Implementation Plan

[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.]

Contents

[Business context 3](#_Toc33960522)

[Introduction 4](#_Toc33960523)

[Goals and Objectives 4](#_Toc33960524)

[Scope 6](#_Toc33960525)

[Assumptions 6](#_Toc33960526)

[Constraints 7](#_Toc33960527)

[Project Management Plan 8](#_Toc33960528)

[Strategy Implementation 10](#_Toc33960529)

[System Development Life Cycle 11](#_Toc33960530)

[Enterprise IT Architecture 16](#_Toc33960531)

[References 18](#_Toc33960532)

# Business context

 The implementation plan presented in this document is about the financial services company PBI-FS. PBI-FS is the acquisition of Island Banking Services by Padgett-Beale which is a multinational organization having an extended business in different countries of the world. Island Banking Services was previously a reputable organization of financial services having clients in different parts of the United States and the world, a call center and a lot of financial resources. The banking services started getting frequent losses in the business and started getting legal charges against it so much so that its reputation and operational success started getting down. Island banking service was charged by regulatory authorities for not complying with the standard principles and regulations. The service was forced to be terminated along with all the operations by regulatory authorities due to charges of money laundering and other activities that come under financial crimes or misconduct. Not only were the operations terminated but all the resources including software and hardware infrastructure, financial records, and financial transactions were sealed by the Bankruptcy Court after proper hearing s of the case. Padgett-Beale decided to acquire the financial services by successfully convincing the regulatory bodies and bankruptcy courts to resume the service again from the beginning in the form of PBI-FS. After getting permission from the regulatory authorities and getting some of the resources of the previous business, Padgett-Beale is now looking to implement a state of the art cybersecurity plan of action to avoid situations faced by Island Banking Service. In the previous project, an extensive plan of action and strategy was presented to the Merger & Acquisition team of the business which is working under the supervision of CISO of Padgett-Beale. As the process of acquisition is moving from the stage of developing a strategy to the implementation, a thorough and effective plan for implementation of the cybersecurity strategy is going to be presented to the M&A team.

# Introduction

The industry of financial services is at constant risk of cyber-attacks and data breaches based on observation of frequently related activities in the past few decades. These incidents and practices have raised a significant threat in organizations dealing with financial services and urged them to adopt effective techniques of data security and privacy. An effective cybersecurity plan of action is key to the success of any organization and its proper implementation is even more important. The implementation plan covers the objectives and goals of the implementation plan, scope, constraints and assumptions, an exclusive project management plan and a model for strategy implementation. In the end, the project implementation plan will also cover the schematic representation of IT infrastructure and security controls required as a comprehensive model of implementation for PBI-FS.

# Goals and Objectives

In many organizations, there are some specific goals and objectives that are defined based on the nature of business. PBI-FS is a company related to banking and financial services, so the business strategy and the implementation plan is designed in order to fulfill the business requirements to achieve those specific goals. PBI-FS has three important and significant business goals which are considered while developing the implementation strategy. Three main business goals are marketing, sales, and IT systems. The main objective of marketing is to increase the number of sales and in the case of PI-FS, customers. This requires an inbound marketing strategy to be included in the plan of action which may include incorporation of marketing automation tools and new CRM. These steps will help the business to target a greater number of customers by using customer tracking tools and enabling targeted email campaigns. The second business goal is sales where it is necessary for the sales team to speed up the process of taking the order while attracting more and more customers. They may need an app developed by the developer team which can be integrated with the marketing automation tool or CRM to achieve the goal (Cybersecurity objectives, 2017). The third business goal of a financial services organization is IT systems. A significant increment in the storage capacity of the systems and operating capabilities is central to support growth and development. For this purpose, the IT department can come up with new tools and software programs based on specific requirements of the business. Also, for further improvements, cloud migration is also one of the options which can be considered to migrate all the key systems and software application to the cloud. These are business goals or objectives of PBI-FS and must be considered while developing the implementation plan for the company.

As far as project goals are concerned, there are three main goals that are under consideration while making the implementation plan. These goals are the security of the financial assets of the organization and customer’s data, secure IT infrastructure and compliance management. The first goal is very clear and understandable as securing resources is essential for a successful business and smooth operations throughout. The second goal is associated with the implementation of cybersecurity techniques and protocols to minimize vulnerabilities which are also discussed in detail in Project 1 (the plan of action). The third goals are compliance management that is also discussed in detail in the first project. The importance of compliance management can be understood from the example of Island Banking Services which could not manage compliance with regulatory requirements of the business which ultimately resulted in the termination of operation along with resources sealed by the Bankruptcy court. The goals for project implementation are in accordance with cybersecurity strategic plan that was presented to the M & A team and now, proper implementation is the next step.

# Scope

Before the implementation of the cybersecurity plan of action, it is important to define the scope. The scope determines the areas which are going to be covered in a particular project and are under the domain. In the implementation plan, the detailed plan of action i.e. projects 1 will be considered for defining the scope of the project. The scope of the project is organizing the strategic plan using the system life cycle process model for the effective execution of the project in a systematic way. The process will be implemented by considering compliance management, risk assessment done in the previous project by assessing the risk register, and implementation of all the necessary controls analyzed and discussed for protecting the financial services of the PBO-FS and IT infrastructure (software and hardware).

The implementation of the strategic plan of action is the responsibility of the M & A team which comes under the supervision of COSI of Padgett-Beale. This indicates that issues and matters which may lie out CISO’s control are also out of the scope of this project. As an example, issues pertaining to the requirement of finance/funding are out of the scope of this project as it comes under CFO’s domain which is Chief Financial Officer.

# Assumptions

In developing strategies and implementation plans, it is always important to have assumptions regarding the effectiveness of the program. CISOs make these assumptions in order to cross-check their implementation and recommendations by looking into the matter from a critical point of view. Assumptions in the implementation of the network security infrastructure can vary immensely especially when we are dealing with organizations in the banking sector. Since the market continues to vary in size and types of services being provided, the controls that are being implemented also continue to change with the passage of time. The assumptions that we should keep in mind while implementing this infrastructure plan are detailed as follows:

* Processes such as international transactions are already happening inside the organization and the basic infrastructure already exists.
* Networks exist in the organization working on the approved networking protocols.
* The organization has mechanisms to forego international transactions with companies and individuals who have accounts in other accounts or countries.
* The organization is willing to implement financial security protocols to stop corruption and other fraudulent activities from taking place (Tytarenko,2017).
* The organization has a good record with the authorities in terms of audits with law enforcement agencies.
* The organization is willing to let the Information security professionals implement the controls.

# Constraints

Every project faces some considerable constraints which are inevitable to overcome. In the project planning or before the implementation, it is important to consider these constraints so that the project’s scope can be defined more exclusively to make the tasks easy and more predictable. Financial services provided by Padgett-Beale also have some constraints which are listed as.

* The operation is primarily restricted to the local and national levels despite the fact that Padgett-Beale is a multinational level company.
* The company was started from scratch as it was banned by bankruptcy courts which means that it does not possess self-generated revenue.
* The company is only restricted to financial services so a focus on only one domain will be required exclusively.
* The newly hired employees from the Island are not experienced enough to be included as effective members of the team for the implementation plan.

# Project Management Plan

The implementation plan is a complete project which requires proper defined times and resources towards its completion. For an effective completion according to the estimated time, it is very important to consider different resources associated with the project including people, processes and time. In this section, details, and requirements about these resources are given across different stages of the project.

The first aspect to consider is the requirement of human resources in the project. In our strategy, after determining the regulatory and compliance management, key stakeholders are identified. Key human resources involved in the implementation plan project are.

* Merger and acquisition team of PBI-FS and CISO of Padgett-Beale
* 10-12 new candidates hired from the Island along with one supervisor for the call center.
* Stakeholders in the business having a share in revenue generation and resource management
* A cybersecurity analyst/It technician for the implementation of new controls and practices on the IT infrastructure described in the strategic plan.

Important processes involved in the project are online financial services, implementation of NIST guidelines for an effective code of practice, and risk management. Risk management is thoroughly covered in the first part of the cybersecurity plan of action. In this project, several risks/gaps identified along with their solutions will be considered for implementation. Important processes include compliance management, risk mitigation, and implementation of proper budgeting and auditing.

 The third important resource is technology. After reviewing the existing infrastructure used by the Island Banking Service, the M& A team of the PBI-FS has identified that the already deployed equipment is approximately 5 years old and can be used for operations after proper experiments and analysis. Instead of outsourcing, it is decided to use the equipment for PBI-FS and save unnecessary expenditure. The equipment is also included in the implementation plan and will be used according to the implementation strategy discussed in later sections. These technology resources or equipment include

* Telecommunications, network equipment
* Banking applications including their servers and databases
* Data recovery and backup systems
* Public Web Server and Electronic WebMail.
* Computer workstations used by employees

The project of implementation requires the above-mentioned resources for the proper implementation of the strategy or cybersecurity plan of action.

# Strategy Implementation

This is the most important section of the project where all the important steps and details are going to be discussed.

The implementation plan deals with several controls recommended by NIST. To assist the organizations in selecting appropriate controls for effective security management, NIST introduced baseline controls. These controls are actually the starting points for determining the selection process of security controls. These controls are of many types but for the project at hand, we have selected High-Impact Baseline controls which are usually incorporated to protect sensitive information related to financial services and for other organizations that deal with sensitive data. Baseline controls used and implemented in the plan include

* AU-9 for protection of Audit Information
* AU-11 for Audit-Record retention
* CP-8 for telecommunication services
* PE-2 for Physical Access authorization (Bodeau & Graubart,2013)

Compensatory controls are used to minimize the gaps in IT compliance management associated with financial services. These controls are also incorporated in the implementation plan of the cybersecurity strategy as discussed in the plan of action project.

# System Development Life Cycle

 In this section, the implementation plan is represented in the form of a system development life cycle to show the succession and organization of key steps that are going to be performed. In this development model, phases of a project are defined based on a time schedule to clearly specify the different steps of operation and time duration. The cybersecurity implementation plan for the PBI-FS is divided into different phases while breaking down the project into different steps. The development of life cycle is explained below.

 **System planning**: This the first step of the project in which planning is finalized regarding new standards and techniques that are going to be implemented. Also, compliance management, selection of security controls and application of risk mitigation strategies are also discussed.

**Analysis**: In this step, the entire program is analyzed based on the scope, assumptions, and limitations of the project that are discussed in the above sections. Analysis of compliance management, auditing, risk mitigation techniques, and strategies and suggested security controls are done int his phase.

**Design**: This is the third phase of the program development life cycle and is characterized by adaption of a new design for the implementation based on system planning and analysis. The system design covers requirements of the software, hardware, cybersecurity defenses, and the network infrastructure.

**Implementation**: This is the central phase where all the planned controls and techniques are implemented according to the requirements. In the implementation plan of cybersecurity of PBI-FS, the plan of action is implemented in accordance with suggested security controls and techniques mentioned in the risk management and compliance management sections to protect the financial services.

**Testing and Integration**: In all the processes, implementation is followed by testing and integration phase. In the testing phase, the progress of the system/ project is determined after comparing it with the previous situation. As in the case of PBI-FS, the infrastructure used by Island Banking Service is used new security policy. In this phase, the progress of the systems and security is analyzed to check the integrity of the plan.

**Maintenance:** This is the last stage of the implementation plan in which the issues and problems identified in the testing and integration phase are addressed. In case of new updates to the systems or suggested controls, the implementation is considered to get the desired results.

 **Program development Life Cycle**

|  |  |  |  |
| --- | --- | --- | --- |
| Phase | Objective/Function | Milestone | Resources |
| Project planning |  The first step of the project regarding new standards and techniques that are going to be implemented.Compliance management, selection of security controls and application of risk mitigation strategies are also discussed. | The project milestone of this stage is making a complete plan based on the risk register and regulatory requirements in the first project. | Processes using guidelines, standards, and cybersecurity techniques.  |
| Analysis | The program is analyzed based on the scope, assumptions, and limitations of the project that are discussed in the above sections. Analysis of compliance management, auditing, risk mitigation techniques, and strategies and suggested security controls are done int his phase. | Analyze the milestone developed at phase one by the M&A team of Padgett-Beale | People (M&A team, cybersecurity analysts |
| Design | This is the third phase of the program development life cycle and is characterized by adaption of the new design for the implementation based on system planning and analysis. The design covers requirements of the network software, hardware, cybersecurity defenses infrastructure | The milestone of this phase is system design development in just before proper implementation | People (M&A team, cybersecurity analysts) and resources include network software, hardware, cybersecurity defenses infrastructure and Telecommunications, network equipment  |
| **Implementation** | The central phase of PDLC where all the planned controls and techniques are implemented according to the requirements. In the implementation plan of cybersecurity of PBI-FS, the plan of action is implemented in accordance with suggested security controls and techniques mentioned in the risk management and compliance management sections to protect the financial services. | To implement the recommended controls and all recommendations in this one phase | Telecommunications, network equipment Banking applications including their servers and databases Data recovery and backup systemsPublic Web Server and Electronic WebMail.Computer workstations used by employees |
| **Testing** | implementation is followed by the testing and integration phase. In the testing phase, the progress of the system/ project is determined after comparing it with the previous situation. As in the case of PBI-FS, the infrastructure used by Island Banking Service is used new security policy. In this phase, the progress of the systems and security is analyzed to check the integrity of the plan. | Testing frequently after proper implementation | M&A Team |
| Maintenance | The last stage of the implementation plan in which the issues and problems identified in the testing and integration phase are addressed. In case of new updates to the systems or suggested controls, the implementation is considered to get the desired results. | Addressing the problems identified in testing phase well in time | Cybersecurity analyst |

# Enterprise IT Architecture

 IT infrastructure of PBI-FS for the financial services is comprised of hardware, software, and network elements. After a thorough analysis of the project planning, a comprehensive design is made for the implementation. Software requirements consist of several software implications of financial services like PCI-DSS and other basic security controls associated with the networking of the system. Firewalls are dedicated to virtual private networks that are incorporated to have control over the internet traffic. All the data including sensitive information goes through a proxy network which hides the address of host (company) computers and replaces it with the remote private network, In this way, the possibility of the man in the middle attacks or exploitation of the company’s network and ultimately data breach is minimized. NIST cybersecurity standards and guidelines and basic necessary security control related to Audit Information, physical Access Authorization, Audit record retention, and telecommunication services are also implemented. Hardware infrastructure shows telecommunication, routing path, firewalls, and configuration of banking and transactional data path. The IT infrastructure is made to show the access network and how a customer accesses the financial services of the PBI-FS.



References

*Cybersecurity objectives*. (2017). Retrieved from pakt: https://subscription.packtpub.com/book/networking\_and\_servers/9781788836296/1/ch01lvl1sec14/cybersecurity-objectives

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cybersecurity strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

Bodeau, D., & Graubart, R. (2013). Cyber Resiliency and NIST Special Publication 800-53 Rev. 4 Controls. *MITRE, Tech. Rep.*

Tytarenko, O. (2017). *Selection of the best security controls for rapid development of enterprise-level cyber security*. Naval Postgraduate School Monterey United States.