Cybersecurity Strategy and Plan of Action

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

# Introduction

Cybersecurity is one of re basic requirements of an organization and company or business is safe and secure these days without meeting modern cybersecurity requirements. Growing number of cyber-attacks and data breaches has raised significant threat at organizational level as the most important asset for an organization is data. Data has the potential of affecting company finances directly or indirectly on the basis of security or vulnerability. To ensure security of data and safe transactional procedure of finances, an effective and robust cybersecurity policy or strategy based on a complete plan of action is required. For same purposes, a cybersecurity policy is required for the new acquisition (PBI-FS) which is the acquisition of Island Banking Service by Padgett-Beale. Island banking service was forced to terminate its operations because of money laundering charges against the service and all the financial transactions, records, software and hardware infrastructures were sealed by bankruptcy courts. Padgett-Beale has decided to purchase these assets which include dedicated software systems for financial transactions processing, licensing operating systems for servers and database software for workstations. Padgett-Beale has successfully convinced and negotiated with criminal and bankruptcy courts for provisions of resuming the services again. Island Banking Service lacked a competitive and effective strategy for cybersecurity assessment and planning so a new strategy and plan of actions is required from scratch. Padgett-Beale’s team of Merger and Accountability is responsible for this task which is working with Chief Information Security Officer of Padgett-Beale under his direct supervision and instructions. This document provides a cybersecurity plan of action for M&A team for the acquisition (PBI-FS) by performing a gap analysis, requirements analysis in terms of legal and regulatory aspects and complete overview of the risk analysis. The plan of action or cybersecurity strategy is developed in accordance with the decision of operating this new acquisition as a separate but fully owned subsidiary of Padgett-Beale and acquisition plan is also amended accordingly.

# Gap Analysis

An effective Gap analysis related to cybersecurity is very essential as it provides information and details about limitations and vulnerabilities that are responsible for lack of progress or security issues. In this case we will analyze the gaps from 2 perspectives, one from the issues and problems that were identified in Island Banking Services and resulted in its bankruptcy and secondly, expected loopholes or gaps in the new acquisition (PBI-FS) based on its new journey with Padgett-Beale.

Employees of the Island Banking services were involved in several criminal activities as identified in the report. Managers and company officers were involved in exercising illegal and criminal activities using IT assets of the company without getting detected. This identify the gap with respect to Accountability, AU-Audit and AC Access Control. The audit and accountability incorporate several controls which are helpful in developing audit capacity of the enterprise and also specifies what kind of assets and domains are to be audited. These reports are used to assist in investigations, show compliance and ensure that all the respective security controls are working and implemented properly.

It was found that after termination of the operation by law enforcements agencies, Island Banking Service had no business continuity plan or disaster recovery option in place. Due to loss of workstations and servers, the operation could not be performed again. This gap suggests that there was lack in contingency planning and it is required to apply controls of contingency planning family in order to be able to start the operation and working of the frameworks and systems in case termination due to power outage, theft physical damage, natural disasters or any related issue.

Another issue found in the gap analysis was lack of backup infrastructure on an off-premise location which made it impossible for the company to recover data and important information in case of seizure of operations from Law Enforcement agents.

PBI-FS is opening is shifting to a new place which is in the same town but 10 miles away from the previous position which is the location of Island Banking Service. The new acquisition requires hiring of 10 residents of island and also 2 supervisors for the call center which is being opened on the property owned by Padgett-Beale. Gap analysis of the acquisition has also identified issues related to intercultural communication differences. According to survey was focused on the relationship of communication context based on difference of culture and region. The survey conducted explained that the communication culture of Padgett-Beale was low context while new applicants of the jobs at PBI-FS were expecting a high context communication culture. Also, the applicants were expecting High power distance in the new company/acquisition PBI-FS while the power-distance was medium in Padgett-Beale.

Another issue found in gap analysis during the survey was lack of system life cycle for privacy and security. For this purpose a Risk management framework is required which must include a comparatively flexible process for valuation of organizational assets, a disciplined structure, assessment, authorizations and implementation.

Risk Management is also one of the important requirement of a cybersecurity of a company. Island banking service lacked an effective system for managing risk related to organization, IS view and overall mission of the business. A well-directed guidance is required for and integrated and organization-wide program for risks management of information security to organizational operations.

Another issue/risk found in the gap analysis of the PBI-FS is the lack of code of practice regarding important controls of cybersecurity. Effective guidelines are required in order to provide guidelines related to these guidelines especially for the cloud services.

# Legal and Regulatory requirements

In making an organizational policy, procedures and standards, laws and regulations are major drivers. Cyber security standards are also one of the important factors to consider before adopting any policy. The responsibilities of a company’s CEO include ensuring compliance and compatibility of operations and services with these regulations. PBI-FS is also based on these regulations and standards and it is the responsibility of M&A team to understand these requirements and update CISO about the implementation of these standard and regulations. PBI-FS is organized to follow NIST standards of cyber security strictly to avoid exposure to illegal or crime related activity or attack. These standards are formed to provide a proper framework to help companies and organizations in building their programs of information security based on principles which are defined by a trusted community of the cyber security leaders. Basically, these standards are created and put in place by third-party organizations. A security policy is important to specifically address the extent of every one’s stake related to information security in an organization. Also, the information about privacy and confidentiality of the information, availability, and integrity, implementation of the security measures, information’s classification, and the balance of exposure of risk on cost of risk mitigation are discussed and determined in a policy. These policies and regulations are important t follow because companies entirely deal with internet and online business and are vulnerable to different types of scams and cyber threats. Concerns are there from both the ends but for the smooth operation and secure online business and transactions, compliance with rules and regulations is very important. An important thing to note in this regard is the fact that there is no federal law or regulations which is liable to be followed by everyone but there are standards which everyone is recommended to follow for safe and reliable transactions. One of the cybersecurity rules has importance on federal level as it is associated with CUI (Controlled Unclassified Information) generally from federal entities that are mainly handled by the contactors generally. It includes documents including information related to proprietary material, information about legal procedures and health-related content.

It is the job of M&A team of PBI-FS to ensure the implementation of cybersecurity standards and regulations based on specific requirements. Unlike other domains, cybersecurity of a company needs had to comply with more than one regulation or set of standards. The best approach is to outline and identify all the respective regulations that may affect the company primarily and then determine which of the security controls are required to be considered and implemented to get the desired results. Some of the important frameworks which we are going to use and adopt for compliance requirements in PBI-FS are given below.

NIST framework is the most popular and we are going to implement and use this framework more than any other regulatory entity. It is the acronym of National Institute of Standards and Technology and was created to provide a guide which is essentially customized pertaining to matters as how to reduce and manage the cybersecurity risks by combining the best practices, guidelines and standards. It assists in fostering the communication between the external and internal stakeholders by developing a common language of common risk between different organizations. We will implement several standard and guidelines of NIST in PB-FSI in order to mitigate the risks and solve different issues identified in the gap analysis in the above section of the project. NIST is a voluntary framework and any organization/company can opt to implement in order to minimize the overall risk.

Another very important act that is very important to consider in PBI-FS security is PCI-DSS. Island Banking service had experienced discrepancies regarding online transaction of finances and in the utilization of modern ways of transfer of finances and this aspect has also been mentioned and identified in the gap analysis. This has costed previous business significantly in terms of money, security and reliability. This Act is the solution to this problem and is going to be implemented PBI-FS services. It is acronym of Payment Card Industry Data Security Standard and is a set of regulations designed and out in place in order to reduce the frauds and secure the credit information of the customers and clients.

COBIT is another regulatory act that is to be implemented in PBI-FS cybersecurity strategy and to be included in the plan of action. This the acronym of Control Objectives for Information and related Technologies and the framework was introduced to assist the organizations to mage the IT governance by linking the goals of IT and business together. Areas included this regulatory act are assurance and audit compliance, risk and security management, IT operations governance.

These are some of the Legal and regulatory requirements and related standards and frameworks which are going to be implemented in order to ensure effective compliance management and adding security and reliability in operation.

# Risk analysis and Risk Register

References

Last Name, F. M. (Year). Article Title. *Journal Title*, Pages From - To.

Last Name, F. M. (Year). *Book Title.* City Name: Publisher Name.