Information Assurance and Risk Management Program Design for a Property and Casualty Insurance Organization

John Richardson

A WGU Capstone Project

1 November 2020

Table of Contents

EXECUTIVE SUMMARY

Problem Statement:

The Board of Directors directed Amarci Insurance, Inc. (hereafter referred to as “Amarci”), to perform an audit addressing six primary areas and develop a Risk Management program that identifies and designs an Information Assurance and Risk Management program that addresses “the probable frequency and probable magnitude of future loss of confidentiality, integrity, availability, or accountability” (Wheeler, 2011). The six areas the audit review team addressed were:

1. Determine the existence of documentation such as an Information Security Policy, Acceptable Use Policy, etc.
2. Perform a system inventory audit and a risk analysis of the systems and processes
3. Define organizational risks and the controls that mitigate the risks identified in step 2 either through Risk Mitigation, Risk Transference, Risk Acceptance, or Risk Avoidance (Harris, 2013)
4. Identify tools and procedures for such activities as vulnerability assessments and patch management processes to address the risks
5. Establish Key Performance Indicators (KPIs) metrics for security and infrastructure
6. Determine how each of the areas address Confidentiality, Integrity, and Availability with acceptable Risk Appetites

The Information Technology (IT) team was tasked by Amarci’s General Manager with spearheading the review and with developing and executing a plan to address the gaps. The results of the analysis were that the company:

1. Lacked any formal Policy, Standard, or Procedure that addressed Risk Management
2. No prior Risk Assessment reviews or system audits had been performed
3. There were no identified and documented risks, risk scenarios, or mitigating controls
4. There were no tools in place to perform vulnerability assessments or for enterprise patch management.
5. There were no KPI metrics being reported

Background:

Amarci, an insurance company that provides Property and Casualty insurance to both residential and commercial customers, recently experienced massive growth in clients following a competitor deciding to no longer offer insurance in the same market. As such, the Board of Directors sought to determine whether or not the organization had an effective Risk Management program that was designed to adapt and provide a proper custodial obligation and Due Diligence and Due Care concerning customer private information as well as to the organization that ensures suitable handling of corporate trade secrets which are primarily the unique software designed by Amarci to provide a competitive edge in handling claims with 97% satisfaction rate. Following the latest Board meeting in the 3rd quarter, the Board of Directors directed the company to undergo a thorough internal review of the Information Assurance and Risk Management Program and to design a project to address any identified gaps as a result of the review.

Amarci's goal was to have a Risk Management Program that ensured Due Diligence and Due Care were always performed to protect the private and confidential data with consideration for Confidentiality, Integrity, Availability, and Accountability. The project followed the Waterfall method of Project Management and the Program Development Lifecycle (PDLC) with seven key deliverables within five defined milestones:

1. Develop the necessary Security Policies, Standards, and Procedures
2. Perform an asset inventory and perform a risk assessment of each system
3. Deploy an approved patch management system (Dell KACE 2000) with approved maintenance windows
4. Deploy Nessus as a vulnerability management system as well as GFI Languard for an alternate tool to supplement Nessus and the patch management tool
5. Establish a formal process using company personnel to perform penetration tests
6. Create a set of infrastructure controls using COBIT 2019 and NIST 800-53r5 that mitigate the risks and vulnerabilities identified in steps 2, 3, and 4 above
7. Develop the key security metrics for Executive management and the Board

A formal, robust Information Assurance and Risk Management Program is imperative for any organization to ensure that data is properly classified and that the systems on which it resides or is processed have undergone a proper certification and accreditation process to include Risk Assessment, Vulnerability Assessment, has a well-regulated patch management system, and is regularly evaluated for continued compliance with the chosen technical and administrative controls.

By performing a Gap Analysis, the final result of the program was a fully formed, well-designed Information Assurance and Risk Management program that possessed well-documented procedures evidenced through metrics that supported the effectiveness of the program and tools that displayed repeatable and automated processes for protecting the data and the systems.

This paper lays out the analysis of the systems, provides a list of the frameworks and best practices that were leveraged to define the program, the analysis, proof-of-concept, acquisition, configuration, and deployment of the tools chosen for risk assessments, a Governance, Risk, and Compliance documentation methodology, vulnerability assessment and patch management procedures, the KPIs reported to show the security stance and trends of the program and lays out the project management framework with deliverables and tasks that were used to successfully deliver the final Information Assurance and Risk Management Program. Finally, this paper also identifies the new risks that exist as a result of the new technologies and ends with a list of future projects designed to continue improving the process.

As an insurance organization, Amarci is required to comply with the Gramm-Leach-Bliley Act (GLBA). The main components from GLBA that Amarci is required to address as part of the Information Assurance and Risk Management program fall under Section 501B which identifies these three high-level control objectives: (Davis, 2011)

1. “Ensuring the confidentiality of customer financial records”
2. “Protecting against anticipated threats against customer records”
3. “Protecting against unauthorized access to customer information that could result in substantial impact to the customer”

The project was initiated on Friday, 23 October 2020, and concluded on Friday, 15 January 2021.

Root Cause Analysis

The company used the IT Operations staff to lead the self-audit, perform a gap analysis, work with the business to capture any Business Impact Analyses, and to identify business-critical systems and data, and when the review had been completed to design and execute a plan to address the findings. This review team (hereafter referred to as “the audit review team”) consisted of the following personnel:

- IT Manager: John Richardson, CISSP PMP CEH CHFI MCSE
- Senior Network Engineer: Michael Fruthy, CCNP
- Senior Systems Engineer: Michael Williams, MCSE
- Senior Database Architect: Vickie Avers, MCDBA OCP
- Senior Developer: Robert Duga, OCMJEA

The findings as a result of the analysis were that the company lacked any formal Policy, Standard, or Procedure that addressed Risk Management, the servers had not had any risk assessment review performed, and there were no tools in place to perform vulnerability assessments or for enterprise patch management. Additionally, there was no established method for clear procedures for classifying data as Private, Secret, Confidential, or Public.

Through interviews with the key leaders of each of the business units, the audit team determined that people failing to follow best practices with Information Assurance and Risk Management were ultimately the root cause for the lack of proper processes and documentation. There was a lack of direction from the Board of Directors to establish an Information Security or Risk Management program. The General Manager and the business units also relied on the company being small and not of key interest to potential threat actors as well as an informal reliance on each of the technology teams to “just do what is right and expected.”

Stakeholders:

As part of the review process, the review team determined that there were five primary groups of stakeholders:

- Clients, both residential and commercial: These are the customers who rely upon the services offered by the company and whose data it is imperative to protect

- The Board of Directors: These are the individuals collectively responsible for ensuring that the proper policies are in place to direct the company in Due Diligence and Due care concerning data protection
- The General Manager: This is the individual who is responsible for ensuring that the requirements set forth by the Board are translated into the orders given to each of the organizational business units for data classification, data protection, Risk Management, etc.
- The Executive Staff: Chief Financial Officer (CFO), Chief Operations Officer (COO), Chief Marketing Officer (CMO), Chief Information Officer (CIO): These are the key persons responsible to the General Manager and the Board for ensuring that the proper Standards and Procedures are written and published for performing Due Care for implementing, managing, and monitoring an effective Information Assurance and Risk Management program
- Business Units: Claims, Underwriting, Operations, Information Technology (Operations, Development, Project Management): These are the collective whole who will write the Procedures, establish the Risk Management Program, and ensure operational goals are set and adhered to for alignment to and compliance with the established Risk Management program

Each stakeholder group, except for the Clients, were key in the review process and responsible for completing their specific parts such as Data Classification, Asset Classification, Risk prioritization, Business Impact Analyses (BIA), and Service Level Agreements (SLA) to include Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Maximum Tolerable Downtime (MTD). They were also responsible to each of the other groups for providing input into the Information Security and Risk Management Program. Finally, Amarci as an organization is ultimately responsible to the client for protecting their private data as well as to the Board for the protection of company Secret and Private data.

Analysis of Systems and Processes:

There were several assumptions made concerning the project:

1. The Board and Executive Management were fully supportive of the project and would communicate their support to the company
2. The necessary business members would be available for the interview process for tasks like the Business Impact Analysis, System and process prioritization, and Data Classification

3. The budget would be available to purchase necessary systems and tools as well as training

To approach the project logically, the audit review team broke the review into two primary areas:

1. Review of the processes, including Policies, Standards, and Procedures
2. Review of the systems, including tools, assessments, etc.

Processes:

The IT Manager was responsible for reviewing the Policies, Standards, and Procedures and working with the Board, the General Manager, and the top Business Units' leadership to determine where the gaps existed and to author, get approval on, and publish any necessary documents. As a result of the gap analysis, the IT Manager determined that there were effectively no documents to address the Information Assurance or Risk Management program. The documents that were written as a result of the project are identified and detailed in this section below.

The technology Subject Matter Experts (SME), the Sr. Network Engineer and Sr. Systems Engineer, found that the processes and controls in place lacked any alignment with or compliance to industry Best Practices frameworks such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53r5 (National Institute of Standards and Technology, 2020), OWASP Top 10 (OWASP, 2020), COBIT 2019 (COBIT, 2020), or the Center for Internet Security (CIS) Top 20 Controls (Center for Internet Security, 2020).

Systems:

The network and systems engineers as well as the database administrator and lead developer were responsible for reviewing the systems for secure coding, effective hardening, proper controls to mitigate risks and address vulnerabilities, and for the protection of private and secret data. The team determined that while the right controls were essentially performed, though not documented in a Governance, Risk, and Compliance (GRC) or Risk and Control format. The team further found that the process lacked the performance of any Threat Modeling activities for the systems and risk scenarios to determine the Inherent Risk, likelihood, magnitude of impact, mitigating controls, or to determine the Residual risk.

The team identified the following gaps:

- There was no automated patch management system

- There was no vulnerability assessment system or process
- The asset management process was manual and laborious with a high degree of potential failure
- There have been no risk assessment activities performed on the systems
- There was no (GRC) system for documenting and tracking Risk Mitigating efforts
- There was no listing of controls identified for the systems and no references to risks being addressed

Project Requirements:

After the audit and interviews were concluded, the audit review team identified seven key components that would be necessary to establish and deploy an effective Information Assurance and Risk Management program. The seven items that were critical to the success of this project are listed below. There were additional items recommended for subsequent projects and are briefly highlighted following these seven areas.

In-Scope

1. Develop the necessary Security Policies, Standards (See Appendix B for the System Security Standard), and Procedures
2. Perform a full Asset Inventory
3. Deploy an approved Patch Management System (Dell KACE 2000) with approved maintenance windows
4. Deploy Nessus as a Vulnerability Management system as well as GFI Languard for an alternate tool to supplement Nessus and the Patch management tool
5. Establish a formal process for performing penetration testing utilizing company personnel
6. Create a set of infrastructure controls using NIST 800-53r5
7. Develop key security metrics for Executive management and the Board

During the review, there were some additional areas identified as necessary to improve upon the delivered Information Assurance and Risk Management Program that is not in scope for this project but will be completed through future projects.

Not In-Scope

1. Establish a formal Enterprise Architecture framework using TOGAF

2. Development of a Chief Compliance Officer role
3. Development of a Chief Risk Officer role
4. Formation of an Internal Audit department
5. Development of an Oversight Group
6. Implement a formal Change and Release Management program
7. Establish a Risk Management Office
8. Establish an automated Vulnerability Assessment, Patch Management, and Risk Management process with a Test Environment and scripting processes using an Automated Build process, either in GO or Jenkins with a manual checkpoint for promotion into production
9. Implement a Security Information and Event Management system, e.g. AlienVault OSSIM
10. Formalize a Risk Modeling process such as FAIR, STRIDE, OCTAVE, or DREAD as a standard risk evaluation methodology using Qualitative and Quantitative measurements
11. Develop a Business Continuity and Disaster Recovery procedure and plan

Data Collection for Gap Analysis to support the project

The Audit team identified early on in the project that the organization lacked any policies, standards, or procedures upon which to build a more complete repository of documents. As such, the teams looked outside of the organization to identify the proper frameworks that would be needed to form the foundational Best Practices of the program. The IT Manager also reached out to various peers at similar organizations as well as to peers in other industries to find out what kinds of processes they used to develop or manage their programs. The following sections capture the results of this research and form the method that Amarci used to establish the Information Assurance and Risk Management program that was made operational on 15 January 2021.

Industry-standard methodology for managing the project:

The Audit Review team determined that the framework for managing the project which fit well with the project requirements was the Project Management International (PMI) Waterfall methodology (Project Management International, 2017) (see Appendix A for the Task timeline). The separate milestones had distinct deliverables with a linear progression. While Waterfall worked for the design and implementation

of the Information Assurance and Risk Management project, once the systems were deployed and operational, the project management methodology in operations would be Agile Project management.

As part of the design of the program, the Audit Review team, comprised of the various technical disciplines, determined that several Best Practice Frameworks would be leveraged to design, build, document, and implement a leading Information Assurance and Risk Management program. The key frameworks chosen to build the program around were:

1. Risk Assessments (NIST 800-30) (National Institute of Standards and Technology, 2020) that framed the methodology for performing the assessments
2. Managing Information Security Risk (NIST 800-39) (National Institute of Standards and Technology, 2011) that developed the key steps for managing the identified risks
3. Patch Management (NIST 800-40R3) (National Institute of Standards and Technology, 2020) that described the process and importance of a formal patch management process
4. Penetration Testing (NIST CSF v1.1) (National Institute of Standards and Technology, 2020) that determined the visibility of the company to external threat actors and to help identify and create proper controls for mitigating the risks and findings
5. Key Controls in COBIT 2019 (COBIT, 2020) that was used to help describe in greater detail the activities and practices expected in the specific compensating controls
6. Best Practices framework (NIST 800-53r5) (National Institute of Standards and Technology, 2020) that, with number 5 above, helped to define the practices for the compensating controls
7. OWASP Top 10 (OWASP, 2020) that helped to classify the critical controls for web-based application development
8. CIS Top 20 Controls (Center for Internet Security, 2020) that helped to identify the key areas to address around system protection and attention for Confidentiality, Integrity, Availability, and Accountability.

Deliverables

Upon completion of the audit review, the audit team determined that to meet the specific requirements for the gaps in the process, several key items were critical for delivery to guarantee a successful implementation:

- A Governance, Risk, and Compliance tool
- A Vulnerability Assessment tool
- A Risk Assessment process
- A Patch Management tool
- Documentation for processes and management

To elaborate on the last item in the list above, concerning documentation, the following Policies, Standards, and Procedures were written:

1) (ADMINISTRATIVE) Information Security Policy, including but not limited to the following sections:
    a) Purpose
    b) Audient
    c) Objectives
    d) Authority and Access control Policy
    e) Data Classification
    f) Data Support
    g) Security Awareness (with an Employee Training Standard)
    h) Responsibilities and duties of the staff
2) (ADMINISTRATIVE) Acceptable Use Policy, including but not limited to the following sections:
    a) Privacy and Personal Rights
    b) Social Media Posts
    c) Protection of Company equipment
    d) Internet Usage
    e) Downloading and installing unapproved software
    f) Unlawful or Inappropriate content
    g) Cyberbullying
3) (ADMINISTRATIVE) REMOTE USER ACCESS POLICY, including but not limited to these key sections:
    a) Virtual Private Network connection

b) Multifactor authentication

4) (ADMINISTRATIVE) RISK MANAGEMENT POLICY, including but not limited to these key sections:
   a) Performance of Threat Modeling
   b) Risk Assessments
   c) External Penetration Testing
   d) Vulnerability scanning and metrics
   e) Asset Management
5) (ADMINISTRATIVE) USER SECURITY AWARENESS AND TRAINING POLICY, including but not limited to these key sections (This training will apply to all users and will also include specific training for key roles):
   a) Specific roles: Data processor, Financial, Developer
   b) Risk awareness
   c) Industry-standard requirements
6) (ADMINISTRATIVE) DATA CLASSIFICATION POLICY, including but not limited to these key sections:
   a) Level of sensitivity
   b) Trade Secret
   c) Personal Health Information (PHI)
   d) Personal Identifiable Information (PII)
   e) Payment Card Information (PCI)
7) (TECHNICAL) PERIMETER NETWORK STANDARD, including but not limited to these key sections:
   a) Firewall
   b) Intrusion Prevention Systems
   c) DMZ Zone
8) (TECHNICAL) NETWORK INFRASTRUCTURE ARCHITECTURE STANDARD, including but not limited to these key sections:

a) Demilitarized Zone (DMZ)

b) Virtual Local Area Network (LAN) Segmentation

c) Payment Card Industry Data Security Standard (PCI-DSS) Zone

9) (TECHNICAL) PASSWORD STANDARD, including but not limited to these key sections:

a) Complexity

b) History

c) Length

10) (TECHNICAL) ENCRYPTION STANDARD, including but not limited to these key sections:

a) Data at Rest

b) Data in Motion

c) Acceptable encryption algorithms

d) Database Encryption

11) (TECHNICAL) SERVER HARDENING STANDARD (with a separate Procedure that will be the specific details for the process), including but not limited to these key sections:

a) Malware Protection

b) Disabling unused services

c) Intrusion Prevention

d) Encrypted storage for Non-Public Information, Personally Identifiable Information (PII), Secret, and Trademark data

e) Logging

12) (TECHNICAL) ENDPOINT PROTECTION STANDARD, including but not limited to these key sections:

a) Antivirus

b) Malware Protection

c) Full Disk Encryption

d) Updates and Patches

13) (TECHNICAL) NETWORK AND SERVER EVENTS LOGGING STANDARD, including but not limited to these key sections:

a) Central Logging Server

b) Alerts for events exceeding thresholds

c) Logon/Logoff events

d) Failed Login attempts

14) (TECHNICAL) CHANGE AND RELEASE MANAGEMENT STANDARD, including but not limited to these key sections:

a) Tracking

b) Change Approval request

c) Development

d) Testing

e) Approval to release

f) Warranty period (for business to accept)

g) Certification and Acceptance

15) (TECHNICAL) ASSET MANAGEMENT STANDARD, including but not limited to these key sections:

a) Asset Management Database

b) Required Configuration Item details

16) (TECHNICAL) MOBILE DEVICE MANAGEMENT STANDARD, including but not limited to these key sections:

a) Purpose

b) Applicability

c) Responsibilities

d) Device Approval

e) Bring Your Own Device

f) Mobile Device Management application

17) (TECHNICAL) WIRELESS NETWORK ACCESS STANDARD, including but not limited to these key sections:

a) Restricted usage

b) Approved groups

c) Specific PCI-DSS restrictions against wireless access

d) Approved wireless protocol, enterprise authentication

Implementation Strategy

Amarci identified several outcomes to be delivered at the conclusion of this project:

1) That there will be formal, approved Policies, Standards, and Procedures that govern:
   a) Risk Assessments
   b) Vulnerability Assessments
   c) Patch Management
   d) Key metrics reporting through reports and dashboards
2) A formal Risk Assessment process will be in place to classify systems in the degree of criticality, based on role and sensitive data that it contains or processes
3) A formal Vulnerability Assessment process to identify and prioritize vulnerabilities that make a system prone to negative impacts on Confidentiality, Integrity, or Availability
4) A formal patch management process to mitigate known vulnerabilities per company SLA requirements.
5) A Risk and Control process that identifies weaknesses in systems and develop formal controls that aid in mitigating the level of risk to a degree that falls within the organizational risk tolerance levels.

There were five major milestones with aggressive timelines established for this project (See detailed tasks for each milestone in Appendix A). The five milestones were:

- Milestone 1 - Creation of Policies, Standards, and Procedures (Begin 23 Oct 2020, End 15 Jan 2021)
- Milestone 2 - Asset Inventory and Risk Assessment process (Begin 26 Oct 2020, End 11 Dec 2020)
- Milestone 3 - Patch Management System (Begin 26 Oct 2020, End 27 Nov 2020)
- Milestone 4 - Vuln Assessment system (Begin 26 Oct 2020, End 27 Nov 2020)

- Milestone 5 – Governance, Risk, and Compliance and the identification of the KPIs and the creation of the dashboard for reporting the metrics (Begin 26 Oct 2020, End 24 Dec 2020)

The project kick-off meeting was held on Monday, 19 October 2020 with the primary stakeholders, except for the clients, in attendance. During the kickoff meeting, the tasks and milestones were discussed in detail and it was also explained to each of the leaders in the meeting that the success of the project depended on their involvement. This was reiterated by the representative from the Board of Directors as well as Amarci's General Manager.

The technical training requirements for this project were narrow in scope, limited to the IT Operations staff who are responsible for implementing and managing the tools. As part of the process, IT Operations requested and received funding for training on the new vulnerability and patch management systems. The Sr. Systems Engineer attended the Patch Management training, and the Sr. Network Engineer attended the Vulnerability Assessment Training. Upon their return, each member who attended training was required to then train the rest of the staff on the use of the tools. The non-technical training needed was in the Risk Assessment process. The training for this process was an informal process of working with the business leaders to develop a process for performing Business Impact Analyses and proper identification and classification of data.

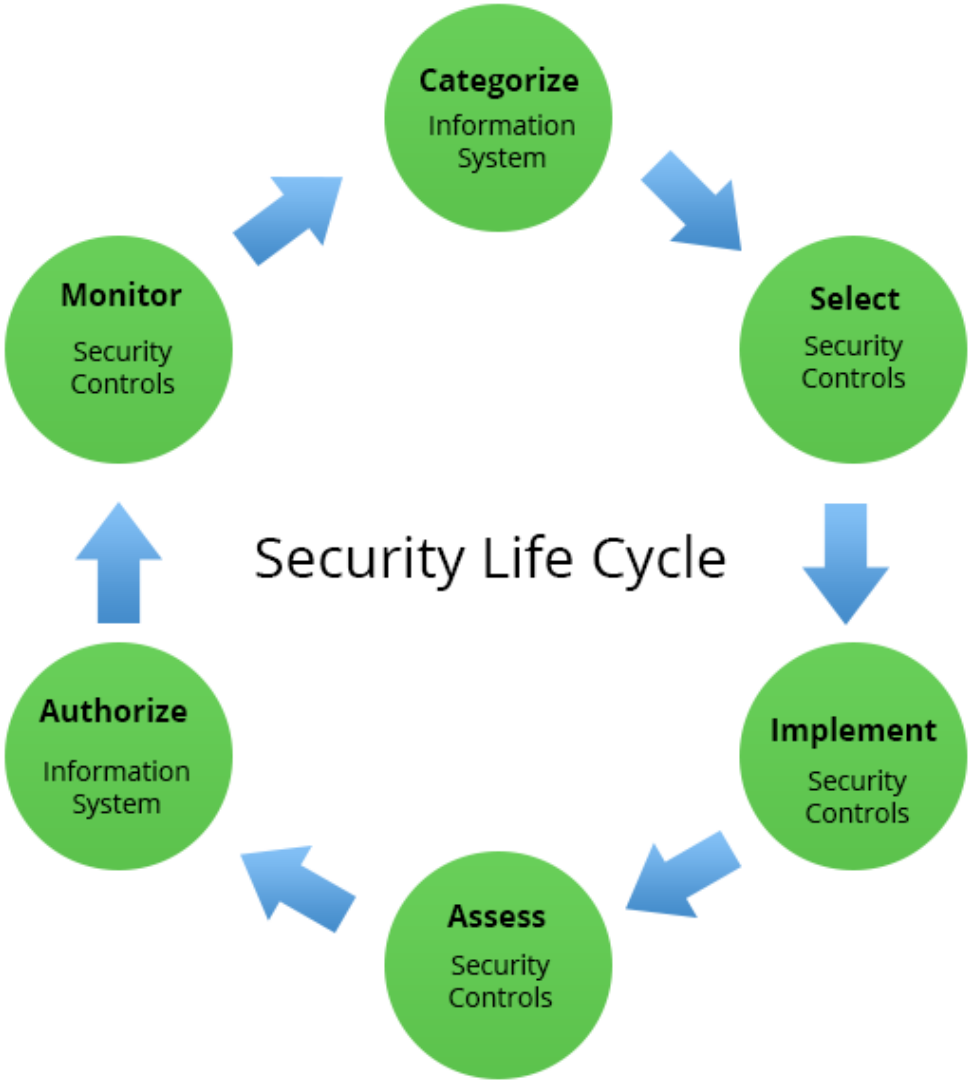
PROJECT IMPLEMENTATION QUALITY ASSURANCE PLAN

Due to the nature of the project and the importance of ensuring that key elements of data protection, risk and vulnerability assessments, patch management, and system security controls were all properly addressed in the end product, the following details outline the process that was established and followed for performing quality assurance checks through the project design and implementation phases and throughout the System Security design lifecycle.

Foundational to any security system is understanding the lifecycle of the process from the Categorization of the systems through to the monitoring phase, in an iterative process. The following image identifies the six primary phases of the lifecycle. These steps were critical in outlining and building the quality assurance plan.

The image below represents the Security Life Cycle.

Image 1: Security Life Cycle (C4 Planning Solutions LLC, 2020)



The five major milestones were used to delineate the division of areas for the Quality Assurance process and performing the checkpoint Go-Live actions for completion of the milestone.

1. Milestone 1 - Creation of Policies, Standards, and Procedures
    a. Formative Evaluation Plan: During the creation of each Policy, Standard, or Procedure, there were initial and ongoing meetings with the primary stakeholders and impacted areas. This assured accuracy, clarity, and applicability of the documents before final sign-off and publication.

i. Key teams providing input: Business process owners, IT Manager, Sr. System and Sr. Network Engineers

b. Summative Evaluation Plan: Once the documents were created, each business unit leader was responsible for reviewing the final document and then approving the document for publication or sending it back for additional clarification.

i. Key evaluation questions:

1. Does the document accurately reflect the key elements of the requirement, e.g. Does the standard identify the components of Who, What, When, and Why or other critical elements as applicable?
2. Does the business unit agree with and identify the components of the document for applicability to their area?
3. Does the document reference the elements that are pulled from best practice frameworks such as NIST 800-53r5 or COBIT 2019?

c. Revision process: The process for revision was an iterative process to develop the document. After approval of the final document for publication, it was established that each document would undergo an annual review (or following major changes in the environment) process for approval, updated as necessary, and re-publication.

2. Milestone 2 - Asset Inventory and Risk Assessment process

a. Formative Evaluation Plan: The Sr. Network and Sr. Systems engineers, along with the IT Manager, reviewed the current asset inventory system which was maintained in a simple spreadsheet.

i. Key teams providing input: Business Process Owners, IT Manager, Sr. System and Sr. Network Engineers

b. Summative Evaluation Plan: During the iterative development of the enhanced spreadsheet to capture additional configuration items such as serial numbers, hardware components, installed software, etc. the IT Manager and his two Sr. Engineers performed system reviews and on-site audits of the environment to ensure that the spreadsheet

accurately reflected the systems. The following questions were covered during every iteration of the process.

i. Key evaluation questions:

1. Are all of the systems in the environment accurately captured in the asset management system?
2. Does the Threat Model process reflect the major elements?
    a. Asset value
    b. Inherent Risk rating
    c. Asset vulnerability
    d. Threats
    e. Controls
    f. Residual Risk rating

c. Revision process: The process for revision of the inventory was determined by performing both a comparison of the items as tracked on the initial spreadsheets with the information captured in the enhanced spreadsheets. This was cross-checked with a visual inspection as well as by speaking with each of the departments to ensure no shadow systems were being used. The revision of the Risk Assessment occurred organically through table-top reviews and the key items from STRIDE, (Spoofing Identify, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) (Stallings, 2019). As areas were clarified and more data were available, the documentation and process incorporated the changes either into the asset inventory system or into the Risk Assessment model.

3. Milestone 3 - Patch Management System

a. Formative Evaluation Plan: The quality assurance for this phase of the project included performing a comparative analysis of available tools to determine specifications and features. This evaluation allowed for a determination as to the ability of the tool to meet the needs of the business.

i. Key teams providing input: IT Manager, Sr. System and Sr. Network Engineers

b. Summative Evaluation Plan: The quality assurance for this component of the project included a limited Proof of Concept where a small portion of the QA test environment was grouped into the assets inventory of the application and patches were automated for deployment. This allowed the Sr. Network and Sr. Systems engineer to validate the Fit for Purpose and Fit for Use of the process for recommendation to fully deploy.
    i. Key evaluation questions:
        1. Are all of the assets identified in the chosen Patching technology?
        2. Is the system configured for automated scans for patch status?
        3. Is the system configured to deploy approved patches at the scheduled intervals?
        4. Is there a defined process for checking systems for patch success?
        5. Is there a documented process for correcting any findings where patches did not successfully deploy?

c. Revision process: The established process for revision, should it have been needed, was to work with the Technical Account manager and vendor SMEs to work through any issues. Amarci also established an annual review of the application along with a recurring vetting of new tools based on Gartner's Magic Quadrant for similar products to ensure the chosen tool still meets the needs of the organization.

4. Milestone 4 - Vulnerability Assessment system
    a. Formative Evaluation Plan: The quality assurance for this phase of the project included performing a comparative analysis of available tools to determine specifications and features. This evaluation allowed for a determination as to the ability of the tool to meet the needs of the business.
        i. Key teams providing input: IT Manager, Sr. System and Sr. Network Engineers
    b. Summative Evaluation Plan: The quality assurance for this component of the project included a limited Proof of Concept where a small portion of the QA test environment was grouped into the assets inventory of the application and vulnerability assessment scans

were automated with report generation. This allowed the Sr. Network and Systems engineer to validate the acceptability of the process for recommendation to fully deploy.

i. Key evaluation questions:

1. Are all of the assets identified in the Vulnerability Assessment technology?
2. Is the system configured for automated vulnerability scans?
3. Is the system configured to determine vulnerability scans based on the Common Vulnerability Scoring System and customized for variances based on organizational risk assessments and determinations?
4. Is there a defined process for automated opening of tickets based on pre-defined findings, e.g. all findings with a CVSS score 7 and higher?
5. Is there a documented process for sending scan results to key IT staff members, IT Manager, Sr. Network Engineer, and Sr. Systems Engineer?

c. Revision process: The established process for revision, should it have been needed, was to work with the Technical Account manager and vendor SMEs to work through any issues. Amarci has also established an annual review of the application along with a recurring vetting of new tools based on Gartner's Magic Quadrant for similar products to ensure the chosen tool still meets the needs of the organization.

5. Milestone 5 – Governance, Risk, and Compliance

a. Formative Evaluation Plan: This phase included the deployment of the Practical Threat Analysis tool, the Risk Assessment of each system, the development of the Administrative, Technical, and Physicals Controls applicable to the organization for the protection of the data and systems.

i. Key teams providing input: Business process owners, Sr. System and Sr. Network Engineers

b. Summative Evaluation Plan: The following questions were asked during the Proof of Concept and any exception, variance, or non-compliance with the stated desired outcome was addressed and adjusted accordingly.
    i. Key evaluation questions:
        1. Are all key Risks and Controls entered into the system?
        2. Is there a key business owner and key technology owner named for each asset, risk, and control?
        3. Is there a security rating identified for each control?
        4. Are the key elements of the control, e.g. Preventive, manual, quarterly, documented?
        5. Is there a required period for review and attestation and certification of the controls?
c. Revision process: If the technology did not contain at least the five items listed in the Key evaluation plan, then the business and technology owners were notified of the missing elements. Sign-off was not provided until all of the identified controls were documented with enough information to ensure Due Diligence and Due Care were supported.

Assessment of additional or new risks associated with the implementation

The audit team implemented as part of the tasks associated with each phase of the overall project a review process to identify potential risks as well as the requirements for Fit for Use and Fit for Purpose sign-off with each phase in the beginning. By implementing this task, the audit review team, implementation teams, and management were aware of the potential risks. Before a project phase was signed off, the audit review team performed a pre-close review with key stakeholders to determine if any of the potential risks had occurred and, if so, were the risks appropriately addressed and mitigated accordingly or if the business had to make a Risk Treatment determination to accept, avoid, transfer, or implement compensating controls to bring the risk within acceptable risk tolerance levels.

After the project, the audit review team, created a Risk Register to identify, document, and monitor all of the inherent and residual risks. The result of the project is that the design and

implementation of each phase of the project completed with minimal risk, and all residual risk fell within acceptable risk tolerance levels as determined by the Board of Directors and the Executive Management.

An example of the risk register that was created is shown below

Image 2: Amarci Risk Register example

Effects of Sample Treatments on Scoring in the Risk Register

			Inherent Risk				Residual Risk		
	Risk Item	Rationale for Inherent Risk	Likelihood	Impact	Risk Score	Risk Treatment	Likelihood	Impact	Risk Score
Accept the risk →	Laptops break down during their useful lives.	x% printer replacement cost attributable to replacements made ahead of schedule.	1.0	1.0	1.0	Scheduled replacement precludes the need to extend laptop lives. Accept the risk of the cost of premature failure and replacement.	1.0	1.0	1.0
Reduce the risk →	Injuries incurred during operations.	x% accident rate with $y annual cost of claims.	3.0	2.0	6.0	Develop and implement tested, proven safety protocol X.	2.0	1.0	2.0
Reduce the risk →	A major supplier fails to deliver materials	X% of raw materials purchases concentrated in a single supplier.	4.0	3.0	12.0	Spread raw materials purchases over x suppliers with no more than y% of purchases concentrated in any one supplier.	1.0	3.0	3.0
Transfer the risk →	The organization experiences a flood.	Property coverage excludes flood coverage.	3.0	3.0	9.0	Extend property insurance to provide coverage for floods. (Residual impact is the additional premium.)	3.0	1.0	3.0
Transfer the risk →	Extra costs incurred due to installation difficulties.	Annual costs of $x for installation remediation and $y for installation administration.	3.0	3.0	9.0	Outsource installation service. (Residual impact is the outsource cost.)	2.0	1.0	2.0
Avoid the risk →	A new product does not prove to be profitable.	Anticipate x% market penetration for $yy revenue versus $YY operational cost and $ZZZ capitalized cost.	5.0	4.0	20.0	Do not develop the product.	0.0	0.0	0.0

The following risks are those that were created and identified after the program was delivered and made operational. As part of the Risk Assessment, they were entered into the Risk Register, into the GRC tool, and controls were established to mitigate the risks to acceptable levels.

1. The new process of classifying the systems based on the data contained therein could be inappropriately classified, leading to either too little or too many security controls being implemented
2. Procedures would change organically over time and those changes would not be reflected in the documentation
3. With staffing changes, the tools that were deployed would no longer be effective due to skill sets
4. Without appropriate checks and balances of oversight, controls could potentially be considered as effective through self-assessments due to a lack of a critical internal validation review process
5. Future Threat Modeling could not incorporate accurate and realistic Risk Scenarios
6. Basic penetration tests performed by staff could be insufficient and not identify key vulnerabilities

7. Basic penetration tests performed by staff could result in actual damage to the systems if not performed safely and correctly

Required technology environments, tools, costs, staff:

The following items identify the task, necessary tools, environment, costs, and staff needed to successfully execute each portion of the project

1. Developed Security Policies, Standards, and Procedures (PCI Security Standards, 2020)

   Tools: No tools were required for the phase of this project. A future project will be established to develop a central document storage environment, such as SharePoint, Confluence, or some other similar system.

   Environment: No special environment was required for this phase of the project

   Cost: No cost

   Staff: The creation of the Policies and Standards required input from the General Manager and the Board of Directors for content approval. The Procedures were written by the Subject Matters from each of the areas to ensure proper alignment with the Best Practice Frameworks

2. Performed a full Asset Inventory (Center for Internet Security, 2020)

   Tools: Amarci tracked system inventory in a set of Microsoft Excel spreadsheets. While out of scope for this project, a future project will be initiated to implement an asset inventory system that will perform automatic discovery and track specific configuration items such as serial number, Operating System, Security Level, etc. For this project, the team enhanced the spreadsheet to add additional configuration items to help classify the systems correctly according to value, data, risk, etc.

   Environment: No special environment was required for this phase of the project

   Cost: No cost

   Staff: The Sr. Systems Engineer and the Sr. Network Engineer performed an asset inventory in their respective environments

3. Deployed an approved Patch Management System (Dell KACE 2000) with approved maintenance windows (National Institute of Standards and Technology, 2020)

   Tools: Purchase of the Dell KACE 2000 appliance

Environment: Data Center access, rack space availability, networking and power capabilities

Cost: $20,000

Staff: IT Manager, Sr. Systems Engineer

4. Deployed Nessus as a Vulnerability Management system as well as GFI Languard for an alternate tool to supplement Nessus and the Patch management tool

   Tools: Purchase of Nessus and GFI Languard software

   Environment: 2 virtual machines to host each system

   Cost: Nessus $3,000/yr. / GFI Languard $1,600/yr. (100 licenses at $15.99 ea.) (Tenable, 2020) (GFI Languard, 2020)

   Staff: IT Manager, Sr. Systems Engineer, Sr. Network Engineer

5. Established a formal process for performing penetration testing utilizing company personnel

   Tools: The tools required are freely available for download. The tool chosen by the organization was Kali Linux.

   Environment: The tool was installed as a virtual machine on the laptops of the IT Manager, the Sr. Network Engineer, and the Sr. System Engineer

   Cost: No Cost – Open-source

   Staff: IT Manager, the Sr. Network Engineer, and the Sr. System Engineer

6. Created a set of infrastructure controls using NIST 800-53r5 and COBIT 2018 (National Institute of Standards and Technology, 2011)

   Tools: NIST 800-53r5 for the framework, COBIT 2019, and PTA Technologies Practical Threat Analysis software

   Environment: The tool was installed as a virtual machine

   Cost: No cost – Open-source

   Staff: IT Manager, the Sr. Network Engineer, and the Sr. System Engineer who partner with the key stakeholders to document and input risk and controls

7. Developed the key security metrics for Executive management and the Board

   Tools: Metrics were built to be pulled from the various tools, PTA, KACE, Nessus, GFI Languard and imported into the chosen dashboard

Environment: Tableau Dashboard was already deployed in the company and was leveraged for displaying the metrics

Cost: No Cost

Staff: IT Manager, the Sr. Network Engineer, and the Sr. System Engineer

Projected timeline for project completion

See Appendix A below for the project breakdown

Framework to assess the success

The success of the project was predicated on two key elements:

1. Did the Board approve of the Policies, Standards, Procedures, Controls, and Processes put in place to define the Information Assurance and Risk Management program?
2. Did the chosen technologies, KACE for patching, Nessus for vulnerability assessments, PTA for the GRC components move the organization to a better awareness of data value and amount of residual risk with an automated, and documented Information Security posture and provide the business with actionable details to remediate any findings where security may be adversely impacted?

The Board was provided with the project plan before initiation and they provided their approval to move forward with the project as designed.

Feedback and buy-in from the key stakeholders for each portion of the project were instrumental in ensuring that the new processes provided value to the business in the manner of performing proper data custodial activities for protecting corporate and client private and secret data secure, confidential, and with integrity.

Test cases for the project included the Proof of Concepts, the initial asset identification, vulnerability and risk assessments, and patch management.

The applications were certified and accredited by the IT Manager as Fit for Purpose and Fit for Use. The Policies were reviewed and approved by the Board of Directors and the General Manager. The Standards were approved by the Business Unit leads, and the Procedures were reviewed and approved by the IT Manager.

PROGRAM DESIGN AND DELIVERY

The goal of the program was to build an Information Assurance and Risk Management Program which built a model program that easily integrated several key components of a security program:

- Compliance with Best Practices frameworks
- Effective Security Planning and Management
- Systems Security through vulnerability and risk awareness
- Documented, usable security and system metrics and trends

As Amarci initially had no documented security program, each of these elements wove together to improve and modernize the security assurance program that addressed the need to identify, define, document, administer, and monitor the key elements of the Security Lifecycle shown in Image 1 above.

Under direction from the Board and after a socialization meeting with the organization's key executive stakeholders, the program was validated for its benefit of developing a formal Information Assurance and Risk Management program that

1. had the client's data protection as a central tenet
2. protected the organization's trade secrets
3. addressed the concerns around Confidentiality, Integrity, and Availability

The General Manager and executives all agreed that the project was integral to the future success of the organization and supported the initiatives from a Top-Down approach.

The first step in the process was to decide upon which Best Practices Frameworks to develop the program around. Amarci was not relegated to being mandated to comply with any specific framework and therefore was able to develop a program that took several frameworks and merged them into a process that fit the needs of the organization. The following frameworks were chosen as foundational upon which to build the program:

1. Patch Management (NIST 800-40R3)
2. Risk Assessments (NIST 800-30 and NIST 800-39)
3. Penetration Testing (NIST CSF v1.1)
4. Key Controls (COBIT 2019 and NIST 800-53r5)

5. OWASP Top 10 (OWASP, 2020)
6. CIS Top 20 (Center for Internet Security, 2020)
7. PCI-DSS Controls (Future state) (PCI Security Standards, 2020)

Several applications and systems were also introduced into the program. These tools are identified below with their area and then are discussed briefly after the list.

1. Nessus (Vulnerability Assessments)
2. KACE 2000 (Patch Management)
3. Practical Threat Analysis (Threat Modeling and Controls [countermeasures])
4. KALI Linux (Penetration testing)

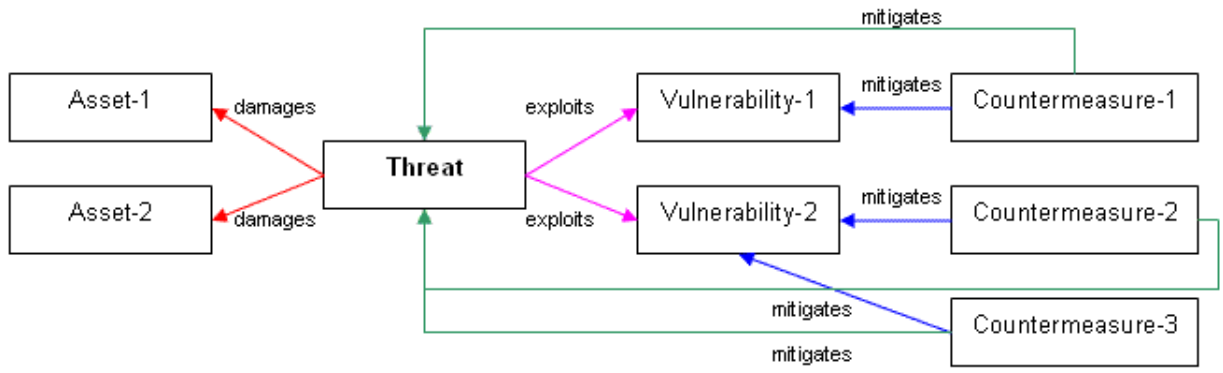
Nessus was chosen as the key vulnerability assessment tool for its ability to automate scans of systems for vulnerabilities and the ability to scan based on various compliance requirements, e.g. PCI-DSS. While Amarci currently does not accept credit cards as a form of payment, the Board did inform the team that it was considering accepting them in the future. Nessus was also chosen for its strength of reputation in the market as being a well-recognized tool and for having excellent support and training. The Sr. Network Engineer attended training and, in turn, trained other staff members in the configuration and use of the tool.

KACE 2000 was chosen as the tool for patch management for its ability to automate patch management based on attributes, system group memberships, and schedules. KACE provides reports that will be used to provide some of the metrics in the reports and Tableau dashboard to evidence compliance with the defined standards and security controls. The Sr. Systems Engineer attended training in the configuration and administration of the tool and, in turn, trained other staff members in the configuration and use of the tool.

KALI Linux was chosen as the tool with which to perform basic penetration testing due to its popularity, accessibility, a large number of various reconnaissance and penetration tools, and a plethora of training videos, programs, books, etc. This testing will serve as a simple, initial footprinting ability and will be supplemented by engaging vendors to perform penetration and social engineering testing going forward.

The Practical Threat Analysis application gave Amarci a tool whereby they were able to document each system individually, identify threats specific to the platform, list the vulnerabilities extant on each system, and identify any countermeasures put into place to mitigate cybersecurity threats and risks and bring it within risk appetite levels. While not an automated tool, this tool allows the organization to identify its key critical systems, determine the likelihood and the magnitude of impact of any potential threats, and prioritize controls based on effect, impact, and cost. The image below shows the logical associations beginning with the asset on the left, moving through the threat model, risk and vulnerability assessments, and listing the specific countermeasures that mitigate the vulnerabilities, which in turn lowered the inherent risk to a residual risk which falls within the stated Risk Tolerance levels for the organization.

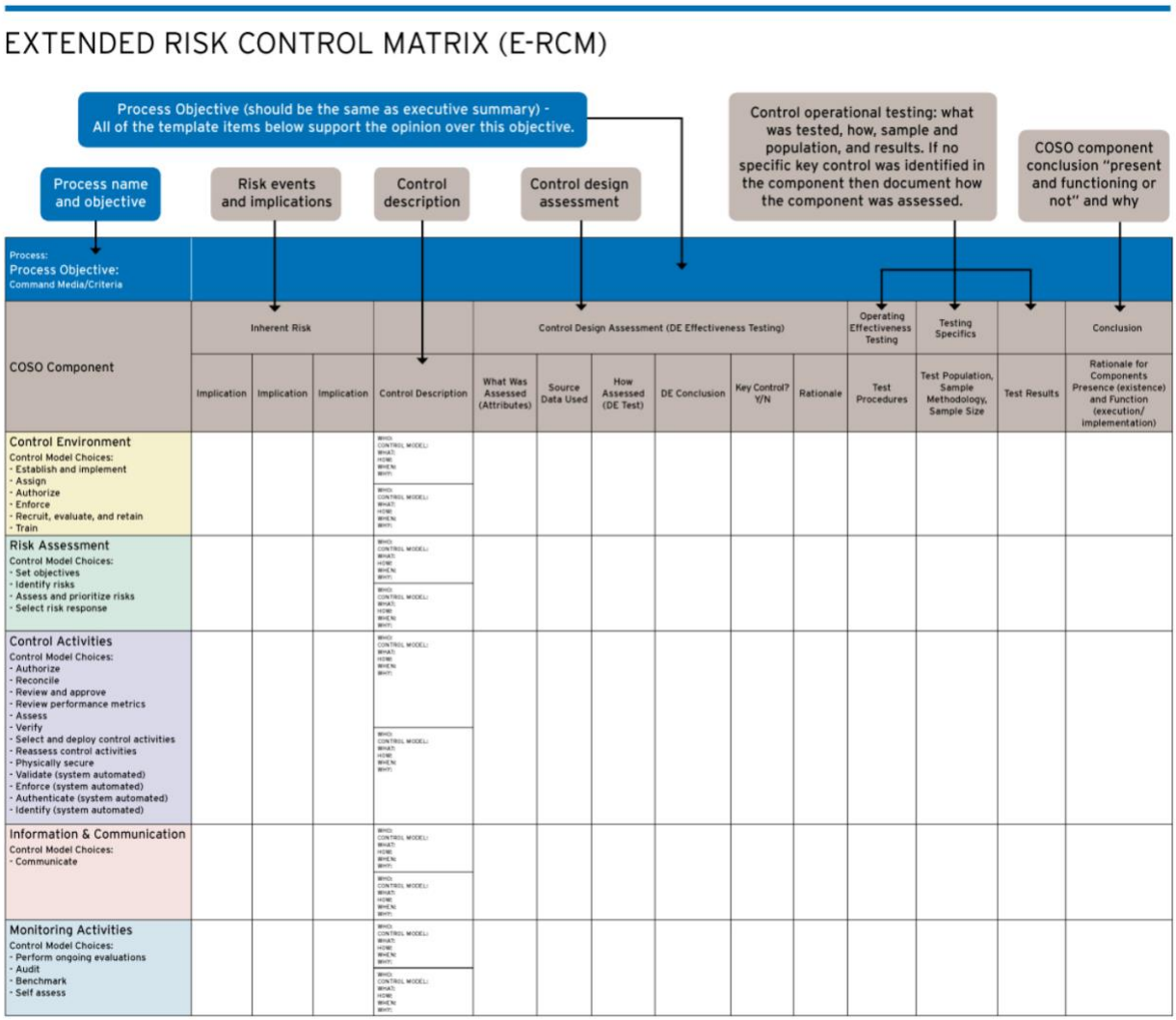
Image 3: Practical Threat Analysis Methodology (PTA Technologies, 2013)



The program followed a logical path incorporating Administrative controls in the form of the Policies, Standards, and Procedures and the Technical controls for patch management followed by implementing countermeasures that were identified during the Threat Modelling process designed to protect the client and company data. One component of the new process was the implementation of a recurring Risk and Controls Validation process, wherein Amarci staff would review the processes and controls for the protection of the systems and, through interviews and process review, validate if the control is designed effectively by identifying WHO does WHAT HOW, WHEN and WHY in the control description and then having the group being reviewed to walk through the process as well as providing a judgmental sampling of prior performances of the control. While this is not a formal AUDIT or

OVERSIGHT review process, it will provide transparency and establish a level of assurance that the security controls are being followed and are performing as expected. This will also provide the digital evidence for Due Care and Due Diligence for immediate and future analysis. Where it is determined that either the control is not properly written, no longer meets the needs of the business and needs to be redesigned, or is still current and effective, this allows for an objective review of the processes and allows for proper decision-support for ensuring effective controls are present. The Risk Control Matrix below is the design that has been implemented for detailed documentation.

Image 4: Risk Control Matrix (Boyle, Tim, 2020)



The chosen metrics were identified as the key measurements management needed to be able to show the current status and trends of various Key Performance Indicators (KPIs). The following image

reflects a Mockup of the Dashboard metrics that were developed during the buildout of the Information Assurance and Risk Management Program.

Image 5: Dashboard Metrics (Regional Bank Technology, 2020)

#	Metric		Current	Prior	Trend	RAS*
Threat Landscape						
1	Number of critical, high and medium security incidents		12	10	↓	<6
Health of Information Security System						
2	Percentage of systems inventoried		91%	91%	→	>90%
3	Percentage of network with full security suite controls installed and configured	Windows	95%	93%	↑	>95%
		Linux	65%	62%	↑	>65%
4	Percentage of employees who completed security training in the Past 12 months		93%	90%	↑	>92%
Effectiveness of Controls						
5	Percentage of firewall configurations reviewed in the past month		92%	92%	→	>90%
6	Percentage of internet facing applications scanned weekly for vulnerabilities		95%	96%	↓	>95%
7	Percentage of change management events compliant with approval and review process		97%	98%	↓	>99%
8	Percentage of high, medium and low alerts reviewed on a monthly basis		98%	98%	→	>98%
9	Passing rate of phishing email tests		85%	85%	→	>88%
Defensibility						
10	Percentage of network patching compliance (within 30 days)	Windows	98%	98%	→	>98%
		Linux	74%	72%	↑	>75%
11	Percentage of externally facing applications with critical or high vulnerabilities		1%	1%	→	<2%

#	Metric		Current	Prior	Trend	RAS*
12	Percentage of network operating on end-of-life systems (hardware & software due for demise)	Hardware	24%	24%	→	<25%
		Software	19%	18%	↓	<20%
13	Percentage of critical applications under identity and access central administration		96%	97%	↓	>95%
14	Percentage of critical and high risk technical vulnerabilities (risk issues) beyond 60 days		15%	13%	↓	<10%
15	Number of critical vendors with open critical and high risk issues		09	08	↓	<10
16	Number of privileged accounts not managed or monitored by an access management solution		05	05	→	<5
17	Percentage of unencrypted data sources with PII data		4%	4%	→	<5%
18	Number of overdue audit & regulatory findings		02	02	→	<2
Recoverability						
19	Number of critical & high severity ops incidents		24	24	→	<25
	- Exceeded RTO		01	01	→	<1
	- Failed to failover		01	01	→	<1
20	Number of failed backups per month		34	34	→	<40
21	Percentage of critical applications that have not performed disaster recovery test in 12 months		3%	4%	↑	<5%

*Risk Appetite Statement

The final component of the project was to deliver a general security awareness program for the entire organization as well as a security training program designed for the general IT staff. The Security Awareness Program was implemented with an annual mandatory training requirement that everyone from the General manager down is required to attend. To supplement the annual training, periodic communications are to be sent out to everyone quarterly as well as having various security posters around the office reminding people of the need to ensure client data is protected, types of social engineering, phishing, vishing, etc. The security training program for the technology departments was also implemented with a mandatory annual required training. This training will include aspects of data protection at rest and in motion, protecting data according to its classification, among other security subjects.

DOCUMENTATION

Cybersecurity Controls

Appendix B represents the chosen System Security Standard that addresses the Vulnerability Assessment and Enterprise Patch Management requirements with the patching and scanning Service Level Agreements.

PROJECT SUMMARY

At the beginning of the process, Amarci, following a Security Process audit as directed by the Board of Directors, found that the security process in place for performing vulnerability assessments and patch management was non-existent and any activity such as patch management was performed haphazardly with no validation or metrics generated. There were no formal vulnerability assessments, no Risk Assessments, and no well-defined patch management process. The practice was to apply patches manually with no pre-test for patches to test for services and processes breakage, there was no method for guaranteeing that all systems were patched, and there was no data or system classification according to the sensitivity of the data stored or processed on the system.

The IT Operations department spearheaded the audit review process and, in coordination with the business, established effective Policies and Standards, and, internal to IT, Procedures for performing asset management, risk assessments, vulnerability assessments, patch management, and reporting usable metrics to the business to ensure that Due Care and Due Diligence for the effective protection of client and corporate data aligns with industry best practices as defined in various frameworks to include COBIT and NIST.

The implementation project successfully delivered an Information Assurance and Risk Management program that was accepted by the organization with support from executive leaders, approved by the Board of Directors and was designed to instill confidence in the stakeholders that security is a key element in the business process, working together for the client. However, while a successful program was delivered in the end, there were still several areas that were identified as being able to benefit from additional improvements and additions. These are identified in the next section.

FUTURE PROCESS IMPROVEMENT PROJECTS

While beyond the time, scope, and resources for this specific implementation, following this implementation, Amarci will look to:

1. Establish a formal Enterprise Architecture framework using TOGAF
2. Development of a Chief Compliance Officer role
3. Development of a Chief Risk Officer role
4. Formation of an Internal Audit department
5. Development of an Oversight Group
6. Implement a formal Change and Release Management program
7. Establish a Risk Management Office
8. Establish an automated Vulnerability Assessment, Patch Management, and Risk Management process with a Test Environment and scripting processes using an Automated Build process, either in GO or Jenkins with a manual checkpoint for promotion into production
9. Implement a Security Information and Event Management system, e.g. AlienVault OSSIM
10. Formalize a Risk Modeling process such as FAIR, STRIDE, OCTAVE, or DREAD as a standard risk evaluation methodology using Qualitative and Quantitative measurements
11. Develop a Business Continuity and Disaster Recovery procedure and plan

APPENDIX A Project Dependencies, Milestones, and Timeline

The table below outlines the milestones for the project with the tasks, dependencies, resources, duration, and start/stop dates.

Table 1: Project Timeline (MS Project)

% Completed	Task #	Task Name	Duration	Start	Finish	Predecessors	Resource Names
	1	**Information Assurance and Risk Management Program Design, Implementation, and Operation**					
	2	**Milestone 1 – Creation of Policies, Standards, and Procedures**					
100%	3	Identify Audit Review Team	1 day	Fri 10/23/20	Fri 10/23/20		IT Manager, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer
100%	4	Audit current Policies	1 day	Mon 10/26/20	Mon 10/26/20	3	IT Manager
100%	5	Create Policies	14 days	Mon 10/26/20	Thu 11/12/20	4	IT Manager
100%	6	Audit current Standards	1 day	Sat 10/24/20	Sat 10/24/20		IT Manager

100%	7	Create Standards	28 days	Mon 10/26/20	Wed 12/2/20	6	ClaimsVP, IT Manager, Operations VP, Underwriting VP
100%	8	Audit current Procedures	1 day	Sat 10/24/20	Sat 10/24/20		IT Manager
100%	9	Create Procedures	60 days	Mon 10/26/20	Fri 1/15/21	8	IT Manager, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer
100%	10	**Milestone 1 Completion**	61 days	Fri 10/23/20	Fri 1/15/21		
	11	**Milestone 2 – Asset Inventory and Risk Assessment process**					
100%	12	Perform Asset Inventory	7 days	Mon 10/26/20	Tue 11/3/20		IT Manager, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer
100%	13	Perform Risk Assessment	28 days	Wed 11/4/20	Fri 12/11/20	12	IT Manager, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer

100%	14	**Milestone 2 Completion**	0 days	Fri 12/11/20	Fri 12/11/20		
	15	**Milestone 3 – Patch Management System**					
100%	16	Research and Identify Enterprise Patch Management system	5 days	Mon 10/26/20	Fri 10/30/20		Sr. Systems Engineer
100%	17	Acquire chosen technology	14 days	Mon 11/2/20	Thu 11/19/20	16	IT Manager
100%	18	Configure and Deploy technology	3 days	Fri 11/20/20	Tue 11/24/20	17	Sr. Systems Engineer, Sr. Network Engineer
100%	19	Import assets into technology	1 day	Wed 11/25/20	Wed 11/25/20	18	Sr. Network Engineer, Sr. Systems Engineer
100%	20	Create a test environment for patching	3 days	Fri 11/20/20	Tue 11/24/20	17	Sr. Network Engineer, Sr. Systems Engineer
100%	21	Create Scheduled procedure for patching systems	1 day	Mon 10/26/20	Mon 10/26/20		IT Manager, Sr. Network Engineer, Sr. Systems Engineer
100%	22	Perform Certification and Accreditation of Patch Management system/Deploy to production	2 days	Thu 11/26/20	Fri 11/27/20	19	IT Manager

100%	23	**Milestone 3 Completion**	26 days	Sat 10/24/20	Fri 11/27/20		
	24	**Milestone 4 – Vuln Assessment system**					
100%	25	Research and identify Vulnerability Assessment system	5 days	Mon 10/26/20	Fri 10/30/20		Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer
100%	26	Acquire chosen technology	7 days	Fri 10/30/20	Mon 11/16/20	25	IT Manager
100%	27	Configure and Deploy technology	3 days	Tue 11/17/20	Thu 11/19/20	26	Sr. Network Engineer, Sr. Systems Engineer
100%	28	Perform Initial Vulnerability Assessment and Remediation tasks	7 days	Thu 11/19/20	Fri 11/27/20	27	IT Manager, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer
100%	29	Create Scheduled procedure for ongoing vulnerability assessments	1 day	Sat 10/24/20	Sat 10/24/20		IT Manager, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer
100%	30	Establish a cycle for performing	1 day	Sat 10/24/20	Sat 10/24/20		IT Manager

		penetration testing					
100%	31	**Milestone 4 Completion**	25 days	Mon 10/26/20	Fri 11/27/20		
	32	**Milestone 5 – Governance, Risk, and Compliance**					
100%	33	Research and Identify Governance, Risk, and Compliance system	7 days	Mon 10/26/20	Tue 11/3/20		IT Manager
100%	34	Establish Risk Controls for each IT department to conform with GRC, data protection requirements, compliance to ensure Confidentiality, Integrity, and Availability are all properly addressed, and risk mitigated	45 days	Sat 10/24/20	Thu 12/24/20	33	ClaimsVP, IT Manager, Operations VP, Sr. Database Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer, Underwriting VP
100%	35	Develop Metrics to reflect Key Risk Indicators, compliance with controls, Risk	14 days	Sat 10/24/20	Wed 11/11/20		ClaimsVP, General Manager, IT Manager, Operations VP, Sr. Database

		Assessment findings and issues, Matters Requiring Attention, etc.					Administrator, Sr. Developer, Sr. Network Engineer, Sr. Systems Engineer, Underwriting VP
100%	36	**Milestone 5 Completion**	45 days	Sat 10/24/20	Thu 12/24/20		
		Project Complete	**61 days**	**Sat 10/24/20**	**Fri 1/15/21**		

APPENDIX B

This document is one of the standards written during the project and represents the system security standard and establishes the Vulnerability and Patch Management process.

System Vulnerability and Patch Management Standard

History

Version	Author	Date	Comment
1.0	John Richardson	2 Nov 2020	Initial version of the document
1.0	John Richardson	5 Nov 2020	Approved by General Manager
1.0	John Richardson	9 Nov 2020	Approved by Board of Directors

Purpose

The purpose of this document is to establish the Amarci Insurance, Inc., (hereafter referred to as "Amarci") standard governing the vulnerability assessment and patching process of servers, network devices, and workstations to ensure compliance with security best practices.

Scope

The scope of this document is to outline the security processes chosen by Amarci and establish the systems against which the tools will be applied.

Security Tools

Amarci will employ a commercial Vulnerability Assessment application and an enterprise Patch Management appliance (see the System Security Procedures document that details the specific applications chosen) to ensure compliance with security requirements. These tools will be scheduled to

scan the servers, network devices, and workstations at established times to ensure continued compliance with best practices.

Systems Covered by this Standard

This policy applies to but is not limited to all Amarci-owned or managed electronic devices as well as any personal electronic device that connects to wired or wireless networks. These devices include servers, workstations, end-point devices, e.g. iPad tablets, Android tablets, HP tablets, Windows tablets, iPhones, Android phones, Windows phones, and any other type of electronic device, workstations, laptops, USB devices, etc. This list is not to be construed as all-inclusive and additional systems as warranted and as identified by management are to also be considered as covered by this policy.

Application Version Management

Amarci will keep current all applications and their versions, pending successful testing of the application before deployment or upgrade. This includes Microsoft applications as well as 3rd party applications. Legacy software applications will require an Exception Approval (reference the Risk Assessment Procedure document) for a variance from upgrading due to dependencies. Amarci IT Management should also ensure that budget requests be generated that allow for maintaining both consistency and currency of application version.

IT Management will perform periodic reviews of the need to continue the variance and re-authorize the variance at each review.

Patch Management

Amarci will use an approved, commercially recognized patch management tool.

IT Operations will ensure that the Patch Management tools have downloaded the recent. IT Operations will then work with Quality Assurance to deploy the patches to a test environment where QA will perform testing to ensure no application is negatively impacted by the patch. Once QA has completed testing, IT Operations will be notified and determine a schedule for deploying to all systems.

Frequency of Scanning

Amarci will adhere to the following schedule for performing vulnerability assessments and patching compliance.

- System and application patches – Performed monthly (with a rotating schedule to patch a portion of the systems weekly)
- Vulnerability Assessments – Performed weekly

Authorization for Scanning

The following authorization levels will be required to initiate any scanning:

- Patching: No authorization needed to scan and patch systems, providing scanning is performed during regular maintenance windows.
- Vulnerability Assessments: No authorization is needed to scan, providing scanning is performed during regular maintenance windows.

Authorization for Remediation

Once IT Operations has performed any of the audit scans for vulnerability, patch requirements, etc., IT Management will be notified and a schedule for remediation will be determined as to feasibility, business units impacted, approval to remediate, etc. Amarci will apply any approved patches following the following Service Level Agreement (SLA):

Low and Medium risk systems – 90 days to patch

High and Critical Systems (and any system that is public-facing) – 30 days to patch

IT Operations will, during remediation and upon completion, keep IT Management informed of the patching and remediation status.

GLOSSARY

Acceptable Use Policy (AUP): A policy that defines the range of uses that are approved concerning information, systems, and services offered by an organization

Availability: The guarantee that a system or service will be usable in the manner designed at the defined and accepted times

Business Impact Analysis (BIA): The analysis of a system or service's requirements and functions that prioritize the degree of loss if the system or service is not available.

Governance, Risk, and Compliance (GRC): A strategy for managing and documenting an organization's overall governance and enterprise risk management approach. Also, the tool that is used to document and track the risk and risk management actions.

Key Performance Indicator (KPI): A measurement of an activity that evaluates the relative success of a process or service

Maximum Tolerable Downtime (MTD): The absolute maximum amount of time that a service or data can be unavailable without critical damage to the organization

Recovery Point Objective (RPO): Refers to the amount of data that cannot be recovered following a data loss or system failure. This is an agreed-upon amount of data, expressed in units of time, e.g. "The database was corrupted and following the restoration of the backup and transaction log files, 30 minutes of data were lost."

Recovery Time Objective (RTO): This refers to an agreed-upon amount of time that is required to bring a system back online or to restore data from a backup.

Service Level Agreement (SLA): The time guaranteed by the organization, business unit, or technology promised for ensuring that the data or system is available for access or use.

Waterfall: Predictive life cycles of a project (Project Management International, 2017)

References

Boyle, Tim. (2020). *Extended Risk Control Matrix*. Retrieved from IA Online: https://iaonline.theiia.org/2016/Pages/Extended-Risk-Control-Matrix.aspx

C4 Planning Solutions LLC. (2020). Security Life Cycle. *Corporate webpage*. C4 Planning Solutions LLC.

Center for Internet Security. (2020). *The 20 CIS Controls and Resources*. Retrieved from CIS Center for Internet Security: https://www.cisecurity.org/controls/cis-controls-list/

COBIT. (2020). *Effective IT Governance at Your Fingertips*. Retrieved from ISACA COBIT 2019: https://www.isaca.org/resources/cobit

Davis, C. a. (2011). *IT Auditing, 2nd Edition.* New York: McGraw Hill.

GFI Languard. (2020). *GFI Software GFI Languard*. Retrieved from GFI: https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

Harris, S. (2013). *All In One CISSP Exam Guide, Sixth Edition.* New York: McGraw Hill.

National Institute of Standards and Technology. (2011, March). *Managing Information Security Risk*. Retrieved from National Institute of Standards and Technology SP 800-39: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Institute of Standards and Technology. (2020, Oct 2). *Framework Documents: Cybersecurity Framework Version 1.1*. Retrieved from NIST Cybersecurity Framework: https://www.nist.gov/cyberframework/framework

National Institute of Standards and Technology. (2020). *Guide for Conducting Risk Assessments*. Retrieved from NIST Information Technology Laboratory: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

National Institute of Standards and Technology. (2020). *Guide to Enterprise Patch Management Technologies*. Retrieved from NIST Information Technology Laboratory: https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

National Institute of Standards and Technology. (2020, Sept). *NIST Publications.* Retrieved from NIST Publications: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

OWASP. (2020). *OWASP Top 10*. Retrieved from OWASP Top 10 Main: https://owasp.org/www-project-top-ten/

PCI Security Standards. (2020). *Maintaining Payment Security*. Retrieved from PCI Security Standards web site: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Project Management International. (2017). *A Guide to the Project Management Body of Knowledge PMBOK Guide Sixth Edition.* Newtown Square: Project Management Institute, Inc.

PTA Technologies. (2013). Practical Threat Analysis Methodology. *PTA Technologies*. PTA Technologies.

Regional Bank Technology. (2020). *Regional Bank Technology Risk Forum.* Austin: Regional Bank Technology.

Stallings, W. (2019). *Effective Cybersecurity: A Guide to Using Best Practices and Standards.* Upper Saddle River, NJ: Addison-Wesley.

Tenable. (2020). *Buy Nessus Pro*. Retrieved from Tenable: https://www.tenable.com/products/nessus/nessus-professional

Wheeler, E. (2011). *Security Risk Management.* Waltham: Elsevier.