# Secure Architecture Report and Recommendation
# Course 11 Project

By Evelyn Wolfe
Cohort: Sept 23 2024 Cyber Security Flex

# Executive Summary

To meet evolving security demands, regulatory obligations, and operational needs, the organization requires a modernized security architecture built on industry best practices. Our strategy is designed to strengthen the protection of sensitive systems and customer data, while ensuring business continuity and supporting scalable, secure growth.

The proposed architecture is guided by a phased implementation plan aligned with **NIST SP 800-53** controls and the **NIST Cybersecurity Framework**, with considerations for **PCI DSS** and **PIPEDA** compliance. Core security domains addressed include **Network Security, Data Protection, Endpoint Security, Identity and Access Management (IAM), Cloud Security, Incident Response, Physical Security**, and **Security Awareness Training**. These domains will serve as the foundation for a layered defense model and long-term resilience.

While this document provides an overview of our strategic goals for the future of the security architecture, the **accompanying video presentation** highlights a focused security strategy centered on three critical pillars: **Network Security, Identity and Access Management (IAM), and Incident Response**. It also walks through a **phased implementation timeline**, beginning with immediate actions to address urgent risks and progressing into short-, mid-, and long-term initiatives. The goal of this approach is to strengthen our security posture while minimizing disruption to employees—and most importantly, to ensure that our clients' and customers' data remains secure at every stage. By building a secure, scalable framework, we'll fulfill compliance expectations, support long-term growth, and continue to earn the trust of those we serve.

# Slide Deck and Video Presentation

- Slide Deck for Security Architecture Review
- Video Presentation

# Current Security Landscape

A security review revealed significant architectural weaknesses that threaten business operations and data security. While a basic firewall is in place, the network lacks segmentation, with all traffic routed through VLAN1 making it easy for threats to move laterally. The overall design lacks layered defenses and centralized oversight, exposing sensitive assets to unnecessary risk. Most critically, the Private Payment Network remains unprotected behind an open external connection (76.71.1.105/28), creating a direct path for potential intrusions. Without an Intrusion Detection or Prevention System (IDPS), malicious activity can go undetected, and the absence of network visibility tools further hinders threat detection and response across the environment.

Endpoint security is weak, with unpatched systems, no EDR, and poor access controls. Authentication relies solely on passwords, lacking Multi-Factor Authentication (MFA), and wireless configurations are insecure, with SSID broadcasting and no WPA3 enforcement. Critical systems are hosted on a single server, creating a single point of failure. Backups are unencrypted and external, increasing ransomware risk, while the absence of Role-Based Access Control (RBAC), SIEM, and a formal incident response plan leaves the organization unprepared to detect or respond to threats.

# Security Architecture Goals

The security architecture must support long-term goals by protecting data, ensuring operational continuity, and maintaining customer trust. As an e-commerce platform, securing payment and customer data is critical. The network must be scalable, resilient, and allow secure remote access. Compliance with NIST SP 800-53, PIPEDA, and PCI DSS drives the need for strong access controls, encryption, and continuous monitoring to balance regulatory demands with risk mitigation.

As the business expands, the security framework must adapt. Growth will introduce new network segments, cloud services, and third-party integrations, requiring a Zero Trust approach. Enhancing IAM, endpoint protection, and cloud security will support secure onboarding. A SIEM solution and incident response plan will improve real-time threat detection and response, reinforcing the company’s resilience and regulatory posture.

# Security Architecture Recommendations

- Network Security
    - Implementation Network Segmentation
        - Separate critical systems using VLANs to isolate sensitive data and functions. Use multiple VLANs to limit lateral movement in the event of a breach.
    - Deploy of Firewall & IDPS (Intrusion Detection & Prevention System)
        - Installing an up to date firewall, both physical or software
        - Using an IDPS at key network entry points, with a high importance on the Private Payment Network tied to 76.71.105/28
    - Enable Secure Remote Access
        - VPN (Virtual Private Network) with MFA (Multi-Factor Authentication)
        - Enforcement of a strict access control for employees working remotely
    - Review & Harden Wireless Security
        - Moving over to a model like WPA3 encryption and disabling SSID Broadcasting where unnecessary
        - Restriction to domain-registered devices where allowed
        - Restriction Guest Wireless segmentation
    - Apply DHCP Snooping and Port Security
        - Preventing rogue DHCP server and unauthorized devices from joining the network
          *NIST SP 800-53 CM-7, AC-3 ,AC-4, AC-17, AC-18,  SC-7, SC-7(12), SC-12/13,  SI-4, IA-2, PIPEDA - Principle 7,  PCI DSS v.4 - 1.5.1,  PCI DSS 4.0 MFA*
- Data Security
    - Implement Strong Encryption
        - Encrypt sensitive data at rest and in transit using AES-256 and TLS 1.2/1.3
    - Secure Backups
        - Switching over to a regular encryption rotation of backups
        - Offline storage to protect against ransomware
    - Enforce Data Loss Prevention (DLP)
        - Monitor and restrict unauthorized data transfer to prevent accidental or malicious data leak
          *NIST SP 800-53 SC-7, SC-12, SC-13, SC-17, SC-28, AC-21, SI-4, CP-9, PCI DSS v4.0 - Backup Media, PIPEDA - Principle 7*

- Endpoint Security
    - Deploy Endpoint Detection & response (EDR)
        - Implement EDR Solution on all employee devices to detect & respond to threat in real-time

  - Enforce Patch Management
    - Automate security update to eliminate vulnerabilities in operating systems & application
  - Apply Device Hardening Policies
    - Restrict USB Access - Limit to Encrypted USB issued only
    - Disable unnecessary services
    - Enforce security configuration on all endpoints
      *NIST SP 800-53 SI-2, SI-4, AU-6, AC-19, CM-2, CM-6, CM-7, MP-7, PCI DSS v4 Protect Stored Account Data, PIPEDA - Principle 7*
- IAM - Identity and Access Management
  - Implement Multi-Factor Authentication (MFA)
    - MFA on all account, with a focus on privileged and remote access
  - Adopt Role-Based Access Controls (RBAC)
    - Only allowing employees to have access to the systems necessary for the job
  - Monitor & Audit user access
    - Regular review of access logs
    - Enforce Least privilege principles to minimize insider threats
      *NIST SP 800-53 IA-2, AC-2, AC-3, AC-6, AU-2, AU-6, PCI DSS v4 MFA Requirements*
- Cloud Security
  - Secure Cloud Storage & Services
    - Encryption, Access Controls, and Logging for all Cloud-Hosted Application
  - Enable Continuous Monitoring
    - Cloud security posture management (CSPM) tools to detect misconfiguration and vulnerabilities
  - Enforce Strong API Security
    - Restrict access to cloud APIs and monitor interactions for potential security risk
      *NIST SP 800-53 SC-12, SC-13, SC-17, SC-31, SI-4, CA-7, AC-3, AC-10, AC-17, AC-19, PCI DSS v4 Requirements Overview*
- Incident Response
  - Develop a formal incident response plan (IRP)
    - Having a structured plan detailing response actions for different types of cyber incidents
  - Implement Security Information and Event Management (SIEM) & Security Logging
    - Deploying SIEM - Security Information & event Management system for centralized monitoring and real-time threat detection
  - Conduct Regular Incident Response Drills
    - Test the response of the procedures through simulated cyberattacks
      *NIST SP 800-53 section 3.8 (IR-1 to IR-8), NIST CSF Incident Response,*
- Physical Security
  - Restrict Physical Access to Critical Systems
    - Secure server room with keycard access and surveillance monitoring
  - Implement Asset Tracking
    - Maintain an inventory of all hardware and track devices that stores or process sensitive information
      *NIST SP 800-53 Section 3.11 (PE-2), CM-8, NIST CSF - Protect, PIPEDA - Principle 7*
- Training Employees on Security Awareness
  - Continuous employee training on social engineering tactics
  - Physical security best practices
    NIST SP 800-53 AT-2, NIST CSF Awareness and Training (PR.AT),

# Implementation Strategy

## Phase One: Immediate Action - Critical Security Enhancements

- Timeline:Immediate to 3 months
- Network Security Enhancement
  - Deploy firewall & IDPS to monitor and filter external traffic
    - Monitor the external private payment services under 76.71.1.105/28
  - Implement Network Segmentation to isolate critical system - VLAN Separation
  - Secure Wi-Fi by enforcing WPA3 encryption and restricting access to domain-registered devices
- Identity & Access Management (IAM) Improvements
  - Implement Multi-Factor Authentication (MFA) for all critical systems
  - Begin Role-Based Access Control (RBAC) implementation, restricting access based on job functions
- Endpoint & Data Security Measures
  - Deploy Endpoint Detection & Response (EDR) on all employee devices
  - Enforce automatic patch management for operating systems and applications
  - Begin encryption of sensitive data at rest and in transit
- Resource Requirements:
  - Personnel: IT Security Team, Network Administrators
  - Technology Updates: Firewalls, IDPS, EDR and Encrytion Tools
  - Budget Consideration: Firewall Purchase and Upgrades, licensing for security solutions

## Phase Two: Intermediate Security Controls - Strengthen Defenses

- Timeline: 3 months to 6 months
- Incident Response & Threat Monitoring
  - Deploy a **Security Information & Event Management (SIEM)** system for centralized logging and anomaly detection.
  - Establish a **formal incident response plan**, including escalation procedures and forensic capabilities.
  - Conduct **security awareness training** for employees on phishing and social engineering threats.
- Data Security & Backup Strategy
  - Implement **Data Loss Prevention (DLP)** to prevent unauthorized data transfers.
  - Secure **cloud storage and applications** with encryption and access monitoring.
  - Implement **encrypted, offsite, and immutable backups** to protect against ransomware.
- Resource Requirements
  - **Personnel:** IT Security Team, Compliance Officers
  - **Technology:** SIEM solution, DLP software, cloud security monitoring tools
  - **Budget Considerations:** SIEM setup, cybersecurity awareness training programs

## Phase Three: Long-Term Security Maturity - Sustainable Security Framework

- Timeline: 6 months to 12 months
- Zero Trust Implementation
  - Strengthen **Identity & Access Management (IAM)** with continuous authentication and behavioral analytics.
  - Implement **least privilege access** and enforce **regular access reviews**.
- Advanced Cloud Security & Compliance Alignment
  - Continuously monitor **cloud security posture (CSPM)** to detect misconfigurations.

    - Conduct regular **compliance audits** to ensure adherence to **PCI DSS, NIST SP 800-53, and PIPEDA**.
- Ongoing Security Operation & Testing
    - Regular **penetration testing and vulnerability assessments** to proactively identify weaknesses.
    - Conduct **incident response drills** and tabletop exercises to test preparedness.
- Resource Requirements
    - **Personnel:** Security Analysts, Compliance Auditors, DevOps Team
    - **Technology:** Behavioral analytics, Zero Trust security tools, continuous monitoring solutions
    - **Budget Considerations:** Annual security audits, security team expansion, continuous education programs

# Conclusion

The security assessment identified critical vulnerabilities that pose a significant risk to the organization's infrastructure, data integrity, and overall operational security. Key findings include lack of network segmentation, absence of robust endpoint security, inadequate authentication controls, and a single point of failure in hosting critical systems. Additionally, the absence of a firewall on external connections and weak access controls leave sensitive assets exposed to potential breaches. Without these safeguards, the business remains highly vulnerable to cyber threats, unauthorized access, and compliance violations.

To mitigate these risks, a structured security implementation plan has been proposed, following a phased approach aligned with NIST SP 800-53 and the NIST Cybersecurity Framework. Immediate actions focus on network segmentation, endpoint protection, and identity access management enhancements, ensuring that foundational security measures are in place. Mid-term initiatives introduce centralized monitoring, incident response planning, and data encryption, enhancing detection and response capabilities. Finally, long-term strategies such as Zero Trust security, cloud security posture management, and continuous compliance assessments will ensure the security architecture remains resilient and scalable.

By implementing these critical security controls, the organization will strengthen its defenses against cyber threats, ensure compliance with industry standards (PCI DSS, PIPEDA, NIST), and support future growth with a secure, adaptable architecture. Prioritizing cybersecurity not only protects sensitive customer and business data but also fortifies trust, operational stability, and business continuity in an increasingly threat-prone digital landscape.

# Citations

## NIST Citations

JOINT TASK FORCE, Ross, W. L., Jr., & Copan, W. (2020). *NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for information systems and organizations*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In *NIST CSWP 29* [Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.-b). *Incident Response | CSRC | CSRC*. https://csrc.nist.gov/projects/incident-response

## PCI DSS v4 Citations:

PCI Compliance Hub. (2024, April 19). PCI DSS 4.0: New Multi-Factor Authentication (MFA) Requirements - PCI Compliance Hub. *PCI Compliance Hub* -. https://pcicompliancehub.com/pci-dss-4-0-new-multi-factor-authentication-mfa-requirements/

PCI Compliance Hub. (2024c, March 11). PCI DSS v4 Requirement 3: Protect Stored Account Data. *PCI Compliance Hub* -. https://pcicompliancehub.com/pci-dss-v4-requirement-3-protect-stored-account-data/

*Official PCI Security Standards Council site - Verify PCI compliance, download data security and credit card security standards*. (n.d.). https://east.pcisecuritystandards.org/document_library

PCI Compliance Hub. (2024a, February 7). The 12 requirements of PCI DSS V4.0 explained. - PCI Compliance Hub. *PCI Compliance Hub* -. https://pcicompliancehub.com/the-12-requirements-of-pci-dss-v4-0-explained/

Baykara, S. (2023, October 9). *What are PCI DSS Backup Requirements*. PCI DSS GUIDE. https://pcidssguide.com/what-are-pci-dss-backup-requirements/

## PIPEDA - Personal Information Protection and Electronic Document Act

Office of the Privacy Commissioner of Canada. (2021, August 13). *PIPEDA Fair Information Principle 7 – Safeguards*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/

## MITRE Citations

*Lateral movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®*. (n.d.). https://attack.mitre.org/tactics/TA0008/

*Authorization Enforcement, Mitigation M0800 - ICS | MITRE ATT&CK®*. (n.d.). https://attack.mitre.org/mitigations/M0800/

Darrington, J. (2025, February 14). *Using MITRE ATT&CK for incident response playbooks*. Graylog. https://graylog.org/post/using-mitre-attck-for-incident-response-playbooks