# Project #2: Cybersecurity Implementation Plan

## Your Task:

The Acquisition of Island Banking Services has moved from the strategy development phase to the integration phase. In this phase, the M&A team will develop transition and implementation plans. Padgett-Beale’s Chief Information Security Officer (CISO) has recommended that a separate Cybersecurity Management Program be established for the Padgett-Beale Financial Services (PBI-FS) subsidiary to isolate as much risk as possible to the PBI-FS organization. This management program will require the establishment of policies, plans, and procedures which are customized to the financial service industry and the operating structure of PBI-FS.

The CISO has asked you to continue supporting the Merger & Acquisition team’s efforts. Your specific tasking is to assist in developing an implementation plan for the previously developed Cybersecurity strategy (Project #1). Since there have been additional developments in the M&A strategy overall, you should pay close attention to the Background Information provided later in this document.

Using your prior work (Project 1), develop a high-level plan for implementing a Cybersecurity Management Plan that will allow PBI-FS to begin operations in its new, on-island location. (The plan for the U.S. headquarters is being developed separately from your efforts.) This plan must take into account compliance requirements for U.S. banking laws, regulations, and standards. It must also include recommendations for required security controls, replacement of outdated hardware and software, and other measures necessary to reduce risk to an acceptable level. You must specifically address measures to reduce risks associated with both insider threats and external threats and threat actors.

**Note: you MUST use the implementation plan outline provided later in this document.**

You may need to perform additional analysis to address issues specific to the findings from the M&A team regarding the as-is state of the purchased assets which comprise the existing IT infrastructure.

Your high-level plan should include the system development life cycle (SDLC) gates/decision points and relevant tasks required to implement changes in the company’s hardware, software, and infrastructure. See <https://www.sebokwiki.org/wiki/System_Life_Cycle_Process_Models:_Vee> for more information about the gates & decision points.

You must also address any systems or software interoperability issues which may arise (especially those associated with the company’s existing custom software applications). You do not need to prepare a comprehensive Interoperability Assessment but, you should identify key issues and concerns. See the following resources for definitions and guidance:

* <https://www.smartgrid.gov/recovery_act/overview/standards_interoperability.html>
* <https://www.fcc.gov/general/interoperability>

You must clearly show that you have applied the following frameworks and concepts in your analysis and planning:

* Cybersecurity Principles: confidentiality, integrity, availability, non-repudiation, authentication, auditability, accountability
* NIST Cybersecurity Framework (see [https://‌nvlpubs. ‌nist.gov/‌nistpubs/‌CSWP/‌NIST. ‌CSWP. ‌04162018.pdf](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) )
* NIST Security and Privacy Controls (see NIST SP 800-53) OR Center for Internet Security (CIS) 20 Critical Security Controls for Effective Cyber Defense (see <https://www.tripwire.com/state-of-security/security-data-protection/security-controls/cis-top-20-critical-security-controls/> )
* Information Security Management Systems (ISMS) – ISO 27001/27002 (see <https://www.praxiom.com/toc35.htm> and <https://www.praxiom.com/iso-27001.htm> )

**Note: Make sure that you include (in detail) the steps you would take to secure the new infrastructure.**

## Background:

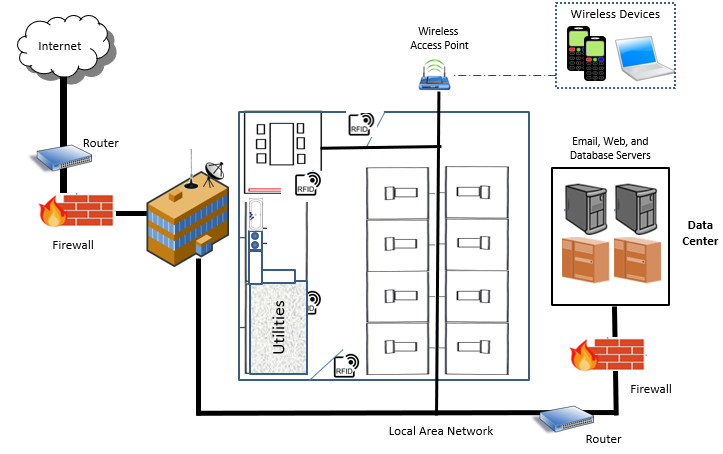
As part of the purchase agreement for Island Banking Services, Padgett-Beale made a commitment to the bankruptcy court to operate the call center and transaction processing center on the island for the next five years. The Padgett-Beale, Inc. Merger and Acquisition Strategy for Island Banking Services has been updated and now includes the following stipulations which are derived from requirements to comply with U.S. laws and regulations while also implementing the contractual agreement to continue some operations on the island.

1. Island Banking Services will become Padgett-Beale, Inc - Financial Services (PBI-FS).
2. PBI-FS will operate as a wholly owned subsidiary with its own management structure.
3. PBI-FS's will be incorporated as a U.S. corporation and will comply with all applicable laws and regulations.
4. PBI-FS's headquarters unit and executive staff (including the CEO, COO, and CFO) will have separate offices from PBI but will be located within a 5 mile radius of the PBI Headquarters.
5. PBI-FS's call center and transactions processing center will remain on the island but will move to a vacant office building adjacent to the existing Padgett-Beale resort property.
6. The deputy CISO from Padgett-Beale will serve as the interim CISO for PBI-FS.
7. The CISO from Padgett-Beale will serve as a consultant to PBI-FS for all matters relating to the establishment of the subsidiary's Cybersecurity Management Program.

As part of its *due diligence* efforts, the Padgett-Beale M&A team reviewed the existing cybersecurity posture for Island Banking Services. This review determined that, while there were some IT security protections in place, Island Banking Services never had a formal IT security program. Instead, the company outsourced management of its hardware, software, and networks to an islander owned and operated IT services company. This company installed and managed the networking equipment, firewalls, and workstations. Some workstations were used by tellers to conduct financial transactions using a web-based interface to a back-end database. The M&A team is suspicious of the existing software and databases due to the level of criminal activity that was uncovered during the police investigation into money laundering.

The M&A team also reviewed the inventory of digital assets (HW/SW/Licenses) included in the purchase of Island Banking Services. The team also reviewed existing contracts for services related to those assets. It has determined:

1. **Telecommunications**. Undersea fiber optic cables connect the island to the global Internet. These cables are managed by a consortium of companies that contract with national and regional governments to provide telecommunications services (voice, video, and data) to a country or region. On-island access to Internet, cable television, and land-line telephone service are provided to residents and businesses on a contract basis by a government owned Communications Services company. The island’s local communications infrastructure was upgraded to buried fiber optic cables providing broad-band service after a hurricane destroyed the previous above ground copper cable infrastructure. Island Banking Services’ contract for communications services includes Voice over IP telephone service, one physical telecommunications connection via fiber optic cable, and one static IP address associated with that connection. Domain name services for the company’s Internet presence are provided by the island’s Communications Services company. The company uses network address translation services provided by the premises router to assign internal IP addresses to workstations and servers.
2. **Network Equipment**. The network equipment is more than five years old and should be replaced. Since the company is moving PBI-FS’s operations to a new physical location, the entire network infrastructure from cables to routers to firewalls to wireless access points will be replaced. The network equipment closet also contains a special purpose access control system that uses hard wired RFID badge readers and RFID badges to control employee access to exterior and interior doors. This equipment is out of date and will need to be replaced once the company moves.
3. **Workstations**. The computer workstations are more than five years old and currently run Windows 8.1. The workstations were custom built using refurbished components. All copies of Windows have an OEM license installed.
   1. Licenses for Office 2019 were included in the purchased assets.
   2. Three business licenses for an anti-virus program were included in the purchased assets. These licenses were installed on computers that were seized and taken into evidence as part of the ongoing law enforcement investigation. It is unclear whether these licenses will be usable in the future.
   3. More than 10 computer workstations were found to be using “free” versions of an anti-virus application. These licenses state “for non-commercial or personal, home use only.”
4. **Banking Applications Database & Servers (Hardware & Software)**. The current banking applications software uses a custom browser-based interface built on an Apache Web server connected to a MySQL database. The Apache Web server also hosted the company’s internal web site. The server software licenses, the code for the custom browser-based interface, and the web server and database server hardware were included in the purchased digital assets. The storage media (hard disk drives) containing the Linux operating system, applications software, and database files were seized as part of the investigation and have not yet been returned to the company.
5. **Electronic Mail and Public Web Server**. At the time of purchase, Island Banking Services was in the middle of converting from an internally hosted email server based on Linux/Exim to individual Gmail accounts (not owned or managed by the company). The company had recently moved its public website from the internal Apache server to the Wix hosting service. This public website provides customers with access to the company’s custom built, web-based mobile banking services application.
6. **Data Backups and Data Recovery Services**. The system administrator for Island Banking Services used a commercial image backup utility to manually backup the company’s servers on a weekly basis. The image backups were written to multiple Solid State Disks (SSDs) that were connected to a Linux server connected to the company’s internal network. The financial transactions software (custom written) used electronic journaling to create copies of each transaction record in a MySQL instance hosted in a private cloud (Platform as a Service). The entire transactions database was copied to this private cloud once every 12 hours. Transaction records were copied to the cloud database every 30 minutes.



**Figure 1. Island Banking Services IT Infrastructure (as-is).**

## Putting It All Together

Your plan will be a combination of a paper and a detailed list of steps and resources that you would follow to implement and complete this project. Think about all of the actions, resources, and tasks that you would need to ensure a successful implementation of the “to-be” state for the PBI-FS cybersecurity program and infrastructure. These should also be included as part of the plan. The minimum structure for this assignment is below:

* INTRODUCTION
  + Purpose of Plan (implementation of the security strategy)
* GOALS AND OBJECTIVES
  + Business Goals and Objectives
  + Project Goals and Objectives
* SCOPE
  + Scope Definition
  + Items Beyond Scope
* ASSUMPTIONS
  + Project Assumptions
* CONSTRAINTS
  + Project Constraints
  + Barriers to Success
* PROJECT MANAGEMENT PLAN (for implementation of the security strategy)
  + People
  + Processes
  + Technologies
* STRATEGY IMPLEMENTATION
  + Security Controls
    - Baseline (mandatory controls)
    - Compensatory Controls (Administrative, Operational, Tactical)
  + System Development Life Cycle/Schedule
    - The 7 phases are: planning, requirements, design, development, testing, deployment, and maintenance
  + Milestones
  + Resource Requirements (People, Finances)
* ENTERPRISE IT ARCHITECTURE (“To-Be” – must include overview diagram)
  + Hardware
  + Software
  + Network Infrastructure
  + Cybersecurity Defenses

## Additional Information

1. Consult the grading rubric for specific content and formatting requirements for this assignment.
2. Your 10-12 page Implementation Plan should be professional in appearance with consistent use of fonts, font sizes, margins, etc. You should use headings and page breaks to organize your paper. The listed page length is a recommended target. You should not, however, exceed double that page count (i.e. no more than 25 pages including diagrams, tables, and lists).
3. Your deliverable should use standard terms and definitions for cybersecurity. See Course Content > Cybersecurity Concepts Review for recommended resources.
4. Your Enterprise IT Architecture Overview diagram may be constructed using commercial clip art but you may not copy / glue together architecture diagrams from other sources. MS Word and Power Point both provide drawing tools and clip art which you can use to construct your diagram. See Figure 1 in this file for an example of the type of diagram / level of detail required.
5. The CSIA program recommends that you follow standard APA formatting since this will give you a document that meets the “professional appearance” requirements. APA formatting guidelines and examples are found under Course Resources. An APA template file (MS Word format) has also been provided for your use CSIA\_Paper\_Template(TOC+TOF,2021).docx.
6. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be on a separate page at the end of your file. These pages do not count towards the assignment’s page count.
7. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
8. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.). Note: you may use footnotes to credit sources when doing so will improve the readability of the deliverable.