Project 2

Edison Maniwang

University of Maryland Global Campus

CSIA 485 Cyber Management and Policy Capstone

Professor Holly Ridgeway

April 22nd, 2025

Introduction

Purpose

This Cybersecurity Implementation Plan outlines the necessary steps to establish a secure, resilient, and compliant information technology (IT) infrastructure for Padgett-Beale Financial Services (PBI-FS), a wholly owned subsidiary of Padgett-Beale, Inc. Following the acquisition of Island Banking Services, PBI-FS is tasked with maintaining critical customer-facing operations — including a call center and transaction processing center — on the island while operating under the jurisdiction of U.S. banking laws and regulations.

The primary purpose of this plan is to translate the cybersecurity strategy developed during the initial merger and acquisition (M&A) phase into a detailed, actionable roadmap that will guide the secure setup and operation of PBI-FS. This plan provides a high-level structure for implementing security controls, upgrading legacy infrastructure, reducing risk exposure, and enabling compliance with legal and regulatory requirements, including the Bank Secrecy Act (BSA) and related federal regulations.

The implementation plan incorporates recognized best practices from:

- The NIST Cybersecurity Framework (CSF) for risk-based cybersecurity management,
- NIST Special Publication 800-53 for security and privacy controls,
- CIS Controls Version 8.1 for practical safeguards against common cyber threats, and
- ISO/IEC 27001/27002 standards for establishing and maintaining an Information Security Management System (ISMS).

The goal is to build an information security program that protects the confidentiality, integrity, availability, non-repudiation, authentication, auditability, and accountability of PBI-FS's systems and data.

This plan acknowledges the unique risks faced by PBI-FS due to inherited IT assets of questionable integrity, the relocation to new facilities, and the necessity of maintaining operations during the transition.

It emphasizes a risk-based, phased implementation approach aligned with the System Development Life Cycle (SDLC) and leverages cybersecurity principles to ensure operational continuity, customer trust, and regulatory compliance.

The successful execution of this plan will lay the foundation for a secure and sustainable operating environment, enabling PBI-FS to serve its customers reliably while protecting its digital and financial assets from internal and external threats.

Goals and Objectives

Business Goals and Objectives

Padgett-Beale Financial Services (PBI-FS) was established to support Padgett-Beale, Inc.'s strategic expansion into the financial services sector following the acquisition of Island Banking Services. The business goals for PBI-FS center on building a secure, compliant, and operationally resilient financial services subsidiary. A primary objective is ensuring full regulatory compliance with applicable U.S. financial regulations, particularly the Bank Secrecy Act (BSA) and anti-money laundering (AML) requirements, by implementing cybersecurity controls aligned with recognized standards such as the NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27001:2022 (International Organization for Standardization, 2022). Operational continuity is another critical goal, with the organization seeking to quickly re-establish and maintain secure call center and transaction processing operations to minimize disruptions for customers.

Risk isolation is a central focus, with cybersecurity measures specifically designed to segregate PBI-FS's infrastructure and operations from Padgett-Beale's broader corporate environment to contain potential threats (Padgett-Beale M&A Profile, 2020). Furthermore, the company aims to rebuild trust with customers, regulators, and business partners by demonstrating a robust commitment to cybersecurity, including the pursuit of third-party validations such as ISO/IEC 27001 certification. Finally, strategic growth enablement is a long-term objective, with PBI-FS investing in scalable and modular IT infrastructure capable of supporting future financial services expansion while maintaining strong cybersecurity and risk management practices.

Project Goals and Objectives

The cybersecurity implementation project is designed to operationalize these business goals by delivering a secure, compliant, and resilient IT environment for PBI-FS. A critical objective is to decommission and replace compromised hardware, software, and network components inherited from

Island Banking Services, ensuring the deployment of trusted, securely configured infrastructure (Padgett-Beale M&A Profile, 2020). The project will implement mandatory and compensatory security controls based on NIST Cybersecurity Framework guidelines (NIST, 2018), NIST SP 800-53 security controls (NIST, 2020), CIS Controls Version 8.1 (Tripwire, 2025), and ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards (International Organization for Standardization, 2022).

The project also focuses on comprehensive threat risk reduction through the deployment of layered cybersecurity defenses designed to detect, prevent, and respond to insider and external threats, such as ransomware and phishing attacks. System interoperability is another project priority, with secure integration across platforms and networks achieved by adhering to interoperability standards set by the Federal Communications Commission (FCC, 2025). The implementation effort will be managed through a disciplined application of the System Development Life Cycle (SDLC), following a phased approach consistent with the Vee Life Cycle Model to reduce project risk and ensure quality outcomes (SEBoK, 2023).

Additionally, the project will establish mandatory security awareness and training programs to reduce human-related risks, aligning with the best practices recommended by CIS Controls (Tripwire, 2025). Finally, audit and compliance readiness will be built into the IT environment from the outset, with security monitoring, logging, and reporting mechanisms established to facilitate internal governance, regulatory compliance, and readiness for independent audits. Continuous improvement processes will be incorporated to ensure that cybersecurity operations evolve in response to emerging threats and changing business requirements (NIST, 2018).

Scope

Scope Definition

The cybersecurity implementation project encompasses all information technology (IT) assets, systems, operations, and personnel involved in the re-establishment and secure operation of Padgett-Beale Financial Services (PBI-FS) on the island. Specifically, the scope includes the protection of call center operations, covering hardware, software, network infrastructure, and telecommunications systems supporting customer interactions and financial services. It also includes transaction processing systems that handle customer financial data, secure payment gateways, and reconciliation platforms.

The project will design and deploy a segmented network architecture incorporating firewalls, virtual private networks (VPNs), intrusion detection and prevention systems (IDS/IPS), and secure wireless access. Data centers and local servers will be rebuilt or replaced to ensure secure data storage, processing, and backup in compliance with relevant data protection laws. Physical security measures, including access control systems and secure server rooms, will be integrated with cybersecurity defenses. Personnel security is within scope, focusing on the enforcement of cybersecurity policies and the delivery of security training to employees, contractors, and third-party service providers. Finally, the project includes the implementation of security logging, monitoring, auditing, and reporting capabilities to enable compliance with regulatory frameworks such as the Bank Secrecy Act (BSA).

The cybersecurity activities undertaken will be governed by best practices and standards, including the NIST Cybersecurity Framework (NIST, 2018), NIST SP 800-53 controls (NIST, 2020), ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (International Organization for Standardization, 2022), and CIS Controls Version 8.1 (Tripwire, 2025).

Items Beyond Scope

The cybersecurity implementation project will not extend to several specific areas. Information systems, networks, and cybersecurity operations supporting Padgett-Beale, Inc.’s mainland corporate

offices are excluded. Additionally, legacy systems and data from Island Banking Services that were seized and subsequently returned by authorities are not within the immediate scope; these assets will require future evaluation and re-certification before potential reintegration.

Third-party vendor-operated networks, such as those maintained by cloud service providers and payment processors, are also outside the scope of direct implementation activities, although integration points with these systems will be secured. Finally, customer-owned devices that connect to PBI-FS systems remotely (e.g., personal computers, smartphones) will not be secured directly by PBI-FS. Instead, communication channels with customers will be safeguarded through secure portals, encryption protocols, and strong authentication measures.

Assumptions

The cybersecurity implementation plan for Padgett-Beale Financial Services (PBI-FS) is based on several key assumptions regarding project conditions, resource availability, and external factors. It is assumed that sufficient budgetary resources will be allocated to procure necessary hardware, software, security appliances, and professional services to support the rebuild and security hardening efforts. Additionally, it is assumed that qualified cybersecurity personnel, including internal IT staff, external contractors, and specialized consultants, will be available to support the planning, deployment, and maintenance phases of the project. Coordination with Padgett-Beale, Inc.'s corporate IT leadership is assumed to be ongoing to ensure architectural compatibility where integration is necessary, even though PBI-FS will operate with segregated systems.

The project further assumes that all legacy IT assets inherited from Island Banking Services that were compromised or involved in the prior criminal investigations will either be securely decommissioned or subjected to thorough forensic examination before any potential reuse. It is also assumed that key regulatory bodies, including U.S. financial oversight agencies, will accept the use of industry-standard frameworks such as the NIST Cybersecurity Framework (NIST, 2018), NIST SP 800-53 controls (NIST, 2020), and ISO/IEC 27001:2022 standards (International Organization for Standardization, 2022) as the foundation for compliance and reporting efforts.

External vendors providing mission-critical services, including cloud hosting providers, telecommunications companies, and payment processors, are assumed to maintain security practices consistent with industry standards and to cooperate with PBI-FS during integration testing and security audits. Furthermore, it is assumed that necessary licenses, permits, and regulatory approvals for new IT infrastructure deployment on the island will be obtained without significant delays. Finally, the project assumes that all employees, contractors, and service providers will adhere to the security policies and undergo mandatory security awareness training prior to being granted access to PBI-FS systems.

Constraints

Project Constraints

The cybersecurity implementation project for Padgett-Beale Financial Services (PBI-FS) operates under several significant project constraints. First, financial limitations must be carefully managed. Although funding has been allocated for rebuilding secure operations, the overall project budget imposes restrictions on the acquisition of cybersecurity technologies, professional services, and staffing, requiring strategic prioritization of security investments. Time constraints are also critical, as PBI-FS must rapidly reestablish secure operations to meet regulatory requirements and customer expectations. The compressed timeline necessitates concurrent execution of infrastructure upgrades, control implementation, and compliance documentation, increasing the complexity of project coordination.

Technological constraints also pose challenges. Legacy systems inherited from Island Banking Services are outdated and may be compromised, necessitating full replacement or thorough forensic analysis, which may delay progress. Personnel constraints further complicate implementation, as there is limited availability of cybersecurity professionals skilled in financial services security standards such as NIST SP 800-53 (NIST, 2020) and ISO/IEC 27001:2022 (International Organization for Standardization, 2022). Competition for qualified experts may increase project staffing costs and extend recruitment timelines. Finally, external dependencies on telecommunications providers, cloud services, and third-party vendors introduce coordination constraints that are outside PBI-FS's direct control.

Barriers to Success

Several barriers to success could impact the effective execution of the cybersecurity implementation plan. One major barrier is vendor interoperability challenges. While external service providers are expected to meet cybersecurity best practices, inconsistencies in security controls or delayed vendor responses could introduce vulnerabilities or project delays (Federal Communications Commission, 2025). Another barrier is regulatory complexity. Financial services cybersecurity is governed by multiple

overlapping regulations, and failure to achieve or demonstrate compliance could result in legal penalties or reputational harm.

Employee resistance to change poses an additional barrier, as effective cybersecurity implementation requires not only technical controls but also changes to organizational culture, behavior, and awareness. Without strong leadership support and robust training programs, end-user noncompliance could undermine security initiatives. The risk of residual vulnerabilities in legacy environments also remains a concern, as systems once compromised may retain hidden threats even after remediation efforts. Finally, unexpected external threats, such as emerging cyberattack techniques, advanced persistent threats (APTs), or regional disruptions (e.g., natural disasters affecting the island), could further complicate or delay project objectives.

To overcome these barriers, the project will adopt a risk-based, phased approach, maintain continuous stakeholder engagement, and integrate cybersecurity governance with operational resilience planning as recommended by NIST (2018) and ISO/IEC 27002:2022 (International Organization for Standardization, 2022).

Project Management Plan

People

The cybersecurity implementation project for Padgett-Beale Financial Services (PBI-FS) will be overseen by a dedicated project management team reporting to the Chief Information Security Officer (CISO) and the executive leadership of PBI-FS. Key personnel will include a Project Manager, Cybersecurity Architect, IT Infrastructure Lead, Compliance Officer, and supporting cybersecurity analysts and system administrators. Where necessary, external contractors specializing in network engineering, cybersecurity architecture, and financial regulatory compliance will be engaged to supplement internal capabilities. Clear roles and responsibilities will be established through a Responsibility Assignment Matrix (RAM), ensuring accountability at each stage of the project. All project participants will be required to adhere to PBI-FS's cybersecurity policies and undergo project-specific security awareness training.

Processes

The project will be managed using a structured, phased approach following the System Development Life Cycle (SDLC), specifically the Vee Life Cycle Model as recommended for complex, high-risk implementations (SEBoK, 2023). Project phases will include detailed planning, requirements analysis, system design, development, testing, deployment, and maintenance. Each phase will incorporate milestone reviews, formal risk assessments, and decision gates to ensure that progress aligns with cybersecurity requirements, regulatory compliance obligations, and project objectives. Risk management processes will be integrated throughout the project lifecycle, with proactive identification, mitigation, and escalation of risks to appropriate stakeholders. Project performance will be tracked using key performance indicators (KPIs) tied to specific deliverables, such as secure system deployments, implementation of mandatory controls, and successful audit outcomes.

Technologies

The cybersecurity implementation will leverage a comprehensive suite of technologies selected based on industry best practices and regulatory requirements. Core technologies will include next-generation firewalls, endpoint detection and response (EDR) platforms, Security Information and Event Management (SIEM) systems, multi-factor authentication (MFA), encrypted communications, and secure configuration management tools. Technology selection will prioritize solutions that align with the NIST Cybersecurity Framework (NIST, 2018), NIST SP 800-53 controls (NIST, 2020), ISO/IEC 27001:2022 standards (International Organization for Standardization, 2022), and CIS Controls Version 8.1 (Tripwire, 2025). Interoperability standards, as defined by the Federal Communications Commission (FCC, 2025), will guide integration efforts to ensure secure data exchange between systems and third-party services. Vendor evaluations will consider cybersecurity certifications, interoperability capabilities, and support for secure cloud and on-premises environments.

Strategy Implementation

The Strategy Implementation section provides a comprehensive roadmap for operationalizing the cybersecurity strategy developed for Padgett-Beale Financial Services (PBI-FS). This roadmap outlines the selection and deployment of security controls, the application of a structured System Development Life Cycle (SDLC), milestone tracking to ensure project progress, and resource requirements necessary for successful implementation. Each component of the strategy is designed to build a secure, compliant, and resilient IT environment aligned with recognized cybersecurity standards. The implementation approach integrates best practices in cybersecurity governance, technical execution, and continuous improvement to support the long-term success of PBI-FS operations.

Security Controls

A robust security controls framework is essential to safeguarding Padgett-Beale Financial Services (PBI-FS) against evolving cybersecurity threats while ensuring compliance with financial industry regulations. The security controls implementation will follow a defense-in-depth strategy, combining baseline mandatory controls with layered compensatory controls to address specific risks. Controls are selected and prioritized based on recognized cybersecurity frameworks and standards. Together, these controls will establish a secure operational foundation, mitigate threats to critical systems, and promote resilience in the face of both internal and external cyber risks.

Baseline (Mandatory Controls)

The cybersecurity implementation for Padgett-Beale Financial Services (PBI-FS) will establish a mandatory baseline of security controls to meet regulatory requirements and defend against common threats. Baseline mandatory controls will include the deployment of firewalls and intrusion detection/prevention systems (IDS/IPS), the implementation of multi-factor authentication (MFA) for all privileged accounts, encryption of sensitive data at rest and in transit, centralized logging and monitoring through a Security Information and Event Management (SIEM) system, endpoint detection and response

(EDR) solutions on all systems, and strong access controls utilizing least privilege and role-based access models.

These mandatory controls are designed to establish a foundational level of security necessary for compliance with the Bank Secrecy Act (BSA) and to reduce the organization's overall risk posture. Deployment of these controls will be prioritized early in the project to ensure a secure environment during the rebuild of operational capabilities.

Compensatory Controls (Administrative, Operational, Tactical)

To address gaps where baseline controls may not fully mitigate identified risks, PBI-FS will implement layered compensatory controls across administrative, operational, and tactical domains. Administrative controls will include comprehensive cybersecurity policies, employee security awareness training programs, and mandatory acceptable use agreements for all system users. Operational controls will encompass physical security measures such as badge access to secure areas, visitor management systems, and surveillance monitoring, along with operational processes for incident response and disaster recovery. Tactical controls will include secure software development practices for internally developed applications, proactive threat hunting initiatives, and continuous vulnerability scanning and patch management.

Where interoperability with third-party systems is required, compensatory measures such as contractual cybersecurity obligations and security questionnaires will ensure alignment with organizational security standards (Federal Communications Commission, 2025). The combination of mandatory and compensatory controls will establish a multi-layered defense-in-depth architecture that mitigates both internal and external threats effectively.

System Development Life Cycle/Schedule

The cybersecurity implementation project will adhere to a structured System Development Life Cycle (SDLC) based on the Vee Life Cycle Model (SEBoK, 2023) and the seven standard phases:

planning, requirements, design, development, testing, deployment, and maintenance. Each phase will follow cybersecurity best practices and integrate security from the earliest stages.

- **Planning Phase:** Define the project scope, objectives, high-level security requirements, risk appetite, and resource needs. Initial risk assessments and regulatory compliance mapping will be conducted (NIST, 2018).
- **Requirements Phase:** Gather detailed business, technical, and cybersecurity requirements, ensuring traceability to regulatory obligations and standards such as ISO/IEC 27001 (International Organization for Standardization, 2022).
- **Design Phase:** Architect the network, systems, applications, and security controls, ensuring defense-in-depth principles and secure-by-design approaches are incorporated.
- **Development Phase:** Implement network infrastructure, systems, and security tools according to the design specifications, maintaining secure coding standards and configuration management practices.
- **Testing Phase:** Conduct rigorous security testing, including vulnerability scanning, penetration testing, interoperability testing, and compliance audits to validate system security and functionality (NIST, 2020).
- **Deployment Phase:** Transition tested systems into production environments, ensuring secure onboarding of users and activation of continuous monitoring solutions.
- **Maintenance Phase:** Sustain security operations through ongoing vulnerability management, incident response, patch management, and periodic reassessments to adapt to evolving threats.

The SDLC will be integrated with the project's milestones and resource allocation schedules to ensure coordinated execution and early identification of security gaps.

Milestones

The project will use milestone-based tracking to measure progress and maintain accountability throughout the implementation phases. Key milestones include:

- Completion of initial risk assessment and requirements documentation
- Acquisition and deployment of baseline security technologies (firewalls, SIEM, EDR)
- Full decommissioning and secure disposal of legacy Island Banking Services infrastructure
- Completion of secure network and systems design documentation
- Successful testing and validation of security controls in staging environments
- Launch of call center operations under new secured infrastructure
- Completion of staff cybersecurity training programs
- Internal audit confirming alignment with NIST CSF, ISO/IEC 27001, and BSA compliance
- Readiness for external compliance audit and potential ISO/IEC 27001 certification assessment

Milestones will be reviewed during scheduled project status meetings and serve as formal decision points for advancing to subsequent SDLC phases.

Resource Requirements (People, Finances)

Successful execution of the cybersecurity implementation project will require a combination of internal staffing, external consulting, technology investments, and operational budget allocations. The following estimates reflect anticipated resource needs based on current industry salary surveys and cybersecurity product pricing data.

Personnel Costs

Staffing requirements include the recruitment or contracting of specialized roles. The average salary for a Cybersecurity Architect in the United States is approximately $150,816 per year (Glassdoor, 2025). Two Security Analysts are anticipated, each earning an average annual salary of $112,750 (Glassdoor, 2025), totaling approximately $225,500. A Network Engineer contracted for six months is estimated to cost approximately $65,000 based on industry averages. A part-time Compliance Officer, internally reallocated, is budgeted at $50,000. A Training Specialist contracted for three months is estimated at $30,000. Overall, personnel costs are projected to be approximately **$521,316** for the initial implementation period.

Technology Acquisition Costs

Technology acquisition will require investments across core cybersecurity domains. Hardware costs for Next-Generation Firewalls (NGFWs) suitable for a mid-sized enterprise range from $1,500 to $4,000 depending on model and capabilities (Fortinet, 2025). An Endpoint Detection and Response (EDR) solution, such as CrowdStrike Falcon, is priced starting at $59.99 per device annually, translating to approximately $6,000 for 100 endpoints (CrowdStrike, 2025). Security Information and Event Management (SIEM) solutions typically cost between $60,000 and $120,000 annually for managed services, depending on data volume and features (UnderDefense, 2025). A Multi-Factor Authentication (MFA) solution is estimated at $20,000 for licensing and deployment. Secure email gateways and anti-phishing tools are projected to cost $15,000 annually. Server and storage hardware refresh projects are estimated at $120,000, while secure configuration management and patch management toolsets are estimated at $25,000. Encrypted backup and disaster recovery solutions are projected at $35,000. The total initial technology acquisition cost is therefore estimated at approximately **$370,000**, with ongoing maintenance and licensing costs of approximately **$150,000 annually**.

Additional Project Costs

Other key project expenses include professional services for penetration testing and third-party risk assessments, budgeted at $50,000, and regulatory compliance consulting services estimated at $40,000. Cybersecurity awareness training programs for approximately 200 employees are projected to cost $7,728 annually, assuming a mid-range pricing model of $3.22 per user per month (CanIPhish, 2025). A contingency fund representing approximately 10% of total project costs, estimated at $100,000, will be reserved for addressing unforeseen issues or emergent risks.

Overall Budget summary

Including personnel, technology, external services, training, and contingency reserves, the total projected first-year budget for the cybersecurity implementation project is approximately **$1.09 million**. Ongoing annual operational costs, including licensing renewals, security audits, incident response readiness, and training refresh programs, are projected to fall between **$300,000 and $400,000 per year** to maintain a compliant and resilient cybersecurity posture.

Enterprise IT Architecture (“To-Be” State)

The future-state ("To-Be") enterprise IT architecture for Padgett-Beale Financial Services (PBI-FS) will be designed to support secure, scalable, and compliant financial service operations. The architecture will incorporate a defense-in-depth approach, layering cybersecurity controls across the network, server infrastructure, endpoint devices, and cloud services to protect the confidentiality, integrity, and availability of data. The core elements of the "To-Be" architecture include the following:

Hardware Infrastructure

The hardware environment will consist of new enterprise-grade equipment to ensure system performance, scalability, and security. A secured on-premises data center will be established, housing redundant servers with hardware-based encryption modules, network storage appliances, and backup power solutions. Next-generation firewalls (NGFWs) will protect the network perimeter, while internal network segmentation will be enforced using VLANs and layer-3 switching to separate sensitive systems from general operations.

Workstations for call center and administrative staff will be equipped with trusted platform modules (TPMs) for hardware-based security and will run current, patched operating systems. Mobile device management (MDM) policies will be applied to all authorized mobile endpoints to ensure consistent enforcement of security configurations.

Software Environment

The software stack will include an updated enterprise productivity suite, secure customer relationship management (CRM) systems, and financial transaction processing applications. Operating systems for servers will primarily consist of hardened Microsoft Windows Server installations, while user endpoints will run Windows 11 Enterprise with device guard features enabled.

Critical security applications will include endpoint detection and response (EDR) platforms, multi-factor authentication (MFA) systems, email security gateways, and vulnerability management solutions. Centralized log management and a Security Information and Event Management (SIEM) solution will monitor network activity, support incident detection, and generate audit logs for compliance reporting.

Network Infrastructure

The network design will emphasize resilience, scalability, and segmentation. A dual-firewall DMZ architecture will host externally accessible services such as customer web portals, VPN gateways, and email servers. Internal network zones will segregate call center operations, administrative systems, data storage, and management interfaces, reducing the potential blast radius of security incidents.

Virtual Private Network (VPN) access will be required for all remote users, with enforced MFA and network access controls. Intrusion Detection and Prevention Systems (IDPS) will monitor both perimeter and internal traffic to detect anomalous or malicious activity. Wireless access points deployed within the facilities will utilize WPA3 encryption standards, and guest network traffic will be logically separated from internal operations.

Cybersecurity Defenses

Cybersecurity defenses will integrate prevention, detection, and response capabilities. Next-generation firewalls will filter incoming and outgoing traffic based on contextual awareness. Endpoint security platforms will provide real-time threat detection, behavioral analysis, and automated containment of malware or unauthorized activity.

SIEM systems will aggregate logs from endpoints, firewalls, servers, and applications, using correlation rules to detect indicators of compromise (IOCs) and trigger automated responses. Incident response plans will define escalation paths and response procedures for cybersecurity events. Data Loss

Prevention (DLP) tools will be implemented to monitor and prevent unauthorized transmission of sensitive financial or personally identifiable information (PII).

Encryption of data at rest and in transit will be mandatory across all systems handling sensitive information. Role-based access control (RBAC) and least privilege principles will govern all user and administrator access rights.

Overview Diagram

The image below provides a detailed overview of the target ("To-Be") enterprise IT architecture for Padgett-Beale Financial Services (PBI-FS), illustrating how the organization will structure its network, systems, and defenses to support secure and compliant operations:

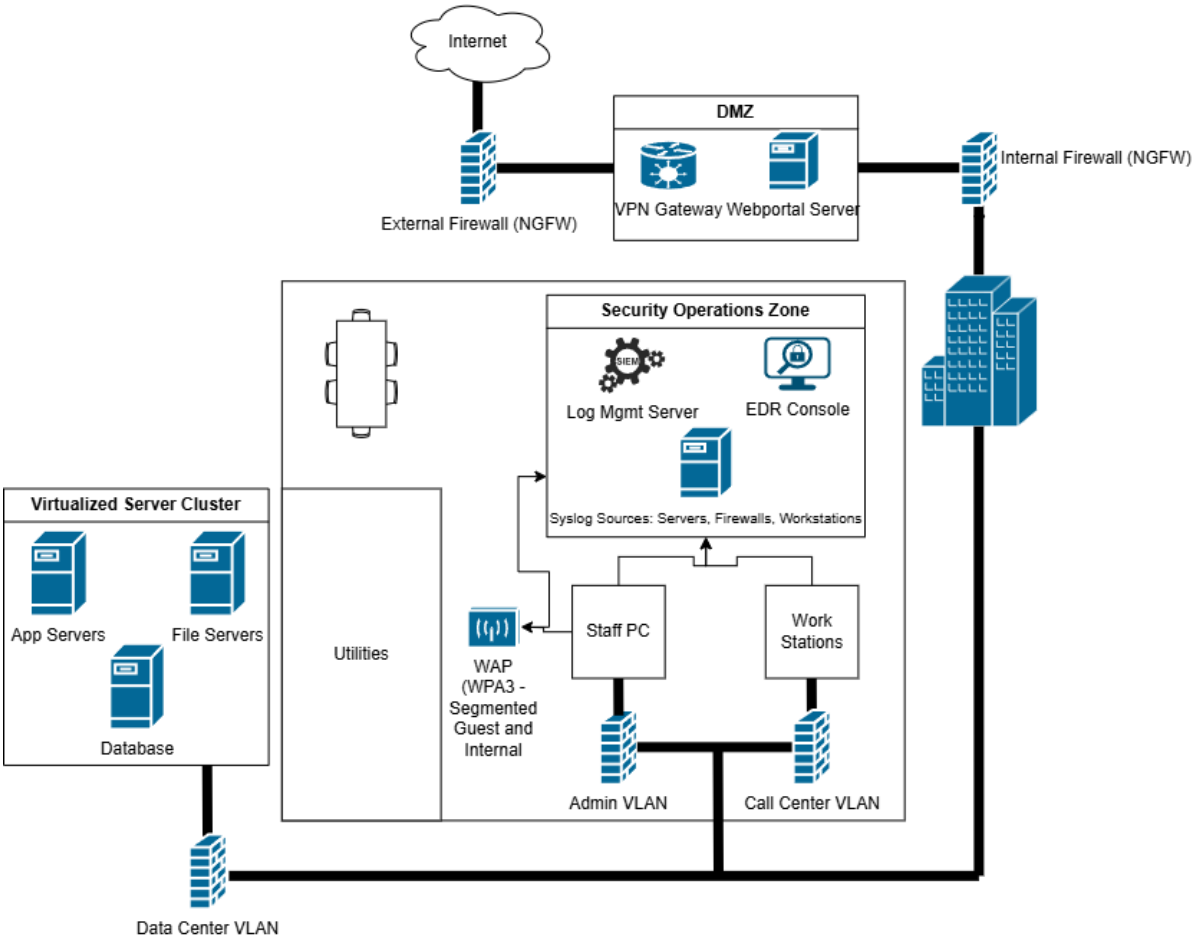

Figure 1. Island Banking Services IT Infrastructure (To-Be)

References

CanIPhish. (2025). *Security awareness training price guide for 2025*. https://caniphish.com/blog/how-much-does-security-awareness-training-cost

CrowdStrike. (2025). *Endpoint, cloud & identity protection products*. https://www.crowdstrike.com/en-us/products/

Federal Communications Commission. (2025). *Interoperability*. https://www.fcc.gov/general/interoperability

Fortinet. (2025). *Network firewall price: Comparing security costs*. https://www.fortinet.com/products/network-firewall-pricing

Glassdoor. (2025). *Cyber security architect salary*. https://www.glassdoor.com/Salaries/cyber-security-architect-salary-SRCH_KO0,24.htm

Glassdoor. (2025). *Security analyst salary*. https://www.glassdoor.com/Salaries/security-analyst-salary-SRCH_KO0,16.htm

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022). ISO.

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002:2022). ISO.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, Version 1.1* (NIST CSWP 04162018). https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

Padgett-Beale M&A Profile. (2020). *CSIA 485 merger and acquisition profile.* University of Maryland Global Campus.

SEBoK. (2023). *Vee life cycle model*. https://www.sebokwiki.org/wiki/Vee_Life_Cycle_Model

Tripwire. (2025). *CIS Controls Version 8.1: What you need to know*. https://www.tripwire.com/state-of-security/security-data-protection/cis-controls-version-8-1-what-you-need-to-know/

UnderDefense. (2025). *Managed SIEM pricing guide*. https://underdefense.com/blog/managed-siem-pricing-guide/