# Cybersecurity Risk Management — Scenario Document

## Scenario

This project focused on conducting a detailed risk management exercise for a medium-sized enterprise. The scope included identification of potential cyber threats, assessment of risks, and evaluation of the business impact. Based on the findings, controls and mitigation strategies were proposed to strengthen the organization’s overall security posture.

## Key Objectives

1. Perform risk identification and classification of cyber threats. 2. Conduct risk assessment with likelihood and impact evaluation. 3. Define Recovery Time Objective (RTO) and Recovery Point Objective (RPO). 4. Recommend security controls to mitigate identified risks. 5. Develop a business continuity plan and incident response strategy.

## Frameworks & Standards Applied

The project aligned with several internationally recognized frameworks and standards: • NIST Cybersecurity Framework (CSF): For risk assessment, mitigation planning, and security controls. • ISO/IEC 27001: For establishing information security management controls. • ISO 31000: For risk management methodology and decision-making. • ACSC Essential Eight: For baseline mitigation strategies against cyber incidents.

## Deliverables

• Risk Assessment Report documenting identified risks, likelihood, and impact ratings. • Business Impact Analysis (BIA) detailing critical assets, systems, and dependencies. • Business Continuity Plan (BCP) outlining recovery objectives and strategies. • Security Control Recommendations mapped to industry frameworks.

## Skills Applied

• Cybersecurity Risk Assessment • Business Impact Analysis (BIA) • Incident Response Planning • Governance, Risk, and Compliance (GRC) • Application of security frameworks (NIST CSF, ISO 27001, ISO 31000, ACSC Essential Eight) • Technical documentation and reporting