Professor Alen Hendricks

George Washington University

NDANet’s Risk Assessment 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 assessment plan designed to guide future risk assessments. 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 assessment plan covers critical asset identification, threat identification, vulnerability identification, probability analysis and impact analysis. These processes identify a risk value assigned to each threat and vulnerability pair. With a risk value assigned NDANet’s risk management team can prioritize the risks within the three levels: critical, major and minor. A critical risk impacts NDANet’s critical business functions and could cause serious losses and damage to NDANet’s reputation. A major risk could slow down NDANet’s critical functions and result in some losses. A minor risk slows down business operations and reduces the efficiency of employees.

Once the prioritization of risks has been identified this information is used in the risk management plan to identify and prioritize controls. The final aspect of a risk assessment is the monitoring phase. This involves monitoring systems for vulnerabilities and identifying any potential threats for the next risk assessment.

During the risk assessment plan’s development, the risk management team evaluated sixteen threat vulnerability pairs, and was able to identify five critical risks, seven major risks, and four minor risks to the operations of the organization. The five critical risks focus on data loss due to company property being unlawfully removed from rotation and insufficient online security leaving NDANet’s most critical assets vulnerable. NDANet’s Risk Mitigation Plan will outline the corrective actions to be taken to expedite normal business operations and reduce any liability that NDANet faces.

Outline

[Executive Summary 1](#_Toc68571173)

[Introduction 3](#_Toc68571174)

[Scope 3](#_Toc68571175)

[Critical Areas 3](#_Toc68571176)

[Key Roles and Responsibilities 3](#_Toc68571177)

[Risk Assessment Process 5](#_Toc68571178)

[Risk Assessment Process Schedule 5](#_Toc68571179)

[System Characterization 6](#_Toc68571180)

[NDANet’s Assets 6](#_Toc68571181)

[Risk Identification 7](#_Toc68571182)

[Previously Identified Risks 7](#_Toc68571183)

[Identification of New Threats and Vulnerabilities 8](#_Toc68571184)

[Risk Analysis 9](#_Toc68571185)

[Likelihood of Identified Risks 9](#_Toc68571186)

[Impact Analysis 10](#_Toc68571187)

[Prioritization of Risks 12](#_Toc68571188)

[Maintaining the Risk Assessment 13](#_Toc68571189)

[References 14](#_Toc68571190)

# Introduction

The Northeast Doctor Affiliates Network, Inc’s computer security incident response team (risk management team) preformed a risk assessment to identify and prioritize potential risks that face the organization. During the course of this risk assessment the risk management team identified NDANet’s critical assets, previous threats, current controls, new threats and vulnerability pairs and prioritized them. The risk assessment will be used further to develop a risk mitigation plan related to implementing controls to mitigate identified risks.

# Scope

The Northeast Doctor Affiliates Network, Inc is looking to update its outdated risk assessment plan. NDANet has an infrastructure of three corporate offices located in Arlington VA, Portland MA and Binghamton NY with a datacenter near each office. NDANet employs 600 employees with 1,000 production servers and 650 laptops and mobile devices being accounted for. This plan will provide qualitative risk assessment for NDANet’s infrastructure which will include the domains being impacted as well as an assigned risk factor. This will identify critical areas of the organization and will allow prioritization to key areas that can affect the organization’s compliance concerns, IT infrastructure or mission-critical operations that require immediate attention. It will also provide an analysis of the probability of the identified risks with mitigation techniques. This is necessary to provide a proper re-evaluation of the ever changing and growing risks that pose a concern to NDANet.

# Critical Areas

The risk management team identified the potions of NDANet operations which are most crucial to the organization’s mission. Critical areas include physical locations, critical hardware and software, critical personnel and departments, critical functions, relevant regulations and policies. Identification of critical areas allow the risk management team to efficiently identify the impact potential risks would have on NDANet.

# Key Roles and Responsibilities

Within NDANet, multiple departments hold responsibilities regarding risk assessment. 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 assessment are performed effectively in the relevant departments. The risk assessment 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 assessment is displayed below:

|  |  |
| --- | --- |
| Roles | Responsibilities |
| Chief Information Officer (CIO) | * Oversees, guides and supports the risk management process * 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 assessment 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 Assessment 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 Assessment process * Identify access controls for data compliance * Identifying and reporting threats * Identifying and reporting vulnerabilities |
| 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 | * Conduct an assessment of the management, operational, and technical information security controls * Determine the effectiveness of the controls |
| Other Internal Partners | * Includes other enterprise stakeholders (e.g., legal affairs, human resources, business managers, sales, finance/purchasing, public relations) with an interest in the risk management and risk decisions performed |

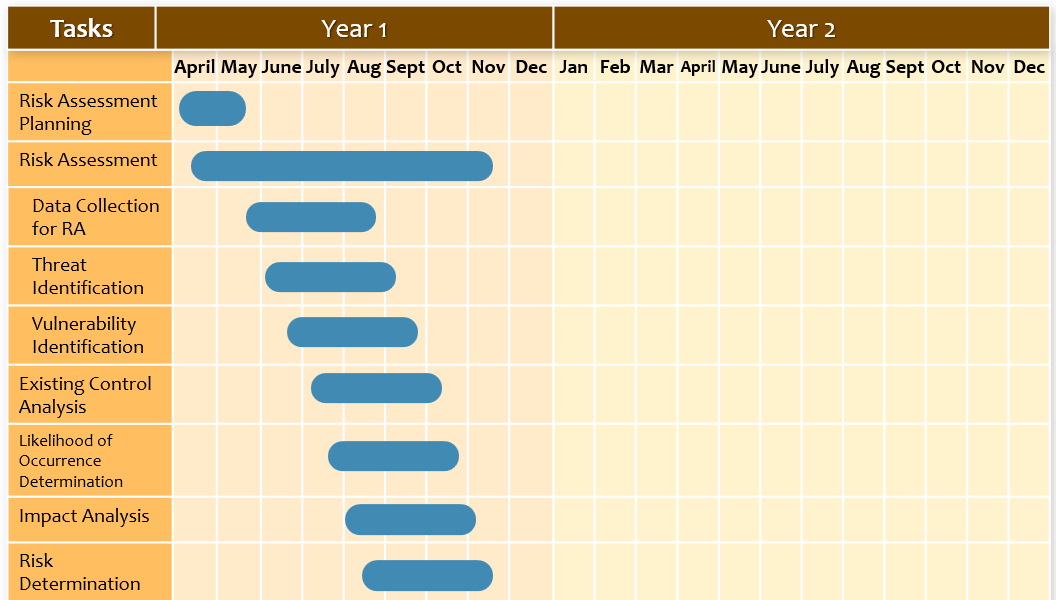
# Risk Assessment Process

The risk assessment process outlined in NDANet’s risk assessment plan involves six major steps: threat identification, vulnerability identification, existing controls analysis, likelihood determination, impact analysis and risk determination. This process provides a structured method to identifying and evaluating the risks facing NDANet.

## 

## Risk Assessment Process Schedule

NDANet’s risk management team developed the schedule below with milestones to keep the risk assessment on track. Implementing a schedule allows the risk assessment process to stay within scope and progress at a steady pace.



### NDANet’s Assets

The identification of assets is an essential first step in managing risk as the assets impact the nature and level of risk. NDANet identified the following assets for the purpose of threat identification, future mitigation compatibility, assisting in the Cost Benefit Analysis and the identification of critical functions associated with those. Asset identification is a crucial step in risk assessment as it helps provide a outline of what and how risks can be mitigated and how to prioritize them.

|  |  |  |
| --- | --- | --- |
| Asset Name | Asset Quantity | Asset Function |
| NDANetData | 1 | The primary source of revenue for the company. The service handles secure electronic medical messages that originate from its customers, such as large hospitals, which are then routed to receiving customers such as clinics. |
| NDANetPay | 1 | A Web portal used by many of the company’s NDANetData customers to support the management of secure payments and billing. The NDANetPay Web portal, hosted at NDANet production sites, accepts various forms of payments and interacts with credit-card processing organizations much like a Web commerce shopping cart. |
| NDANetConnect | 1 | An online directory that lists doctors, clinics, and other medical facilities to allow NDANet customers to find the right type of care at the right locations. It contains doctors’ personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer. |
| Production Servers | 1,000 | Supports the 3 primary products of NDANet. Includes the transition of secure transactions, storing sensitive health related information, providing selective access based on personal credentials over the internet to NDANetData, NDANetPay and NDANetConnect. |
| Corporate Owned Laptops and Mobile Devices | 650 | Facilitates user access to NDANet’s network. |
| Offices | 3 | Physical location of employees and corporate functions. |
| Data Center | 3 | Physical location of production servers. |
| Employees | 600 | Users who facilitate company’s functions and promote NDANet’s mission. |

## Risk Identification

Within the risk assessment, risk is defined as the relationship between a threat and an organization’s vulnerabilities based on probability of occurrence, impact of an incident and current controls set to prevent an incident. These aspects of risk are identified by a risk management team to determine which risks need to be mitigated and in which order.

### Previously Identified Risks

NDANet has performed multiple risk assessments previously. While these risks have already been identified and controls have been put into place or are in the process of getting put in place to mitigate them, they still need to be analyzed to ensure the current controls are still effective. Previously identified risks included threats and vulnerabilities which NDANet has identified through threat and vulnerably assessments previously within the organization’s regular functions.

### Identification of New Threats and Vulnerabilities

During the course of a risk assessment the risk management team identifies new threats. These threats can be identified through past incidents, threats currently targeting the health industry or threats within NDANet’s physical location. Once the threats have been established, NDANet’s risk management team collects the data from audits and vulnerability scans to identify the organization’s vulnerabilities. With the identification of which threats can exploit the vulnerabilities, the risk management team identifies the threat and vulnerability pairs using a threat vulnerability matrix. These threat vulnerability pairs make up an aspect of the risks that could affect NDANet’s critical assets and functions.

|  |  |  |
| --- | --- | --- |
| 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 |

## Risk Analysis

Conducting a risk analysis identifies the likelihood of the threat exploiting a vulnerability and the impact that exploitation would have on NDANet’s critical business functions. The impact and probability of the following risks where identified through inhouse surveys completed by experts in relevant areas. These values were used to identify a risk value to allow for prioritization of the risks and identification of their risk values: critical, major and minor.

### Likelihood of Identified Risks

Identification of risks allows the risks to be known to NDANet, however prioritization of the risk requires additional analysis. Determining the probability of a threat exploiting a vulnerability is dependent on a couple of factors including past incidents, current controls, current threat activity, access to threat actor tools and access to insider information. The following is a chart to assist in determining the likelihood of the individual threats and vulnerability pairs:

|  |  |  |
| --- | --- | --- |
| Likelihood scale | | |
| Probability | Description | Value and Range |
| Low | The risk is unlikely to occur. Threats are not active, vulnerabilities either are not known or have been mitigated. | 0% to 10 % |
| Medium | A moderate chance exists that the risk will occur. It has occurred in the past, but mitigation controls have reduced recent occurrences | 11% to 50% |
| High | A high Probability exist that the risk will occur. It has occurred in the past and will occur again if not mitigates. | 51% to 100% |

*\*From Table 5-1 p. 120 Managing Risk in Information Systems*

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Vulnerability Pairs | | |  |
| Threats | Vulnerabilities | Threat Vulnerability Identifier | Likelihood Value (%) |
| Loss of company data due to hardware being removed from  production system | Hardware malfunctions | TV1 | 30 |
| Data bearing devices are physically removed | TV2 | 20 |
| Loss of company information  on lost or stolen company-  owned assets, such as mobile  devices and laptops | Weak passwords | TV3 | 60 |
| Unencrypted data | TV4 | 50 |
| Employee quits or is fired and keeps company assets | TV5 | 75 |
| 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 | 50 |
| Employees are unaware of how to act during a DDoS attack and cannot find the source of the threat. | TV7 | 10 |
| Lack of data backups. | TV8 | 100 |
| Internet threats due to company products being  accessible on the internet | Mismanaged firewalls configurations | TV9 | 90 |
| Firewalls and IDPS cannot filter out unauthorized users or programs. | TV10 | 85 |
| Unsecure connections | TV11 | 70 |
| Insider threats | Employees are given access to unauthorized documents or data which should not be accessible to them. | TV12 | 50 |
| Lack of user training | TV13 | 45 |
| Changes in regulatory landscape that may impact operations | Policies are not being updated yearly to match the changing landscape | TV14 | 40 |
| Undertrained employees | TV15 | 70 |
| Loose regulation policies | TV16 | 45 |

### Impact Analysis

Once the likelihood of a risk occurring has been established, the risk management team established the magnitude of the impact on NDANet’s operations. This is determined by identifying and prioritizing the critical assets and functions. Then the risk management team assigned a magnitude of impact based on the criteria below.

|  |  |  |
| --- | --- | --- |
| Impact scale | | |
| Probability | Description | Value and Range |
| Low | If the risk occurs, it will have minimal impact on NDANet. The attack will not impact any critical data or systems. | 0% to 10 % |
| Medium | If the risk occurs, it will have a moderate impact on NDANet. It may affect critical data or systems but not to a large extent. | 11% to 50% |
| High | If the risk occurs, it will have a high impact on NDANet. It will affect critical data or systems and cause substantial damage. | 51% to 100% |

*\*From Table 5-2 p. 120 Managing Risk in Information Systems*

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Vulnerability Pairs | | |  |
| Threats | Vulnerabilities | Threat Vulnerability Identifier | Impact Value (%) |
| Loss of company data due to hardware being removed from  production system | Hardware malfunctions | TV1 | 10 |
| Data bearing devices are physically removed | TV2 | 90 |
| Loss of company information  on lost or stolen company-  owned assets, such as mobile  devices and laptops | Weak passwords | TV3 | 25 |
| Unencrypted data | TV4 | 30 |
| Employee quits or is fired and keeps company assets | TV5 | 90 |
| 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 | 30 |
| Employees are unaware of how to act during a DDoS attack and cannot find the source of the threat. | TV7 | 60 |
| Lack of data backups. | TV8 | 100 |
| Internet threats due to company products being  accessible on the internet | Mismanaged firewalls configurations | TV9 | 100 |
| Firewalls and IDPS cannot filter out unauthorized users or programs. | TV10 | 100 |
| Unsecure connections | TV11 | 100 |
| Insider threats | Employees are given access to unauthorized documents or data which should not be accessible to them. | TV12 | 30 |
| Lack of user training | TV13 | 15 |
| Changes in regulatory landscape that may impact operations | Policies are not being updated yearly to match the changing landscape | TV14 | 60 |
| Undertrained employees | TV15 | 10 |
| Loose regulation policies | TV16 | 45 |

### Prioritization of Risks

The risk management team has established the likelihood and impact of potential risks. Utilizing this information, the risk management team was able to preform a risk matrix to prioritize the identified risks. This generates a grid, which places each risk on the grid based on priority. The lowest priority begins in the lower left corner and increases to the highest priority in the upper right corner of the following grid. Additionally, the risk management team calculated the risk value based on the likelihood value and the impact value to determine the priority of each risk, the greater the risk level the greater. Then, each threat is characterized into critical risks, major risks, and minor risks. This is determined by the risk value. Critical risks hold a risk value exceeding 50%, major risks hold a risk value between 11% and 50% and minor risks hold a risk value of 10% and lower.

TV14

24

TV13

6.75

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Vulnerability Pair Identifier | Likelihood (%) | Impact (%) | Risk level  (Likelihood x Impact) | Risk Category |
| TV1 | 30 | 10 | 3 (0.3 x 10) | Minor |
| 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 |
| TV5 | 75 | 90 | 67.5 (0.75 x 90) | Critical |
| TV6 | 50 | 30 | 15 (0.5 x 30) | Major |
| TV7 | 10 | 60 | 6 (0.1 x 60) | Minor |
| 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 |
| TV12 | 50 | 30 | 15 (0.5 x 30) | Major |
| TV13 | 45 | 15 | 6.75 (0.45 x 15) | Minor |
| TV14 | 40 | 60 | 24 (0.4 x 60) | Major |
| TV15 | 70 | 10 | 7 (0.7 x 10) | Minor |
| TV16 | 45 | 45 | 20.25 (0.45 x 45) | Major |

# Maintaining the Risk Assessment

Once risk assessment has been performed and the results have been evaluated another risk assessment is needed to be preformed again. A risk assessment needs to be preformed whenever there has been a major change to NDANet’s critical functions or infrastructure or on an annual basis. This prevents risks from developing without being identified. To ensure that a risk assessment can be preformed it is crucial to stay up to date on news surrounding potential threats and audit and vulnerability scans. This allows risk assessments to be performed efficiently when they are needed.

# 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.

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