RISK ASSESSMENT REPORT

ACME Online Store (E-Commerce Platform)

Prepared by: Tarun Kalyani
Date: 15th October 2025

Self-Directed Project

Regulations: PIPEDA, PCI DSS

Executive Summary

This report presents a simulated information security risk assessment conducted for ACME Online Store, a fictional e-commerce organization that processes customer personal information and payment card data. The objective of this assessment was to identify critical information assets, evaluate associated threats and vulnerabilities, and assess risks to business operations while aligning security controls with PIPEDA and PCI DSS requirements.

The assessment focused on key systems, including the customer database, payment processing environment, e-commerce website, employee email systems, staff laptops, and cloud hosting infrastructure. A qualitative risk assessment methodology was applied, evaluating risks based on impact and likelihood and categorizing them as low, medium, or high. Inherent risk levels were identified prior to control implementation, with residual risk estimated after recommended mitigation measures.

The assessment identified customer data protection, payment card data security, and phishing-related threats as the highest risk areas. These risks could result in regulatory non-compliance, financial loss, and reputational damage if not adequately addressed. Recommended controls include multi-factor authentication, encryption of sensitive data, role-based access controls, security awareness training, and enhanced logging and monitoring.

Overall, implementing the recommended controls would significantly reduce ACME Online Store's risk exposure and strengthen its security posture while supporting compliance with PIPEDA's Safeguards Principle and key PCI DSS requirements. This assessment demonstrates a practical application of governance, risk, and compliance (GRC) principles within an e-commerce environment

Organization Overview

ACME Online Store is a mid-sized e-commerce company that sells consumer products through a web-based platform. The organization processes customer personal and payment information, manages online orders, and relies on cloud-based infrastructure to support daily operations. Due to the nature of e-commerce, the confidentiality, integrity, and availability of information systems are critical to business success and customer trust.

Scope of Risk Assessment

The scope of this risk assessment includes ACME Online Store's primary information assets involved in online sales and internal operations. The assessment covers digital assets such as e-commerce websites, customer databases, payment systems, employee email, and staff laptops. Physical security and third-party vendor assessments were considered out of scope for the exercise.

Methodology

This assessment was conducted using a qualitative risk assessment approach. Key information assets were identified, and potential threats, vulnerabilities, impact, inherent risk, and residual risk were documented for each regulation against PIPEDA and PCI DSS. Risks were evaluated based on estimated impact and likelihood and categorized as low, medium, or high. For risks rated as medium or high, appropriate administrative, technical, and organizational controls were recommended to reduce risk to an acceptable level.

Keys Findings

This risk assessment identified several high-risk assets requiring enhanced security controls. The customer database was assessed as a high-risk asset due to the potential for unauthorized access to personally identifiable information (PII), which could result in privacy breaches and loss of customer trust under PIPEDA.

The employee email system was also identified as high risk, as it is a common target for phishing attacks that may lead to credential compromise and unauthorized access to internal systems and customer data.

In addition, the payment processing system was identified as a high-risk asset due to its role in handling payment card information. Inadequate protection of cardholder data could result in financial fraud and non-alignment with PCI DSS requirements. Risks associated with this asset include third-party dependency, improper access controls, and insufficient monitoring of payment transactions.

While the organization relies on a cloud hosting environment to support its web-based platform, the use of cloud services is permitted under PIPEDA and PCI DSS provided that appropriate safeguards are implemented. Weak encryption, insufficient vendor oversight, or inadequate access controls could increase the risk of non-compliance and data compromise.

Recommendations

- **Strengthen Access Controls for Customer and Payment Data**

  Implement multi-factor authentication (MFA) and role-based access control (RBAC) for systems storing or processing customer personal information and payment data. Access to sensitive systems should be restricted to authorized personnel only and reviewed periodically to ensure continued appropriateness.

  This supports PIPEDA safeguarding requirements and PCI DSS access control expectations.

- **Encrypt Sensitive Data at Rest and in Transit**

  Ensure that customer personal information and payment-related data are encrypted both at rest and during transmission. Encryption keys should be securely managed, and access limited to authorized roles.

  This reduces the risk of unauthorized disclosure and supports PIPEDA and PCI DSS data protection principles

- **Enhance Security Awareness and Phishing Protection**

  Provide regular security awareness training to employees, with a focus on phishing detection and safe email practices. Implement email security controls such as spam filtering and phishing detection to reduce the likelihood of credential compromise.

  This mitigates high-risk threats related to employee email systems.

- **Strengthen Payment Processing and Third-Party Oversight**

  Where possible, limit the storage and handling of cardholder data by using tokenization or trusted third-party payment processors. Conduct periodic reviews of third-party security practices to ensure continued alignment with PCI DSS requirements.

  This reduces financial fraud risk and third-party exposure.

- **Improve Cloud Security and Vendor Accountability**

  Ensure cloud service providers implement appropriate safeguards, including strong access controls, encryption, logging, and incident response capabilities. Clear roles and responsibilities should be established to maintain accountability for personal information under PIPEDA.

  This addresses shared-responsibility risks associated with cloud hosting.

- **Establish Ongoing Monitoring and Incident Response Processes**

  Implement logging and monitoring for critical systems to detect unauthorized access or suspicious activity. Develop and maintain an incident response plan to ensure timely detection, containment, and notification of security incidents involving personal or payment data.

  This supports compliance readiness and operational resilience.

Conclusion

This risk assessment identified key risks affecting ACME Online Store's customer and payment data, with the customer database, employee email system, and payment processing environment assessed as the highest-risk assets. Using a qualitative risk-based approach, risks were prioritized based on impact and likelihood to support effective decision-making. The assessment highlights the need for stronger access controls, encryption, employee security awareness, and third-party oversight to support alignment with PIPEDA and PCI DSS. Implementing these controls would significantly reduce risk exposure and strengthen the organization's overall security and compliance posture.

.