**Professor Alan Hendricks**

George Washington University

NDANet’s Risk Mitigation Plan

*Produced by: Luis Ruiz, Zhyldyz Chow, Kari Hattabaugh, Mona Al Amouri, and Kanghee Kim*

**PSCS 2303 Compliance and Risk Management**

March 30th, 2021

# Executive Summary

Over the course of March 2021 NDANet’s risk management team developed a risk mitigation plan designed to guide future risk mitigations. This was designed as a method of operation to keep future risk assessments within scope and in the same format for easy comparison.

This risk mitigation plan covers identification of controls, prioritization of mitigations and a cost benefit analysis, which identifies the difference of projected benefits and the costs associated with the specific control. This process identifies which controls are cost effective for implementation within NDANet. Once the recommended controls have been identified, NDANet’s senior management can approve which controls should be implemented.

Once the most critical and cost-effective controls have been identified a plan of implementation is developed in the form of Plans of Actions and Milestones (POAM). The POAM includes the steps that need to be taken for implementations, the materials required, milestones to keep the implementation process on track and who is responsible for which actions. Finally, the risk management team needs to conduct a gap analysis to identify whether the risk assessments and risk mitigations were effective.

During the risk mitigation plan’s development, the risk management team evaluated sixteen threat vulnerability pairs, and was able to identify forty-three potential controls. Through the course of the cost benefit analysis, the risk management team was able to identify eight controls to mitigate the five critical risk facing NDANet while staying within budget. The risk management team has identified the following controls: Implementing a data backup schedule to keep data up to date, even in the even of a failure. Securing VPNs and Firewalls to filter out known threats to prevent unauthorized access to NDANet’s network. Updating Firewall rules and software to the latest version to ensure that the firewalls are a strong line of defense for the network. Implementing training for employees focused about internet use best practices to limit the possibility of employees to unwittingly allow unauthorized to NDANet’s network. Updating to a stronger encryption method to maintain the confidentiality of essential data lowering the risk of liability to the company. Establishing a secondary site of operations to be implemented in the case of a infrastructure failure, preventing reputation loss and the loss of profits. Routinely updating the Intrusion Detection and Prevention Systems signature database to provide the protective software with the strongest ability to identify threats on NDANet’s network. Installation of remote wipe software on company owned devices to protect confidential data in the case of theft or loss of company owned devices. The implementation of these eight recommended controls holds a total countermeasure value of $4,486,000.00, saving NDANet a great deal in financial assets and offering protection from liability.

Outline

[Executive Summary 1](#_Toc68524220)

[Introduction 3](#_Toc68524221)

[Scope 3](#_Toc68524222)

[Roles and Responsibilities 4](#_Toc68524223)

[Current Controls 5](#_Toc68524224)

[In-place Controls 5](#_Toc68524225)

[Planned Controls 6](#_Toc68524226)

[Approved Controls 6](#_Toc68524227)

[Overlapping Controls 6](#_Toc68524228)

[Prioritization of Risks 6](#_Toc68524229)

[Critical Risks 7](#_Toc68524230)

[Major Risks 8](#_Toc68524231)

[Minor Risks 8](#_Toc68524232)

[Potential Controls 8](#_Toc68524233)

[Prioritization of Mitigations 10](#_Toc68524234)

[Critical Controls 10](#_Toc68524235)

[Major Controls 10](#_Toc68524236)

[Minor Controls 11](#_Toc68524237)

[Cost Benefit Analysis 11](#_Toc68524238)

[Recommended Controls 12](#_Toc68524239)

[Cost Benefit Analysis: Threat Vulnerability Pair 8 12](#_Toc68524240)

[Projected Benefits 12](#_Toc68524241)

[Overall Costs 12](#_Toc68524242)

[Countermeasure Value 12](#_Toc68524243)

[Cost Benefit Analysis: Threat Vulnerability Pair 9 13](#_Toc68524244)

[Projected Benefits 13](#_Toc68524245)

[Overall Costs 13](#_Toc68524246)

[Countermeasure Value 13](#_Toc68524247)

[Cost Benefit Analysis: Threat Vulnerability Pair 10 13](#_Toc68524248)

[Projected Benefits 13](#_Toc68524249)

[Overall Costs 13](#_Toc68524250)

[Countermeasure Value 13](#_Toc68524251)

[Cost Benefit Analysis: Threat Vulnerability Pair 11 14](#_Toc68524252)

[Projected Benefits 14](#_Toc68524253)

[Overall Costs 14](#_Toc68524254)

[Countermeasure Value 14](#_Toc68524255)

[Cost Benefit Analysis: Threat Vulnerability Pair 5 14](#_Toc68524256)

[Projected Benefits 14](#_Toc68524257)

[Overall Costs 14](#_Toc68524258)

[Countermeasure Value 14](#_Toc68524259)

[Plan of Action and Milestones (POAM) 15](#_Toc68524260)

[Implementation Method 15](#_Toc68524261)

[Required Resources 16](#_Toc68524262)

[Roles and Responsibilities 16](#_Toc68524263)

[Milestones 16](#_Toc68524264)

[Schedule 16](#_Toc68524265)

[Final Gap Analysis 17](#_Toc68524266)

[References 18](#_Toc68524267)

# Introduction

NDANet’s risk management team has identified sixteen threat and vulnerability pairs. They were able to prioritize these risks and establish which order they need to be addressed in with the identified risk value. NDANet’s risk mitigation plan will establish and analyze recommended controls to be implemented and outline how to implement them with a Plan of Action and Milestones.

# Scope

Northeast Doctor Affiliates Network, Inc. (NDANet), a fictitious health services organization headquartered in Arlington, Virginia. NDANet has over 600 employees throughout the organization and generates $500 million in annual revenue. The company has two additional locations in Portland, Maine and Binghamton, New York, which support a mix of corporate operations. Each corporate facility is located near a co-location data center, where production systems are located and managed by third-party data center hosting vendors. NDANet operates in three production data centers that provide high availability across the company’s products. The data centers host roughly 1,000 production servers total, and NDANet maintains 650 corporate laptops and company-issued mobile devices for its employees.

NDANet’s senior management allocated a portion of the budget to cover the mitigations of identified threats. This risk mitigation plan outlined how to identify and assess potential controls to mitigate the risks identified in NDANet’s risk assessment. Any risk mitigations identified will stay within budget while ensuring the most critical risks are addressed first. Then, outlines how these mitigations can be implemented in a way that allows senior management to ensure it is on schedule. Lastly, once controls have been approved, planed and implemented a gap analysis is preformed to ensure that NDANet’s risk management team’s mitigations have been effective.

# Roles and Responsibilities

Within NDANet, multiple departments hold responsibilities regarding risk mitigation. With full cooperation of these departments the management of risk can be completed effectively and in a timely manner. There are some significant leadership roles to help keep a plan on task, NDANet’s CIO, Chief Communications Officer and the Project Manager (PM) are tasked with ensuring the aspects of the risk mitigation are performed effectively within the relevant departments. The risk mitigation will require actions from the IT, HR, sales, physical security, finance/purchasing and PR departments, as well as the Chief Compliance Officer. The key responsibilities of these individuals and departments during NDANet’s risk mitigation is displayed below:

|  |  |
| --- | --- |
| Roles | Responsibilities |
| Chief Information Officer (CIO) | * Provide guidance, assistance, support, and management risk management processes * Ensure the implementation of risk assessment for NDANet’s IT systems and the security provided for these IT systems |
| Chief Information Security Officer (CISO) | * Ensuring the risk mitigation program is executed as planned in a timely fashion * Ensuring risks to the client and risk assessment team of conducting the risk assessment program are appropriately managed |
| Chief Risk Officer (CRO) | * Manage and communicate risk across the enterprise |
| Chief Financial Officer (CFO) | * Approve the use of emergency overtime * Approve the allocation of funds * Ensure costs stay within budget * Allocate additional funds for Risk Mitigation, if necessary |
| Risk Committee | * Oversee the Risk Assessment results and assignment of resources |
| Project Manager (PM) | * Ensuring the costs are controlled * Ensuring quality is maintained * Ensuring the project stays on schedule * Ensuring stays on scope * Tracking and managing all project issues * Ensuring information is available to stakeholders * Raising issues and problems as they become known * Ensuring others are aware of their responsibilities and deadlines |
| Information Security Operations Department (ISOD) | * Develop and administer the Risk Mitigation process * Identify access controls for data compliance |
| Privacy Officer | Provide guidance on:   * Requirements of state and federal laws * Disclosure of and access to sensitive information * Information security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and information security issues |
| Security Control Assessor/Audit | * Determine the effectiveness of the controls |
| Other Internal Partners  (e.g., legal affairs, human resources, business managers, sales, finance/purchasing, public relations) | * Identify losses with recommended mitigations * Identify losses without recommended mitigations * Assists in the gathering of pertinent data and the implementation of controls |

# Current Controls

When a threat vulnerability pair has been identified, NDANet’s CISRT identified controls to mitigate them. The controls are detailed within NDANet’s System Security Plan (SSP). These controls put in place need to be evaluated as well as considered when identifying new controls. This evaluation allows for the effectiveness of the control as well as identification on whether there are options for more cost-effective controls.

## In-place Controls

The risk management team identified the controls that are currently in service. The identification of these controls allows for them to be evaluated on whether they are preforming to the standard necessary as well as whether there are any controls that can supplement or replace those current controls.

## Planned Controls

Once the in-place controls have been identified, the risk management team identified planned controls. Planned controls are those that have been approved by management and a plan is in motion to implement those controls. Planned controls need to be identified to determine whether any can mitigate the risks currently being evaluated. This reduces the opportunity for unnecessary spending.

## Approved Controls

The risk management team also identified approved controls, which have been approved by higher management, however, have not yet been planned. This is necessary to identify if these controls would be capable of mitigation those risks currently being addressed. This prevents unintentional redundancy and unnecessary spending.

## Overlapping Controls

Additionally, the risk management team identified overlapping controls. Overlapping controls are two or more controls that are implemented to reduce the impact of a control failure. Overlapping controls are crucial for critical risks because these controls are designed to improve security.

# Prioritization of Risks

During the course of, the Risk Assessment NDANet’s risk management team was able to identify, categorize and prioritize risks by identifying the likelihood of occurrence and impact these risks would have on NDANet’s critical operations. Once the risks were prioritized, NDANet’s risk management team will be able to identify which risks need to be resolved in a timely manner.

|  |  |  |
| --- | --- | --- |
| Threat Vulnerability Pairs | | |
| Threats | Vulnerabilities | Threat Vulnerability Identifier |
| Loss of company data due to hardware being removed from  production system | Hardware malfunctions | TV1 |
| Data bearing devices are physically removed | TV2 |
| Loss of company information  on lost or stolen company-  owned assets, such as mobile  devices and laptops | Weak passwords | TV3 |
| Unencrypted data | TV4 |
| Employee quits or is fired and keeps company assets | TV5 |
| Loss of customers due to production outages caused by various events, such as natural disasters, change management,  unstable software, and so on | Software has not been patched in a timely manner and flaws are present and unfixed. | TV6 |
| Employees are unaware of how to act during a DDoS attack and cannot find the source of the threat. | TV7 |
| Lack of data backups. | TV8 |
| Internet threats due to company products being  accessible on the internet | Mismanaged firewalls configurations | TV9 |
| Firewalls and IDPS cannot filter out unauthorized users or programs. | TV10 |
| Unsecure connections | TV11 |
| Insider threats | Employees are given access to unauthorized documents or data which should not be accessible to them. | TV12 |
| Lack of user training | TV13 |
| Changes in regulatory landscape that may impact operations | Policies are not being updated yearly to match the changing landscape | TV14 |
| Undertrained employees | TV15 |
| Loose regulation policies | TV16 |

## Critical Risks

Critical risks are identified using the Likelihood and Impact values. This addresses the risks NDANet would more commonly face, as well as the risks that would prevent normal operations within NDANet. Critical risks are those whose risk value is greater than 50. Risk Values are determined by multiplying the Likelihood and Impact values.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Vulnerability Pair Identifier | Likelihood (%) | Impact (%) | Risk level  (Likelihood x Impact) | Risk Category |
| TV8 | 100 | 100 | 100 (1.0 x 100) | Critical |
| TV9 | 90 | 100 | 90 (0.9 x 100) | Critical |
| TV10 | 85 | 100 | 85 (0.85 x 100) | Critical |
| TV11 | 70 | 100 | 70 (0.7 x 100) | Critical |
| TV5 | 75 | 90 | 67.5 (0.75 x 90) | Critical |

## Major Risks

Major risks are identified using the Likelihood and Impact values identified through surveys provided to inhouse experts. Major risks are those whose risk value falls within the range of 11 to 50. This indicated that despite the impact being higher, the likelihood of the risk occurring is low. Minor risks are those whose Risk Value falls below 10. This indicates that the despite the likelihood of the risk may be higher, the impact is low. Risk Values are determined by multiplying the Likelihood and Impact values.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Vulnerability Pair Identifier | Likelihood (%) | Impact (%) | Risk level  (Likelihood x Impact) | Risk Category |
| TV14 | 40 | 60 | 24 (0.4 x 60) | Major |
| TV16 | 45 | 45 | 20.25 (0.45 x 45) | Major |
| TV2 | 20 | 90 | 18 (0.2 x 90) | Major |
| TV3 | 60 | 25 | 15 (0.6 x 25) | Major |
| TV4 | 50 | 30 | 15 (0.5 x 30) | Major |
| TV6 | 50 | 30 | 15 (0.5 x 30) | Major |
| TV12 | 50 | 30 | 15 (0.5 x 30) | Major |

## Minor Risks

Major risks are identified using the Likelihood and Impact values identified through surveys provided to inhouse experts. Minor risks are those whose Risk Value falls below 10. This indicates that the despite the likelihood of the risk may be higher, the impact is low. Risk Values are determined by multiplying the Likelihood and Impact values.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Vulnerability Pair Identifier | Likelihood (%) | Impact (%) | Risk level  (Likelihood x Impact) | Risk Category |
| TV15 | 70 | 10 | 7 (0.7 x 10) | Minor |
| TV13 | 45 | 15 | 6.75 (0.45 x 15) | Minor |
| TV7 | 10 | 60 | 6 (0.1 x 60) | Minor |
| TV1 | 30 | 10 | 3 (0.3 x 10) | Minor |

# Potential Controls

During the course of the risk mitigation, NDANet’s risk management plan has identified potential controls to mitigate the identified risks. These controls are intended to reduce the impact of potential threats facing NDANet. Types of controls could include procedural, technical and physical controls. Procedural controls are controls that modify behavior including, but not limited to, policies, security plans, insurance, training, rules of behavior and software testing. Technical controls are controls that allow automation of security including, but not limited to, log-on identifier, session time-out, system logs and audit trails, data ranges and reasonableness checks, firewalls and encryption. Physical controls are controls that protect the physical environment including, but not limited to, locked doors, guards, access logs, fire detection and suppression, water detection and electrical grounding. It is important to layer these different types of controls to manage risk effectively and ensure protection even if one control were to fail. Below are NDANet’s identified controls in response to the sixteen threat and vulnerability pairs as identified in NDANet’s Risk Assessment plan:

|  |  |
| --- | --- |
| Threat Vulnerability Pairs | Potential Controls |
| TV1 | * Data Backup schedules * Patch Schedule * Implement a policy around regularly scheduled maintenance. |
| TV2 | * Data Backup schedules * Implement physical access controls. |
| TV3 | * Implementing password use policies. * Implementing automated password requirements. * Installation of remote wipe software. |
| TV4 | * Update the encryption method. |
| TV5 | * Update the encryption method. * Installation of remote wipe software. |
| TV6 | * Patch Schedule |
| TV7 | * Employee training * Implementing policy to improve communication. |
| TV8 | * Data Backup Schedule * Warm Site |
| TV9 | * Securing VPNs and Firewalls to filter out known threats. * Implement policy to improve data management. |
| TV10 | * Updating Firewall rules and software to the latest version. * Routinely updating the IDPS signature database. |
| TV11 | * Implement training for employees. * Implement policy to improve data management. |
| TV12 | * Modify permissions to limit employee access. * Implement access controls in sensitive areas. * Introduce employee rotation programs. |
| TV13 | * Implement a policy to restrict company property leaving the building. * Introduce employee rotation programs. * Develop employee training program |
| TV14 | * Implement policy and plans of action and maintenance for compliance laws. * Hire an individual to oversee compliance management. * Compliance monitoring software |
| TV15 | * Hire an individual to oversee compliance management. * Implement policy and plans of action and maintenance for compliance laws. |
| TV16 | * Implement policy and plans of action and maintenance for compliance laws. |

# Prioritization of Mitigations

Once NDANet’s risk management team has identified potential controls, these mitigations need to be prioritized. Prioritizing mitigations is focused around the risk level associated with the threat vulnerability pair that was previously identified in the risk assessment. By resolving those risks with the greatest likelihood and impact to NDANet’s operations, the risk management team is reducing the opportunity for liability, damaged reputation and loss of confidentiality, integrity and availability of NDANet’s data and systems.

## Critical Controls

|  |  |  |
| --- | --- | --- |
| Threat Vulnerability Pair Identifier | Risk level  (Likelihood x Impact) | Potential Controls |
| TV8 | 100 (1.0 x 100) | * Data Backup Schedule * Warm Site |
| TV9 | 90 (0.9 x 100) | * Securing VPNs and Firewalls to filter out known threats. * Implement policy to improve data management. |
| TV10 | 85 (0.85 x 100) | * Updating Firewall rules and software to the latest version. * Routinely updating the IDPS signature database. |
| TV11 | 70 (0.7 x 100) | * Implement training for employees. * Implement policy to improve data management. |
| TV5 | 67.5 (0.75 x 90) | * Update the encryption method. * Installation of remote wipe software. |

## Major Controls

|  |  |  |
| --- | --- | --- |
| Threat Vulnerability Pair Identifier | Risk level  (Likelihood x Impact) | Potential Controls |
| TV14 | 24 (0.4 x 60) | * Implement policy and plans of action and maintenance for compliance laws. * Hire an individual to oversee compliance management. * Compliance monitoring software |
| TV16 | 20.25 (0.45 x 45) | * Implement policy and plans of action and maintenance for compliance laws. |
| TV2 | 18 (0.2 x 90) | * Data Backup schedules * Implement physical access controls. |
| TV3 | 15 (0.6 x 25) | * Implementing password use policies. * Implementing automated password requirements. * Installation of remote wipe software. |
| TV4 | 15 (0.5 x 30) | * Update the encryption method. |
| TV6 | 15 (0.5 x 30) | * Patch Schedule |
| TV12 | 15 (0.5 x 30) | * Modify permissions to limit employee access. * Implement access controls in sensitive areas. * Introduce employee rotation programs. |

## Minor Controls

|  |  |  |
| --- | --- | --- |
| Threat Vulnerability Pair Identifier | Risk level  (Likelihood x Impact) | Potential Controls |
| TV15 | 7 (0.7 x 10) | * Hire an individual to oversee compliance management. * Implement policy and plans of action and maintenance for compliance laws. |
| TV13 | 6.75 (0.45 x 15) | * Implement a policy to restrict company property leaving the building. * Introduce employee rotation programs. * Develop employee training program |
| TV7 | 6 (0.1 x 60) | * Employee training * Implementing policy to improve communication. |
| TV1 | 3 (0.3 x 10) | * Data Backup schedules * Patch Schedule * Implement a policy around regularly scheduled maintenance. |

# Cost Benefit Analysis

A cost benefit analysis is used to determine whether the benefit of a countermeasure outweighs the costs. This can also identify which countermeasure provides NDANet with the greatest magnitude of benefit. The components of a cost benefit analysis include the projected benefits, total costs and a countermeasure value. The projected benefits are calculated by finding the difference between NDANet’s losses without any controls and NDANet’s estimated losses with controls implemented. The countermeasure value can be determined through finding the difference between the costs and projected benefits. If the benefits outweigh the costs, then the countermeasure would be a candidate for recommendation. However, if the benefits and costs are similar, a return on investment can be calculated to determine the long-term effect the countermeasure would have on NDANet. Preforming a cost benefit analysis provides the recommendations that need to be submitted for approval.

## Recommended Controls

Through the process of a cost benefit analysis NDANet’s risk management team was able to identify which controls to recommend to management for approval. These controls were found through identification of the threat and vulnerability pairs NDANet faces, their likelihood and impact to operations, then through a cost benefit analysis to identify whether the mitigation’s benefit outweighs its costs to NDANet. Lastly, these mitigations were limited to those that fit within the budget provided by NDANet’s senior management. Through the rigorous and efficient efforts of the Risk Management Team, they were able to identify the following recommendations to implement:

1. Implementing a Data Backup Schedule
2. Securing VPNs and Firewalls to filter out known threats.
3. Updating Firewall rules and software to the latest version.
4. Implement training for employees focused about internet use best practices.
5. Update encryption methods.
6. Establish a warm site.
7. Routinely updating the IDPS signature database.
8. Installation of remote wipe software on company owned devices.

## Cost Benefit Analysis: Threat Vulnerability Pair 8

### Projected Benefits

|  |  |  |  |
| --- | --- | --- | --- |
| Mitigation | Losses without Controls | Projected Losses with Controls | Projected Benefit (PB) |
| Data Backup Schedule | $1,280,000.00 | $80,000.00 | $1,200,000.00 |
| Warm Site | $820,000.00 | $60,000.00 | $760,000.00 |

### Overall Costs

|  |  |  |
| --- | --- | --- |
| Mitigation | Initial Costs (IC) | Annual Costs |
| Data Backup Schedule | $960,000.00 | $60,000.00 |
| Warm Site | $180,000.00 | $125,000.00 |

### Countermeasure Value

|  |  |
| --- | --- |
| Mitigation | Countermeasure Value (PB - IC) |
| Data Backup Schedule | $1,000,000.00 |
| Warm Site | $580,000.00 |

## Cost Benefit Analysis: Threat Vulnerability Pair 9

### Projected Benefits

|  |  |  |  |
| --- | --- | --- | --- |
| Mitigation | Losses without Controls | Projected Losses with Controls | Projected Benefit (PB) |
| Securing VPNs and Firewalls to filter out known threats. | $1,300,000.00 | $140,000.00 | 1,160,000.00 |
| Implement policy to improve data management. | $300,000.00 | $250,000.00 | $50,000.00 |

### Overall Costs

|  |  |  |
| --- | --- | --- |
| Mitigation | Initial Costs (IC) | Annual Costs |
| Securing VPNs and Firewalls to filter out known threats. | $280,000.00 | $60,000.00 |
| Implement policy to improve data management. | $60,000.00 | $20,000.00 |

### Countermeasure Value

|  |  |
| --- | --- |
| Mitigation | Countermeasure Value (PB – IC) |
| Securing VPNs and Firewalls to filter out known threats. | $880,000.00 |
| Implement policy to improve data management. | -$10,000.00 |

## Cost Benefit Analysis: Threat Vulnerability Pair 10

### Projected Benefits

|  |  |  |  |
| --- | --- | --- | --- |
| Mitigation | Losses without Controls | Projected Losses with Controls | Projected Benefit (PB) |
| Updating Firewall rules and software to the latest version. | $760,000.00 | $220,000.00 | $540,000.00 |
| Routinely updating the IDPS signature database. | $600,000.00 | $180,000.00 | $420,000.00 |

### Overall Costs

|  |  |  |
| --- | --- | --- |
| Mitigation | Initial Costs (IC) | Annual Costs |
| Updating Firewall rules and software to the latest version. | $10,000.00 | $10,000.00 |
| Routinely updating the IDPS signature database. | $22,000.00 | $22,000.00 |

### Countermeasure Value

|  |  |
| --- | --- |
| Mitigation | Countermeasure Value (PB - IC) |
| Updating Firewall rules and software to the latest version. | $530,000.00 |
| Routinely updating the IDPS signature database. | $398,000.00 |

## Cost Benefit Analysis: Threat Vulnerability Pair 11

### Projected Benefits

|  |  |  |  |
| --- | --- | --- | --- |
| Mitigation | Losses without Controls | Projected Losses with Controls | Projected Benefit (PB) |
| Implement training for employees. | $600,000 | $110,000.00 | $490,000.00 |
| Implement policy to improve data management. | $220,000.000 | $180,000.00 | $40,000.00 |

### Overall Costs

|  |  |  |
| --- | --- | --- |
| Mitigation | Initial Costs (IC) | Annual Costs |
| Implement training for employees. | $40,000.00 | $15,000.00 |
| Implement policy to improve data management. | $60,000.00 | $15,000.00 |

### Countermeasure Value

|  |  |
| --- | --- |
| Mitigation | Countermeasure Value (PB - IC) |
| Implement training for employees. | $450,000.00 |
| Implement policy to improve data management. | -$20,000.00 |

## Cost Benefit Analysis: Threat Vulnerability Pair 5

### Projected Benefits

|  |  |  |  |
| --- | --- | --- | --- |
| Mitigation | Losses without Controls | Projected Losses with Controls | Projected Benefit (PB) |
| Update the encryption method. | $700,000.00 | $50,000.00 | $650,000.00 |
| Installation of remote wipe software. | $250,000.00 | $40,000.00 | $210,000.00 |

### Overall Costs

|  |  |  |
| --- | --- | --- |
| Mitigation | Initial Costs (IC) | Annual Costs |
| Update the encryption method. | $180,000.00 | $180,000.00 |
| Installation of remote wipe software. | $32,000.00 | $32,000.00 |

### Countermeasure Value

|  |  |
| --- | --- |
| Mitigation | Countermeasure Value (PB - IC) |
| Update the encryption method. | $470,000.00 |
| Installation of remote wipe software. | $178,000.00 |

# Plan of Action and Milestones (POAM)

A Plan of Action and Milestones (POAM) is designed to outline the how, by who and when recommended controls should be implemented. A POAM will include the method of implementation, what is needed, who is responsible and a schedule to keep implementation on track.

## Implementation Method

NDANet’s risk management team identified controls to recommend to management using the risk assessment procedures and a cost benefit analysis. These recommended controls have specific methods of implementation. To guide the implementation of these controls, NDANet’s risk management team has identified the steps of implementation of these specific controls. These steps and the prioritization of the controls allows the development of a schedule and specific milestones to keep the implementation process in schedule and within scope.

## Required Resources

When Implementing a new control, the resources need to be appropriately allocated. Resources might include money, man power, electricity, physical space, etc.. NDANet’s risk management team would Identify these resources to ensure that they are available for implementation.

## Roles and Responsibilities

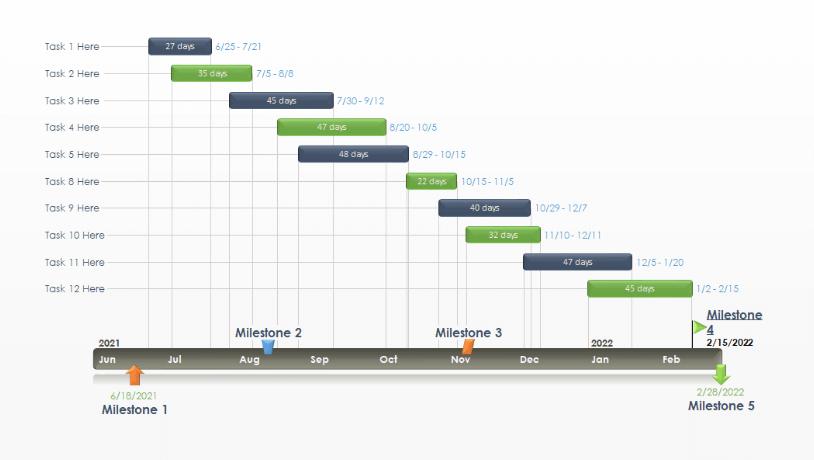
NDANet’s risk management team also needs to identify those who can manage and completing aspects of control implementation. This includes relevant management, individuals within financial to approve purchasing and those responsible to the design and implementation of controls.

## Milestones

NDANet’s risk management team needs to identify the milestones of implementation. This identifies who is responsible for which activity and the dates that an aspect of implementation should start and finish. This is designed to ensure that implementation of controls stays on track and allows management to clearly identify if implementation is on schedule and who is responsible for those activities.

## Schedule

A schedule is developed based on the milestone identified by NDANet’s risk management team. Some methods of doing this include a milestone plan chart, a Gantt chart and a critical path chart. A milestone plan chart is a visual representation of major milestones laid out over a timeline. A Gantt chart is similar to a milestone plan, however, provides more detail. A critical path chart provides a list of project tasks that must completed on time or prevent implementation of the controls from being completed intime. For the purposes of NDANet’s POAM, they will utilize a milestone plan chart. The steps covered in the schedule would include the start date, purchasing required equipment, installation of required equipment, implement any needed utilities, introduce training, installation and configuration, testing and going live. Below is an example of how a milestone plan chart.



# Final Gap Analysis

NDANet’s risk management team must evaluate how effective their risk mitigation was at reducing a risk’s impact on NDANet’s operations. One method doing this is by preforming a gap analysis. A gap analysis involves establishing where an organization is currently, where they would like to be and defining what the difference in that is. A gap analysis can help an organization determine the effectiveness of the mitigations they have implemented.

# References

NIST. (2013). *NIST SP 800-53r4* Security and Privacy Controls for Federal Information Systems and Organizations. https://doi.org/10.6028/nist.sp.800-53r4

Ross, R. (2012), Guide for Conducting Risk Assessments, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online],

Gibson, D., & Igonor, A. (2021). Managing risk in information systems. In *Managing risk in information systems* (3rd ed., pp. 100-320). Burlington, MA: Jones & Bartlett Learning.

Make a timeline. (2020). Retrieved March 30, 2021, from https://www.officetimeline.com/make-timeline/microsoft-word

NIST 800-39. (2011, March). Retrieved April 6, 2021, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf