy:*

- In a brief statement for each, write the following:
 - Purpose, scope, resource requirements, roles, and training.

4. *Ensure Maintenance:*

- Incorporate testing, exercises, and periodic updates.

Designing the Disaster Recovery Plan (DRP)

1. *Define Disaster Classifications:*

- **Natural or man-made.**
- **Rapid or slow onset.**

2. *Outline Recovery Steps:*

- Prioritise critical assets and systems.
- Define roles for recovery tasks like system restoration and data recovery.

3. *Develop the DR Policy:*

- Include key elements like scope, training, and testing.

4. Testing and Improvement:

- Identify suitable methods such as simulations, desk checks, or structured walkthroughs.

Presentation

Prepare a 10-minute presentation covering:

- Key threats identified.
- Highlights of the BC and DR plans.
- Strategies chosen and their justification.
- Testing and maintenance approaches.

Upload your presentation file to the relevant weekly activity post on the module forum.