Project 1

Edison Maniwang

University of Maryland Global Campus

CSIA 485 Cyber Management and Policy Capstone

Professor Holly Ridgeway

April 8th, 2025

Introduction

The integration of Island Banking Services into Padgett-Beale, Inc.'s Financial Services division (PBI-FS) introduces a complex set of cybersecurity challenges and legal responsibilities. As a recently acquired entity, Island Banking Services brings with it an inherited technological environment, outdated infrastructure, and a lack of robust security controls — all of which pose immediate risks to the confidentiality, integrity, and availability of sensitive financial and customer data. Additionally, the organization has a history of internal criminal activity that went undetected due to significant breakdowns in oversight, access control, and system monitoring. These inherited weaknesses represent both regulatory liability and operational risk to PBI-FS if not addressed swiftly and strategically.

This document presents a comprehensive cybersecurity assessment and action plan developed to guide PBI-FS through the secure integration of Island Banking Services. The approach begins with a Gap Analysis that identifies key security deficiencies, many of which involve a lack of governance, insufficient employee training, inadequate identity and access controls, and missing incident detection capabilities. These issues are then translated into a formal Risk Register, where each risk is evaluated in terms of severity, legal exposure, and alignment with regulatory mandates such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), Bank Secrecy Act (BSA), IRS regulations, and Securities and Exchange Commission (SEC) guidelines.

Informed by the NIST Cybersecurity Framework (CSF), the proposed strategy includes five high-impact initiatives: establishing cybersecurity governance, launching organization-wide security awareness training, deploying modern identity and access management solutions, implementing centralized security monitoring, and modernizing outdated infrastructure. Each strategic action is supported by a realistic 12-month implementation timeline and mapped to specific risks, compliance requirements, and industry control standards.

By adopting this strategy, PBI-FS will not only remediate inherited security weaknesses but also create a scalable and sustainable cybersecurity posture. This approach ensures regulatory alignment, reduces the likelihood of future incidents, and positions the company as a secure and trusted provider of financial services.

GAP Analysis

This Gap Analysis identifies ten critical cybersecurity issues inherited from Island Banking Services, the bankrupt financial entity now reconstituted as PBI Financial Services. These gaps are drawn from the Padgett-Beale M&A Profile and related background materials and are informed by the Confidentiality, Integrity, and Availability (CIA) triad, the People, Process, and Technology (PPT) framework, and the NIST Cybersecurity Framework (CSF). The analysis places a particular emphasis on internal weaknesses that enabled extensive criminal behavior to occur without detection by uninvolved employees (NIST, 2018a; Computerworld, 2014).

1. Absence of a Cybersecurity Governance Program

Island Banking Services never established security policies, governance structures, or oversight mechanisms. This foundational failure created an environment where no one was accountable for cybersecurity, significantly impacting all three areas of the CIA triad. According to NIST CSF's Identify function, organizations must establish roles, responsibilities, and oversight mechanisms to manage cybersecurity risk (NIST, 2018a, ID.GV-1–ID.GV-3).

2. Lack of Security Awareness and Insider Threat Training

Employees were unaware of illicit insider activity, indicating not only a lack of training but also a culture where suspicious behavior was not questioned. The NIST CSF emphasizes that users must be trained to recognize and report cybersecurity risks (NIST, 2018a, PR.AT-1–PR.AT-5). The lack of training created a major internal control weakness that contributed to the success of fraudulent activity (Computerworld, 2014).

3. Weak or Nonexistent Access Control Mechanisms

There is no evidence of access control systems that could enforce separation of duties or limit access to sensitive financial data. Without multifactor authentication or role-based permissions, insiders

likely had excessive and unmonitored access. These conditions create prime opportunities for data misuse and fraud (NIST, 2020a, AC family; NIST, 2018a, PR.AC).

4. No Incident Detection or Response Capability

Criminal activity persisted over time without triggering alerts or investigations. The CSF's Detect and Respond functions stress the need for monitoring and response mechanisms to catch and address threats (NIST, 2018a, DE.CM; RS.RP). This gap represents a critical control failure that allowed malicious behavior to thrive without intervention.

5. Lack of Logging and Audit Trails

Island Banking failed to maintain logs or auditing tools that could detect anomalies or reconstruct incidents. Without audit trails, employees lacked the data necessary to report suspicions or verify suspicious activities. According to NIST SP 800-53, monitoring and audit logging are essential for supporting investigations and ensuring accountability (NIST, 2020a, AU and SI families).

6. Unencrypted Financial and Customer Data

The M&A case indicates full customer records were recovered, implying that sensitive data was stored without encryption. This is a major confidentiality lapse and a violation of best practices outlined in the NIST CSF's data protection subcategories (NIST, 2018a, PR.DS-1–PR.DS-5). It also conflicts with financial data protection requirements under laws such as GLBA (Computerworld, 2014).

7. No Vendor Risk Management or Third-Party Oversight

The organization used offshore operations without any reference to vendor security controls or oversight. This violates NIST CSF's Supply Chain Risk Management expectations (ID.SC), which require due diligence and oversight of third parties with access to sensitive data or systems (NIST, 2018a; IT Security Audit, 2022).

8. Use of Legacy and Unsupported Systems

Island Banking operated on legacy infrastructure that was likely unpatched and unsupported. This introduces well-known security vulnerabilities and system instability. The NIST CSF and SP 800-53 call for regular patching, system updates, and lifecycle management (NIST, 2020a, MA and SI controls; NIST, 2018a, PR.MA).

9. No Business Continuity or Disaster Recovery Plans

There is no indication of a disaster recovery or backup plan. This exposes the organization to operational collapse following a cyber incident or outage. The CSF's Recover function stresses the need for well-documented and tested recovery strategies (NIST, 2018a, RC.RP, RC.IM).

10. Noncompliance with Financial Services Laws and Regulations

Island Banking's collapse was due in part to legal and regulatory failures. Its lack of adherence to financial services laws such as GLBA, BSA, and SOX created severe process-level gaps. The CSF highlights the need to understand and meet regulatory obligations as part of a cybersecurity program (NIST, 2018a, ID.GV-2; PR.IP-4).

Legal & Regulatory Requirements Analysis

PBI Financial Services (PBI-FS), as a newly established financial services subsidiary of Padgett-Beale, must comply with a variety of U.S. laws and regulations governing the confidentiality, integrity, and availability of financial and customer data. These legal obligations directly inform how the risks identified in the Risk Register (see Table 1. Risk Profile Table) must be addressed and mitigated through policy, process, and technical control implementations.

The absence of a cybersecurity governance program (Risk 001) directly violates the Gramm-Leach-Bliley Act (GLBA), which mandates a comprehensive information security program including documented policies and internal oversight of risks to customer data (Computerworld, 2014). The Sarbanes-Oxley Act (SOX) also requires financial institutions to maintain internal control structures, especially those affecting the accuracy of financial reporting. The NIST Cybersecurity Framework (CSF) reinforces this through subcategories ID.GV-1 through ID.GV-3, which call for clear governance, risk oversight, and role assignments (NIST, 2018a).

Untrained employees and the lack of insider threat awareness (Risk 002) violate GLBA's expectations around security awareness. Under the NIST CSF PR.AT-1 through PR.AT-5, organizations are expected to ensure that all personnel are trained in cybersecurity policies and practices. The internal fraud at Island Banking Services highlights the consequences of failing to meet this requirement (Computerworld, 2014).

Weak access control practices (Risk 003) also violate GLBA, which requires limited access to nonpublic personal information. SOX and Securities and Exchange Commission (SEC) regulations further require access protections to ensure financial integrity. NIST provides prescriptive control requirements under SP 800-53 (AC family) and CSF PR.AC-1 through PR.AC-6, which mandate multifactor authentication, access logging, and privileged user management (NIST, 2020a).

The lack of incident detection or response planning (Risk 004) represents a major gap under the Bank Secrecy Act (BSA), which requires institutions to detect and report suspicious activity to FinCEN. Additionally, the SEC requires timely reporting of material cybersecurity incidents that may affect shareholders. These requirements are reflected in NIST CSF DE.CM (detection) and RS.RP (response planning) functions (NIST, 2018a).

The lack of audit trails and centralized logging (Risk 005) is another point of failure under both BSA and SOX, which mandate the preservation and review of system records and transaction histories. NIST SP 800-53 (AU and SI families) and CSF DE.AE-1 stress the importance of continuous audit mechanisms to ensure accountability and support post-incident forensics (NIST, 2020a).

Unencrypted customer data at rest and in transit (Risk 006) presents a serious breach of GLBA requirements to safeguard sensitive consumer information. The NIST CSF PR.DS-2 specifically mandates the use of encryption for data in transit, while other subcategories address encryption at rest and access management (NIST, 2018a).

The absence of vendor oversight and supply chain risk management (Risk 007) violates GLBA's Safeguards Rule, which requires institutions to ensure third parties with access to customer data maintain security controls. The NIST CSF ID.SC-3 further highlights the need for formal agreements and continuous assessment of supplier security practices (NIST, 2018a; IT Security Audit, 2022).

Legacy systems in use (Risk 008) introduce risks to data availability and integrity, violating requirements under SOX, GLBA, and Internal Revenue Service (IRS) guidelines, which call for secure and accessible recordkeeping. NIST prescribes system lifecycle management and patch control under PR.IP-3 and SP 800-53 MA family controls (NIST, 2020a).

The lack of a tested backup and disaster recovery plan (Risk 009) may lead to permanent data loss, violating SOX, IRS, and GLBA requirements. The NIST CSF PR.IP-4 and RC.RP-1 emphasize the need

for regularly maintained and tested backups to ensure data continuity in the event of a failure or cyber incident (NIST, 2018a).

Lastly, the general absence of compliance monitoring (Risk 010) is a root cause for the failures described above. GLBA, BSA, SOX, and SEC regulations all require regular internal reviews and updates to ensure compliance. The NIST CSF governance category ID.GV-2 stresses that roles and responsibilities must be aligned with external regulatory expectations (NIST, 2018a).

In summary, PBI-FS must implement a cybersecurity strategy that satisfies both regulatory requirements and industry standards. Aligning its control environment with NIST CSF and SP 800-53 will support compliance while improving risk posture and operational resilience.

Risk Analysis & Risk Register

In addition to financial services-specific laws such as the Gramm-Leach-Bliley Act (GLBA) and the Bank Secrecy Act (BSA), PBI-FS must also comply with a broader set of federal regulations that apply to all U.S.-based companies. These include the Sarbanes-Oxley Act (SOX), Internal Revenue Service (IRS) regulations regarding business record retention, and Securities and Exchange Commission (SEC) rules on reporting and internal controls. As part of this risk analysis, these requirements were reviewed and explicitly mapped to existing risks in the Risk Register where applicable. For example, SOX applies to Risk 001 (absence of cybersecurity governance), Risk 005 (lack of audit trails), and Risk 009 (lack of disaster recovery planning), due to its focus on internal control and data integrity requirements. IRS regulations were added to Risk 006 and Risk 008 to address the need for secure data retention and system availability. Additionally, Risk 010 was newly added during this phase to represent a general, overarching risk of noncompliance with multiple federal regulations—a gap that was not previously captured as a distinct entry but is critical given the organization's regulatory environment. By explicitly incorporating these broader legal frameworks into the Risk Register, PBI-FS ensures that all significant compliance risks are documented and traceable.

To address the risks identified in the Risk Register, PBI-FS applied the risk management principles outlined in Section 1.2 of the NIST Cybersecurity Framework (CSF) version 1.1 (NIST, 2018a). Each risk was evaluated for business impact and legal exposure, and a corresponding risk treatment strategy—accept, avoid, control, or transfer—was selected. For all identified risks, the selected strategy is control, as most of the threats involve noncompliance with binding regulatory requirements and operational risks that must be addressed to ensure the viability of the financial services business. For example, accepting or avoiding risks such as data encryption (Risk 006) or incident response (Risk 004) would be indefensible from both a compliance and ethical standpoint. For each control-based treatment, the Risk Register includes the appropriate NIST CSF category and subcategory, such as PR.AT-1 for training, ID.GV-1 for

governance, and PR.IP-4 for data backup and recovery. These mappings ensure that the chosen controls are aligned with industry standards and can be systematically tracked and measured. This approach not only supports compliance but also creates a clear foundation for strategic cybersecurity improvements aligned with the organization’s operational needs.

Table 1. Risk Profile Table

Risk ID	Risk	Category	Severity	Applicable Laws, Regulations, Standards	Risk Mitigation Strategy (description	Implementation: Required Technologies, Products or Services	NIST Cybersecurity Framework Category and Sub Category Identifier (e.g. ID.AM-1)	Sub-Category Description
001	No cybersecurity governance or policies	Process	5	NIST CSF ID.GV, GLBA, SOX	Implement formal governance with roles, policies, and oversight	GRC platform (e.g., Archer), policy templates	ID.GV-1	Policies, procedures, and governance established
002	Employees untrained in cybersecurity awareness	People	4	NIST CSF PR.AT, GLBA	Launch mandatory awareness & insider threat training	LMS, Phishing simulation tools	PR.AT-1	All users receive cybersecurity awareness training
003	Weak access controls & identity management	Technology	5	NIST SP 800-53 AC, GLBA, SOX	Enforce RBAC, MFA, and periodic access reviews	IAM tools (e.g., Okta), MFA software	PR.AC-1	Identities and credentials managed for auth.

004	No incident detection or response capability	Process	5	NIST CSF DE.CM, RS.RP, GLBA	Implement SIEM, IR plan, and train IR team	SIEM (Splunk, QRadar), IDS/IPS	DE.CM-1	Network monitored to detect potential cybersecurity events
005	No system logs or audit trails	Technology	5	NIST SP 800-53 AU, BSA, SOX	Enable audit logging, centralized log management	Syslog, Splunk, audit log review tools	DE.AE-1	Audit/log records are collected and reviewed
006	Unencrypted customer data at rest/in transit	Technology	5	NIST CSF PR.DS, GLBA	Encrypt data at rest/in transit using TLS and AES-256	Encryption software, TLS certs	PR.DS-2	Data-in-transit is protected
007	No vendor risk management or oversight	Process	4	NIST CSF ID.SC, GLBA	Establish third-party risk management program	Third-party risk assessment tools	ID.SC-3	Contracts with suppliers address cybersecurity risks
008	Legacy and Unsupported Systems in use	Technology	4	NIST SP 800-53 MA, PR.IP, GLBA	Conduct tech refresh, apply patches or decommission	Vulnerability scanners, patch mgmt.	PR.IP-3	Configuration changes are managed through change control
009	No backups or disaster recovery plan	Process / Tech	4	NIST CSF RC.RP, PR.IP-4, SOX	Implement BCP/DR with routine testing	Backup software, offsite storage, DR runbooks	PR.IP-4	Backups conducted, maintained, tested periodically

010	Noncompliance with financial sector regulations	Process	5	GLBA, BSA, SOX, SEC	Conduct compliance audits and gap assessments	GRC tools, legal compliance review	ID.GV-2	Security roles aligned with internal & external partners

Cybersecurity Strategy

To address the risks identified in the Risk Register and to build a secure, compliant foundation for future operations, PBI Financial Services (PBI-FS) must adopt a comprehensive cybersecurity strategy. This strategy integrates the People, Process, and Technology (PPT) framework, maps directly to the NIST Cybersecurity Framework (CSF), and focuses on achieving both regulatory compliance and operational resilience. The following five strategic actions are prioritized based on severity, regulatory impact, and their potential to mitigate multiple risks.

Establish Cybersecurity Governance and Compliance Oversight

PBI-FS must first build a formal cybersecurity governance structure that supports accountability and regulatory alignment. A Chief Information Security Officer (CISO) should be appointed to lead a governance team responsible for setting and enforcing cybersecurity policies. These policies must align with GLBA, SOX, and BSA requirements and include periodic risk assessments and audits. To support oversight, the organization should deploy a Governance, Risk, and Compliance (GRC) platform that facilitates documentation management, policy version control, and compliance tracking. This strategic action mitigates Risk 001 (lack of governance) and Risk 010 (noncompliance with federal regulations), and aligns with NIST CSF subcategories ID.GV-1 through ID.GV-3.

Implement Security Awareness and Insider Threat Training

To reduce vulnerabilities arising from human error or neglect, PBI-FS must implement a robust, organization-wide security awareness and insider threat training program. All employees should receive cybersecurity training at onboarding and at least annually thereafter, with additional role-specific content provided to those in sensitive or high-privilege positions. The training program should include simulated phishing exercises and gamified modules to improve retention and engagement. This strategy strengthens internal vigilance and mitigates Risk 002 (untrained staff) and Risk 004 (lack of incident

response capability). It aligns with NIST CSF subcategories PR.AT-1 through PR.AT-5, which emphasize training as a foundation of cyber hygiene.

Deploy Identity and Access Management (IAM) Controls

Protecting data integrity and confidentiality requires PBI-FS to implement modern identity and access management (IAM) solutions. This includes enforcing role-based access control (RBAC), using multifactor authentication (MFA), and conducting regular access reviews. IAM solutions should integrate with a centralized directory service such as Okta or Microsoft Entra ID to automate onboarding and offboarding processes. These controls mitigate Risk 003 (weak access controls), Risk 005 (lack of logging/audit trails), and Risk 010 (regulatory noncompliance), while aligning with NIST CSF subcategories PR.AC-1 through PR.AC-6.

Build a Centralized Security Operations and Incident Response Capability

To ensure timely detection and response to cybersecurity incidents, PBI-FS must establish a centralized security operations capability. This may involve developing an internal Security Operations Center (SOC) or contracting a Managed Security Service Provider (MSSP). In parallel, the company should create and test an Incident Response Plan (IRP) that includes clearly defined roles, escalation procedures, and post-incident analysis protocols. A SIEM platform should be deployed to collect and analyze logs from across the network, and intrusion detection systems (IDS/IPS) should be configured to alert on anomalous activity. This strategy mitigates Risk 004 (no detection/response), Risk 005 (no audit logging), and Risk 010, and aligns with NIST CSF subcategories DE.CM-1, RS.RP-1, and DE.AE-1.

Modernize Infrastructure and Implement Secure Network Architecture

PBI-FS must address its reliance on outdated systems and introduce a secure, segmented network architecture. This includes conducting a phased refresh of legacy hardware and software,

applying regular patches, and maintaining a comprehensive asset inventory. The network should be segmented into zones—for example, DMZ, finance, HR, and end-user systems—with firewalls and access controls between each. Encryption should be applied to all sensitive data in transit and at rest, and backup solutions should be tested regularly. This strategic action mitigates Risk 006 (unencrypted data), Risk 007 (vendor oversight), Risk 008 (legacy systems), and Risk 009 (no backup/recovery), while aligning with NIST CSF subcategories PR.IP-3, PR.IP-4, PR.DS-2, and RC.RP-1.

A future-state network diagram will accompany this strategy to illustrate the proposed architectural improvements, including segmented zones, redundant systems, and layered security controls.

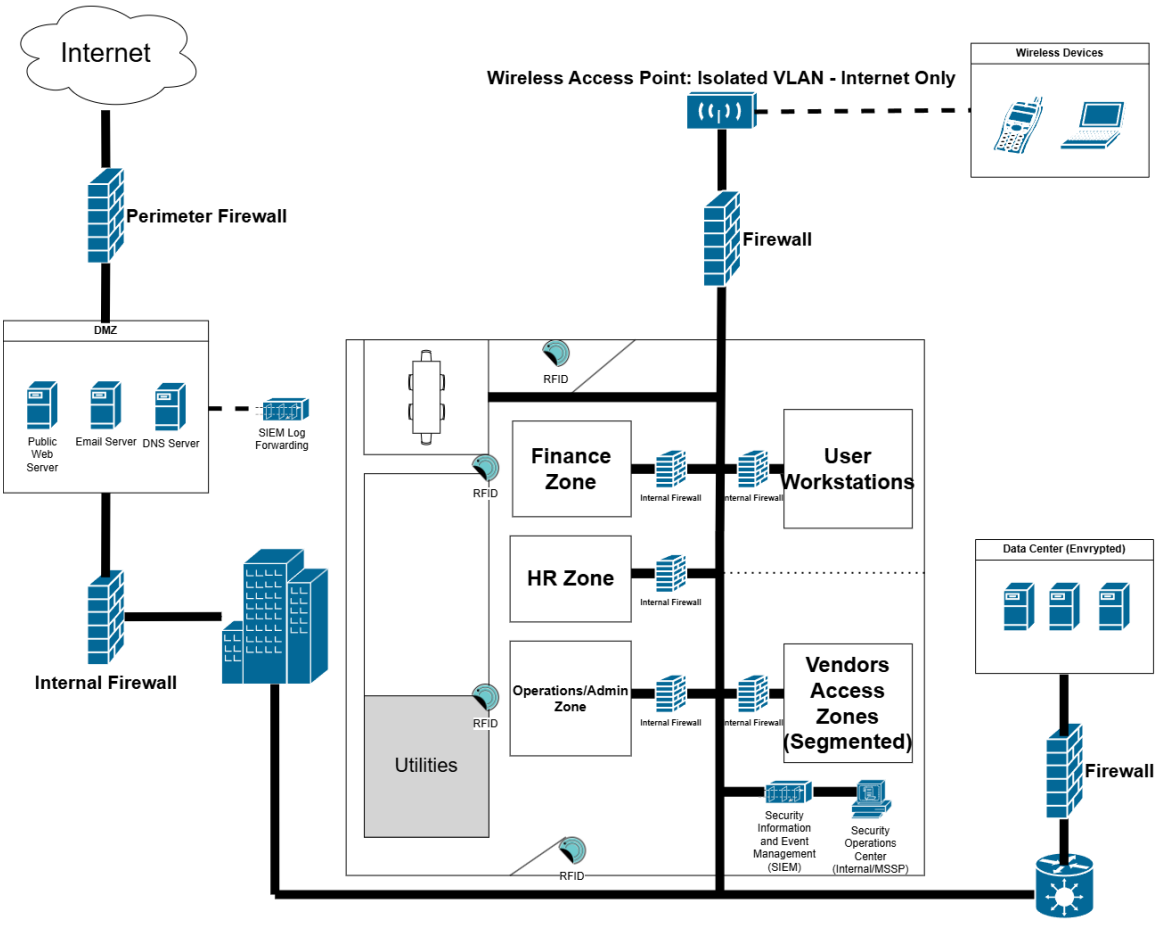

Figure 1. Updated Network Diagram for Padgett-Beale, Inc.

Plan of Action and Implementation Timeline

PBI Financial Services (PBI-FS) will implement its cybersecurity strategy over a **12-month period**. The plan will be executed in five distinct phases, with each phase addressing high-priority security needs and laying a foundation for long-term compliance and security. Below are the action steps, deliverables, responsible teams, and key milestones for each phase.

Phase 1: Establish Cybersecurity Governance and Policies (Months 1–3)

The first priority will be the establishment of a Cybersecurity Governance Program. This involves appointing a Chief Information Security Officer (CISO) and creating a Cybersecurity Governance Committee. This group will be responsible for drafting and publishing the necessary governance frameworks, security policies, and ensuring compliance with industry regulations. By the end of Month 3, all policies should be finalized, and documentation will be shared with the entire organization. This phase will mitigate Risk 001 (lack of cybersecurity governance) and Risk 010 (general noncompliance with federal regulations). Key milestones for this phase include the appointment of the CISO by the end of Month 1, the completion of policy drafts by Month 2, and full implementation of the governance framework by Month 3.

Phase 2: Implement Security Awareness and Insider Threat Training (Months 3–5)

The next priority is to address human risk factors by implementing an organization-wide security awareness program. This program will focus on educating employees about cybersecurity risks and proper protocols for reporting insider threats. Employees will be required to complete annual training, with role-based training for high-risk positions. In addition, phishing simulation campaigns will be launched in Month 4 to measure engagement and identify vulnerabilities. By the end of Month 5, all employees will have completed the training, and the organization will have a clear record of compliance. This phase is crucial for mitigating Risk 002 (untrained employees) and Risk 004 (lack of incident

detection/response). Key milestones include the development of the training content by Month 3, the pilot phase in Month 4, and full deployment by Month 5.

Phase 3: Deploy Identity and Access Management (IAM) Controls (Months 5–7)

Following training, PBI-FS will focus on securing identity and access management (IAM) to control who has access to sensitive systems. This phase includes deploying role-based access control (RBAC), enforcing multi-factor authentication (MFA), and automating onboarding and offboarding processes to ensure only authorized users can access critical assets. By Month 7, all critical systems will be protected by these IAM controls. This action will mitigate Risk 003 (weak access controls), Risk 005 (lack of audit trails), and Risk 010 (regulatory noncompliance). Milestones for this phase include selecting and integrating the IAM platform by Month 5, MFA deployment in Month 6, and the completion of role assignments and access reviews by Month 7.

Phase 4: Launch Security Operations & Monitoring Capabilities (Months 6–9)

Once access controls are in place, PBI-FS will implement a Security Operations Center (SOC) to monitor and respond to security events. A Security Information and Event Management (SIEM) system will be deployed to aggregate and analyze logs from internal firewalls, the DMZ, workstations, and all critical assets. By Month 9, the SIEM system will be fully operational, and security alerts will be routed to the SOC for timely response. This will mitigate Risk 004 (lack of incident detection and response) and Risk 005 (no audit logging). Key milestones include SOC team onboarding by Month 6, SIEM integration by Month 7, and live incident response capabilities by Month 9.

Phase 5: Modernize Infrastructure and Enforce Technical Controls (Months 8–12)

The final phase will focus on upgrading outdated infrastructure and implementing technical controls to further secure data. This will involve encrypting sensitive data at rest and in transit, replacing

legacy systems, and implementing secure backup solutions. A comprehensive disaster recovery plan (DRP) will be tested to ensure that PBI-FS can recover from a potential breach or disaster. The entire process will be completed by the end of Month 12, which will mitigate Risk 006 (unencrypted data), Risk 007 (vendor oversight), Risk 008 (legacy systems), and Risk 009 (lack of backup and recovery planning). Key milestones include initiating infrastructure upgrades by Month 8, deploying encryption protocols by Month 9, and completing DRP testing by Month 12.

This 12-month implementation timeline outlines clear phases of action, with each step addressing critical vulnerabilities and aligning with industry standards like the NIST Cybersecurity Framework (CSF). The successful completion of each phase will ensure that PBI-FS remains compliant, resilient, and prepared to manage any cybersecurity threats. By the end of the 12 months, PBI-FS will have a robust, defensible cybersecurity posture capable of meeting both regulatory and operational needs.

Executive Recommendation Memo

To: Chief Executive Officer, Padgett-Beale, Inc.

From: Edison Maniwang, Cybersecurity Analyst

Date: April 8th, 2025

Subject: Executive Summary and Cybersecurity Recommendation for Island Banking Services Integration

Purpose

This memo provides a summary of key cybersecurity risks identified during the assessment of Island Banking Services and presents a recommended strategy and implementation plan to ensure regulatory compliance, operational resilience, and long-term cybersecurity maturity for Padgett-Beale, Inc. (PBI-FS).

Key Findings

The acquisition of Island Banking Services revealed significant cybersecurity gaps and internal control failures that enabled criminal activity and exposed the organization to reputational, legal, and operational risks. A Gap Analysis identified 10 major cybersecurity deficiencies across governance, training, access control, monitoring, and data protection domains. Many of these gaps stemmed from a lack of defined security policies, outdated infrastructure, and insufficient audit and detection capabilities.

Further analysis showed that these weaknesses violated several financial regulations, including the Gramm-Leach-Bliley Act (GLBA), Bank Secrecy Act (BSA), Sarbanes-Oxley Act (SOX), and IRS and SEC requirements. The absence of cybersecurity governance and proper audit trails (e.g., Risk 001 and Risk 005) would prevent PBI-FS from passing compliance audits or responding effectively to cyber incidents.

Risk Prioritization

A Risk Register was created to assess the severity of these issues. The most critical risks included:

- Lack of cybersecurity governance and compliance oversight (Risk 001, Risk 010)
- Weak access controls and untrained staff (Risk 002, Risk 003)
- Absence of incident response and security monitoring capabilities (Risk 004, Risk 005)

Each risk was mapped to the appropriate NIST Cybersecurity Framework (CSF) category and matched with a treatment strategy focused on applying industry-standard controls.

Recommended Strategy

A five-part cybersecurity strategy has been developed, addressing the organization's most urgent vulnerabilities while supporting scalable, long-term security practices:

1. Establish Cybersecurity Governance to ensure executive oversight and regulatory alignment.
2. Implement Security Awareness Training to reduce human error and strengthen insider threat prevention.
3. Deploy Identity and Access Management (IAM) to restrict access to critical systems and maintain integrity.
4. Launch Security Monitoring (SIEM & SOC) for real-time detection and incident response.
5. Modernize Infrastructure and Backup systems to address legacy risks and ensure recoverability.

This strategy aligns with both the People, Process, and Technology (PPT) framework and NIST CSF and directly mitigates each risk identified in the initial assessment.

Implementation Timeline

The cybersecurity transformation will be executed over 12 months, divided into five implementation phases. High-priority actions—such as establishing governance and launching training—will be completed in the first 3–5 months. Technical deployments (IAM, SIEM, encryption) will follow in later phases. The final quarter will focus on infrastructure upgrades and disaster recovery testing to solidify the company's cybersecurity foundation.

Final Recommendation

It is strongly recommended that the proposed strategy and implementation plan be adopted immediately to protect PBI-FS from continued exposure to cyber threats, financial penalties, and reputational damage. With executive support and appropriate resource allocation, this plan will not only remediate inherited risks from the Island Banking Services acquisition but also position PBI-FS for sustainable cybersecurity maturity and regulatory compliance.

References

Computerworld. (2014). *Learn the science of compliance to survive*. Computerworld. https://www.computerworld.com/article/2489147/learn-the-science-of-compliance-to-survive.html

IT Security Audit. (2022). *Cybersecurity audit services – IT security audit*. IT Governance USA. https://www.itgovernanceusa.com/cybersecurity-audit

NIST. (2018a). *Framework for improving critical infrastructure cybersecurity, version 1.1 (NIST CSWP 04162018)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Revision 5)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Swire, P., & Kennedy-Mayo, D. (2020). *U.S. private-sector privacy: Law and practice for information privacy professionals* (4th ed.). International Association of Privacy Professionals.