**Professor Alan Hendricks**

George Washington University

NDANet’s Risk Management 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

On February 2, 2021 senior management at NDANet requested that a new Risk Management plan be developed to replace the previous and outdated risk management plan. Senior management has also expressed strong support and commitment to a risk management plan that addresses and reacts to newly identified risks. Due to their support, the budget was a secondary concern but remains within reasonable expectations of an organization generating $500 million a year in revenue.

Senior management at NDANet was justified with their concerns as the threat and regulatory landscape have changed dramatically since the publication of the last risk management plan. Within the past year, the costs of data breaches to unprepared or slow to act organizations have increased. The objective of this risk management plan is to prepare the organization to meet the target goals set by regulatory laws and to protect against risks and reduce the impact they may have on company assets or customer data. This risk management plan will be one of the essential components of providing effective security controls to ensure that NDANet’s information assets maintain confidentiality, integrity, and availability. Senior management and stakeholders will also obtain the insight they need to make the best and most effective decision making to react to the identified threats based on their likelihood and impact on the organization’s assets or reputation. To successfully manage the organization’s risks there will need to be ongoing activity that deals with the identification, analysis, evaluation, planning, implementation, control and monitoring of implemented measurements and the enforcement of security policy.

New changes to the regulatory landscape require additional responsibilities when managing customer data and present probable fines to infringing entities. To ensure compliance with these new regulations, the risk management team has determined all compliance laws and regulations regarding customer data and have summarized their effects. It also provides the roles and responsibilities of NDANet’s leadership, committees and departments as required by law or through industry standards. This will allow effective leadership within the organization and will clarify the responsibilities within departments to prevent issues and set accountability. The risk management plan will also provide the planning for Information Security Risk Management which will include the criteria for how Risk Assessments will be performed and the criteria for risk evaluations. Following the planning phase, the risk management will provide a comprehensive guide for how Information Security Risk Management process will be conducted. The schedule for the Risk Management planning process will give senior management and stakeholders a timeline of the tasks previously mentioned so that they can ensure on time completion of the required tasks. The risk management plan will end with a gap analysis which will highlight the current state of our compliance with regulatory laws, what the target is, the gap within those two targets and the action plan to remediate these faults.

Outline

[Executive Summary 1](#_Toc68533235)

[Objectives 3](#_Toc68533236)

[Scope 3](#_Toc68533237)

[Definitions 4](#_Toc68533238)

[Applicable Laws and Regulations 5](#_Toc68533239)

[The Health Insurance Portability and Accountability Act (HIPAA) 5](#_Toc68533240)

[The Health Information Technology for Economic and Clinical Health Act (HITECH Act) 6](#_Toc68533241)

[EU GDPR (European Union General Data Protection Regulation) 6](#_Toc68533242)

[PCI DSS (Payment Card Industry Data Security Standard) 6](#_Toc68533243)

[FISMA (Federal Information Security Management Act of 2002) 6](#_Toc68533244)

[GLBA (Gramm–Leach–Bliley Act) 6](#_Toc68533245)

[SOX (Sarbanes–Oxley Act) 6](#_Toc68533246)

[Roles and Responsibilities 7](#_Toc68533247)

[Information Security Risk Management Planning 10](#_Toc68533248)

[General Requirements 11](#_Toc68533249)

[Frequency of Risk Assessment (RA) 12](#_Toc68533250)

[Criteria for Performing Information Security Risk Assessments 12](#_Toc68533251)

[Risk Evaluation Criteria 12](#_Toc68533252)

[NDANet Information Security Risk Management Process 13](#_Toc68533253)

[Establish scope and boundaries of Risk Assessment 14](#_Toc68533254)

[Identification of Information Assets 14](#_Toc68533255)

[Risk Assessment 15](#_Toc68533256)

[Evaluation of risks 15](#_Toc68533257)

[Prioritization of risks 15](#_Toc68533258)

[Risk Treatment 16](#_Toc68533259)

[Schedule for the Risk Management Planning Process 17](#_Toc68533260)

[Gap Analysis 17](#_Toc68533261)

[References 19](#_Toc68533262)

# Objectives

The objectives of this Risk Management Plan are the following:

* Systematic identification and addressing of information security risks to Northeast Doctor Affiliates Network, Inc. (NDANet) which can compromise the confidentiality, integrity & availability of the information assets, i.e., any Personally identifiable information (PII), Protected Health Information (PHI) and Electronic health records (EHR) that the company owns, customer records, payment records, health records, personal information of the employees and any other company data that the company wants to protect.
* Identification and assessment of likelihood and impact of the risks on the company business.
* Prevention or reduction of undesired effects of the events that can compromise the above-mentioned data and information
* Achievement of continual improvement in the security posture of the company
* Evaluation of existing controls effectiveness and efficiency for mitigation of information security risks
* Identification of risks requiring treatment
* Identification of treatments that commensurate with the information security objectives and in accordance with the Company’s risk appetite
* Identification of applicable laws and regulations
* Assigning responsibilities to respective departments and individuals to implement, operate and monitor this plan

# Scope

The principal goal of NDANet’s Information Security Risk Management plan is to protect the company’s assets, comply with cyber security practices and laws and regulations like HIPAA, PCI DSS by identifying and mitigating risks to the:

* Confidentiality
* Integrity
* Availability

The following data and infrastructure own by the company and its associates (if any) or outsourced:

* Personal Identifiable Information (PII)
* Protected Health Information (PHI) and
* Electronic health records (EHR) and
* Underlying infrastructure on which NDANetData, NDANetPay and NDANetConnect are deployed.

Stakeholders for this RM Plan include:

* NDANet Inc. CEO
* Head of HR Department
* CIO of IT Department
* CISO of cybersecurity Departments
* All customers
* All Employees of NDANet

This plan is not a technical function carried out entirely by Information Technology and Information Security Departments, but rather a business process that requires involvement from many different people, e.g., Senior, and middle management, IT and cyber security departments, employees, culture, laws and regulations, and privacy, etc.) in the organization.

## Definitions

Following are definitions of some of the important related terms:

* Risk: Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization.
* Risk Management: The coordinated activities to direct and control an organization regarding risk are called risk management activities. Often referred to as a risk management process, it can be further elaborated as a set of activities aimed at ensuring that risks are managed so that they do not materially impact the business processes in an adverse way, and that an acceptable level of assurance and predictability to the desired outcomes of any important organizational activity are provided for.
* Risk management process consists of two major components:
  + Risk Assessment: Risk Assessment provides the foundation for an effective risk management. Risk assessment is the process of analyzing threats and associated vulnerabilities that pose a risk to the organization's business processes. Once risks have been identified, they must then be assessed for their potential severity of loss and probability of occurrence.
  + Risk Treatment: Risk treatment is the process of selecting strategies to deal with identified risk, according to business' risk appetite. Risk treatment strategies are:
    - Avoiding, by cessation of risky activities
    - Reducing, by developing and implementing controls
    - Transferring risk to a third party, which could be inside or outside the organization
    - Retaining risk. Risk will usually be retained if there is no cost-effective way to mitigate it, if there is little exposure or potential impact, or if it is simply not feasible to address it effectively.

# Applicable Laws and Regulations

As the company is basically own the following type of data:

* Personal Identifiable Information (PII)
* Protected Health Information (PHI) and
* Electronic health records (EHR)

And, NDANet Inc. is based in US but deals with customers from all US States, Canada and EU and operating payment gateway. Therefore, the following laws and regulations are applicable:

## The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA requires any organizations dealing with healthcare data to be compliant with their administrative, technical, and physical safeguards. The administrative safeguards are risk assessments, a risk management policy, a contingency plan and the restriction of third-party actions when dealing with electronic private healthcare information. NDANet’s technical controls must also follow NIST standards, are required to implement access controls and audit logs. NDANet is also required protect their customer’s electronic private healthcare information and prevent the data from being accessible outside of its organization. Lastly, the physical safeguards focus on the physical location of data, which will be the three data centers and the laptops and mobile devices provided to the staff. NDANet is required to enact policies on how to limit where and how the staff will be using those devices and how that data will be removed from devices when the user or device is no longer under NDANet’s governance.

## The Health Information Technology for Economic and Clinical Health Act (HITECH Act)

The HITECH Act was created to address the use of electronic health records and information by addressing the security and privacy concerns of HIPPA and strengthens their enforceability. This act also addresses what types of violations the organization can face, and the penalties associated to them. These violations may be due to ignorance, reasonable cause, willful neglect, which was corrected or uncorrected, with fines due to the severity, reaching up to $50,000.00 per instance to a yearly maximum total of $1,500,000.00 per calendar year.

## EU GDPR (European Union General Data Protection Regulation)

The GDRP applies to any organization that handles the data of members of the EU and their rights when it comes to the use of their member’s data. These regulations specify how we can use their data, how long we can store it, and the responsibilities that come with handling their data. Our organization may or may not process an EU member’s data therefore, the best practice would be to become GDPR compliant and avoid the heavy fines.

## PCI DSS (Payment Card Industry Data Security Standard)

This standard sets the controls for NDANet which accepts credit card payments. These standards include the requirements that NDANet must maintain data security standards, transactional security, encryption standards and the guidelines to follow them.

## FISMA (Federal Information Security Management Act of 2002)

This law details the security requirements for an organization’s data and systems. NDANet is required to conduct risk assessments and categorizations, provide security plans and controls as well as having an officer in charge of data security.

## GLBA (Gramm–Leach–Bliley Act)

The GLBA is focused on granting individuals additional protection concerning their privacy and sale of their data. NDANet manages or maintains the electronic health records of our customers therefore it is obligated to secure their data, notify customers when data sharing policies are changed policies and allow them to opt-out of that sharing.

## SOX (Sarbanes–Oxley Act)

SOX as a law is focused on financial integrity and holding executives accountable for fraud, however, section 404 applies to NDANet. This section of the law requires NDANet to protect the integrity of their data by using internal controls and third-party auditors to provide additional verification.

# Roles and Responsibilities

A strong culture of cybersecurity is not reliant on one team or department but by allowing employees of all departments to understand and acknowledge the impact of their actions on the security of the organization. Therefore, all the departments and employees must be knowledgeable in their roles in this Risk management Plan. The risk management plan’s success is determined by departments being able to carry out their responsibilities and working in a cooperative and effective methodology. For effective implementation and compliance, some responsibilities are enacted to some designated individuals and groups as stated in the following table:

|  |  |
| --- | --- |
| Roles | Responsibilities |
| **CEO** | Responsible for overall cybersecurity of NDANet Inc. and implementation of this plan. Specific responsibilities include, but are not limited to, the following:   * Providing resources (human, financial and technology) for the plan implementation * Monitoring the implementation and achieved milestones * Assigning responsibilities for sub tasks of the RM plan |
| **Steering Committee (SC)** | Responsible for overall compliance and decision-making regarding IT & cybersecurity of NDANet Inc. Specific responsibilities include, but are not limited to, the following   * Approval of Risk Management Plan * Reviewing Results of risk assessments * Reviewing Progress of risk treatment plan * Reviewing allocated budget (if any) and resources for implementing cyber security controls * Reviewing and accepting the significant risks for which the treatment is either not cost effective or unavailable |
| **Head of HR Department** | Responsible for the identification and categorization of all types of PII, PHI and EHR and their sources. Other responsibilities include, but are not limited to, the following:   * Providing trainings and education for supporting the RM activities and overall cybersecurity * Induction of relevant human resource for compliance * Identifying and evaluating the effectiveness of current training procedures. |
| **CIO/ Head of IT Department** | Responsible for the identification and implantation of controls related to IT infrastructure in combination with cybersecurity department. Other responsibilities include, but are not limited to, the following:   * Implementation of access controls used for data recommended by cybersecurity department for treating vulnerabilities, threats and risks * Costing of each implemented control * Ensure continuous operation and availability of IT infrastructure for cybersecurity and RM plan activities |
| **CISO/ Head of Cybersecurity Department** | Responsible for the overall CIA (Confidentiality, Integrity and Availability) of NDANet assets. Other responsibilities include, but are not limited to, the following:   * Monitoring and ensuring compliance to this plan and applicable laws and regulations * Identify compliance requirements from applicable laws and regulations * Ensuring that risk assessment of information assets is being carried out as per defined frequency. * Ensuring that risk treatment/ mitigation plan is executed and all risks are mitigated within planned time. * Appraising CEO and Steering Committee (SC)   **Through his/ her department:**   * Identify access controls as per required compliance * Identify vulnerability and threats and associated risks and its impacts * Identifying and reporting mitigation strategies and provide recommendation to IT department for implementation * Assess costs associated with mitigation recommendations * Provide assessment of the impact of noncompliance and not implementing the mitigation controls * A list of recommended solutions/ controls to ensure compliance with applicable laws * Ensure the cost-benefit analysis in coordination with the IT and Finance department |
| **Chief Compliance Officer (CCO)** | Responsible for the identification and Implementation of applicable laws and regulations for compliance.  Identify sources of data. Other responsibilities include, but are not limited to, the following:   * Monitoring and ensuring compliance to and applicable laws and regulations * Assess current compliance policies and identify required compliance policies * Identifying current compliance policies * Identifying needed compliance policies * Identifying and reporting mitigation recommendations * Identify and report costs associated with mitigation recommendations * Identify and report the costs associated with not implementing mitigation recommendations * Reporting to CEO regarding compliance level of the Company |
| **Chief Finance Officer (CFO)** | Responsible for providing required funds for the implementation of RM Plan and compliance with applicable laws and requirements. Other responsibilities include, but are not limited to, the following:   * Assess return on investment of the implemented/ recommended controls and strategies * Ensure costs of compliance stay within budget * Allocate additional funds for RMP if necessary |
| **Physical Security Manager** | Responsible for ensuring physical security of the perimeter |
| **Sales Department** | Responsible for complying with the policies and procedures provided by the cybersecurity department. Other responsibilities include, but are not limited to, the following:   * Use only company laptop for company tasks * Never use company provided laptop for personal tasks and for use at home by children |
| **Purchasing/ Procurement Department** | Responsibilities include, but are not limited to, the following   * Purchase of required resources/ equipment / solutions for IT and cybersecurity department and as required by the RM plan. |

# Information Security Risk Management Planning

The company will use a risk-based approach to implement and maintain its Risk Management Plan. The following sections outline the essential guidelines to be followed by Information Technology (IT) Cyber Security team for information security risk management planning.

## General Requirements

* Consider external & internal issues relevant to the purpose of implementing this RM plan at the company.
* Develop an understanding of the needs & expectations of its interested parties and stakeholders.
* Identify the risk(s) for which following popular techniques will be used:
  + Identify the risk scenarios and strategies.
  + Brainstorming.
  + Surveys / Questionnaires.
  + One on one interviews.
  + Issue logs and root cause analysis.
  + Audit Reports.
  + Business Impact Analysis.
  + Process Analysis.
  + Delphi technique.
  + SWAT Analysis.
  + Corporate Knowledge: History of risks provide insight to future threats through:
* Experiential knowledge – collection of information that a person has obtained through their experience.
* Documented knowledge – collection of information or data that has been documented about a particular subject.
* Lessons learned – knowledge that has been organized into information that may be relevant to the different areas within the organization.
* Identify information assets, information assets owners and risk owners.
* Plan actions (risk treatment) to address the identified risks through detailed risk assessment procedures by involving information assets & risk owners respectively.
* Integrate and implement risk treatment actions into existing systems & processes already running within NDANet through effective & sustainable change management plans.
* Measure & evaluate the effectiveness of implemented Risk management Plan, i.e., Risk assessment and Risk treatment plans, controls to ensure that the system remains suitable & adequate with respect to NDANet business requirements.

## Frequency of Risk Assessment (RA)

Following are the timeline of repeating the RA exercises:

1. At least annually.
2. As soon as a new information asset is added and is marked critical by the respective business function.
3. As soon as there is a technological change in the NDANet IT infrastructure.

## Criteria for Performing Information Security Risk Assessments

Information Technology (IT) Cyber Security team in consultation with SC and heads of business functions/ departments will define its risk criteria for evaluation of risk significance. Following factors are to be considered for conducting information security risk assessment:

* Nature and types of information assets: All information assets including information, physical, software, services and people available within the company as per defined geographical and functional scope.
* Nature and types of causes and consequences: All types of threats & vulnerabilities which can compromise the CIA of data and information (i.e., PHI, PII and EHR), physical, software, services and people.
* Defining likelihood & impact: Clear definition of the scale. To be defined on a scale of High, Medium, Low and rated on a scale of 1-3.
* Determining Level of risk: Through a formula: Likelihood \* Business Impact.
* Decision to treat a risk: Through defined risk evaluation criteria.

## Risk Evaluation Criteria

* Risk is considered to be a function of its likelihood of occurrence (probability) and the resulting impact to the NDANet business.
* Risk exposure is to be determined on the basis of calculated risk value (Likelihood \* Impact).
* The identified risk scenarios will be evaluated, treated, prioritized and accepted as per the following scales:

|  |  |  |
| --- | --- | --- |
| 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*

|  |  |  |
| --- | --- | --- |
| 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*

* The following table summarizes the approach and the criteria for risk treatment and its acceptance:

|  |  |  |
| --- | --- | --- |
| Nature of Risk | Risk Level (Likelihood \* Impact) | Evaluation |
| Critical | 100% – 51% | Unacceptable – Needs to be treated |
| Major | 50% - 11% | Tolerable but better to treat as it may lead to a critical risk if not managed on time |
| Minor | 10% - 0% | NDANet. Inc can accept these risks based on their criticality & impact |

# 

# NDANet Information Security Risk Management Process

Risk Management is a comprehensive activity and NDANet Risk Management process will be comprised of the following crucial steps:

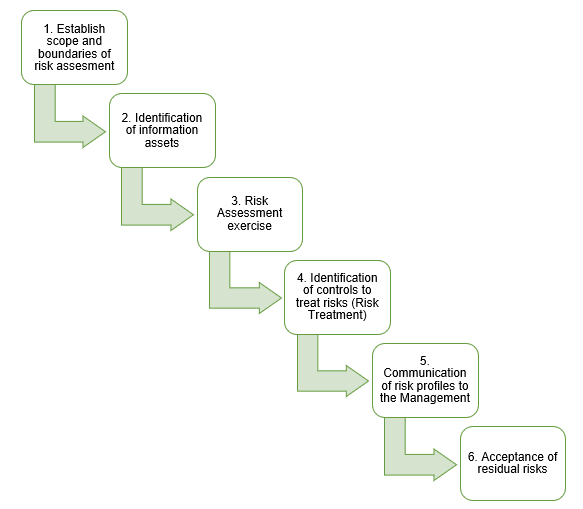


Figure 1 - NDANet Information Security Risk Management Process

The details of the process are given as under:

## Establish scope and boundaries of Risk Assessment

Before commencing the risk assessment or risk treatment activities, Information Technology (IT) Cyber Security team in consultation with SC identify the scope and boundaries for their effectiveness.

## Identification of Information Assets

1. Before risk assessment can begin, all information assets available within the company at each site must be identified and formally inventoried.
2. Every type of information (electronic & hardcopy) & information processing facility, Software, Physical, Services, People and Intangibles available within the company, are all information assets.
3. Every information asset has a dedicated Owner along with a defined set of rules against its use, handling, exchange, disposal and return.
4. Every information asset is assigned a value, type and classification.

## Risk Assessment

1. Risk assessment is to be performed by all Information Asset owners through Risk Management Process with the help of Information Technology (IT) Cyber Security team.
2. In case of Information Asset Delegated Owners (such as IT Department being the custodian of some of the Information Assets), risk assessment will be performed by delegated owners in close coordination with Information Asset owners.
3. The risk assessment methodology encompasses six primary steps, which are described below.



Figure 2 - NDANet Inc. Risk Assessment Process

The formula used to determine risk is: Risk =

It is important to note that while NDANet can minimize the number of vulnerabilities, probability of attacks, the impact and prepare mitigation efforts, it cannot directly affect threats. Threats can take the form of many different events such as attacks, natural disasters, accidents or even equipment failures, as such, there will always be some degree of threat present that cannot be eliminated. Once the risk has been determined, senior management can choose whether they would like to avoid, accept, transfer, mitigate, exploit, or ignore these risks. These decisions are dependent of the risk tolerance of NDANet and the cost presented when reacting towards possible threats.

The details of the risk assessment process are given in the Risk Assessment Plan document.

## Evaluation of risks

1. With determination of risk score, the risk assessment exercise is completed.
2. The information asset owner/ custodian will then compare the risk analysis with the risk evaluation criteria previously established and subsequently prioritizes the risks and categorizes identified risks as Critical, Major or Accepted accordingly.

## Prioritization of risks

1. As per the company risk evaluation criteria, risks which are Critical or Major are planned to be treated on a priority basis.
2. CISO will help information asset owners/ custodians to prioritize treatment of risks.
3. All these actions are performed & subsequently recorded.
4. The following snapshot shows a sample risk assessment sheet to be used formally for Risk assessment in the company for risk assessment:

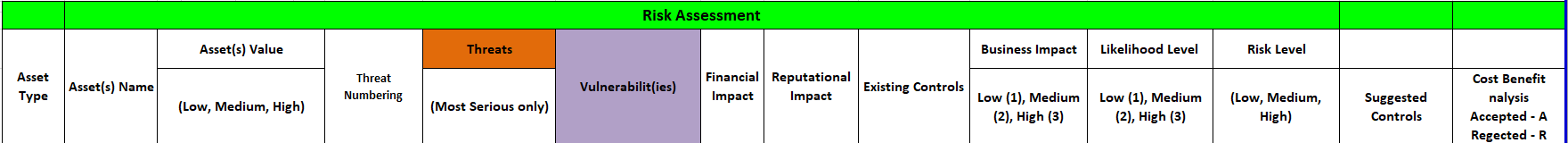


Figure 3 - NDANet Inc. Risk Assessment Sheet Sample

## Risk Treatment

1. Process of selecting controls to deal with identified risk, according to business' risk appetite is risk treatment.
2. After risk assessment, the activity to select appropriate controls as per risk prioritization scheme to treat identified risks will be performed.
3. Risk assessment results, the company risk evaluation criteria and risks prioritization are the key factors for decision to treat risks.
4. The risk treatment process involves the following steps

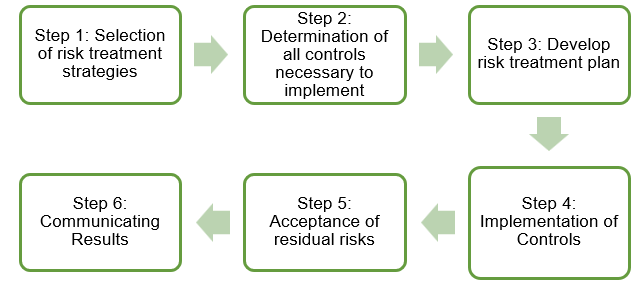


Figure 4 - NDANet Inc. Risk Treatment/ Mitigation Process

The details of the risk treatment process are given in the Risk Mitigation Plan document.

The following snapshot shows a sample risk treatment sheet to be used formally for Risk treatment plan in the company for risk mitigation:

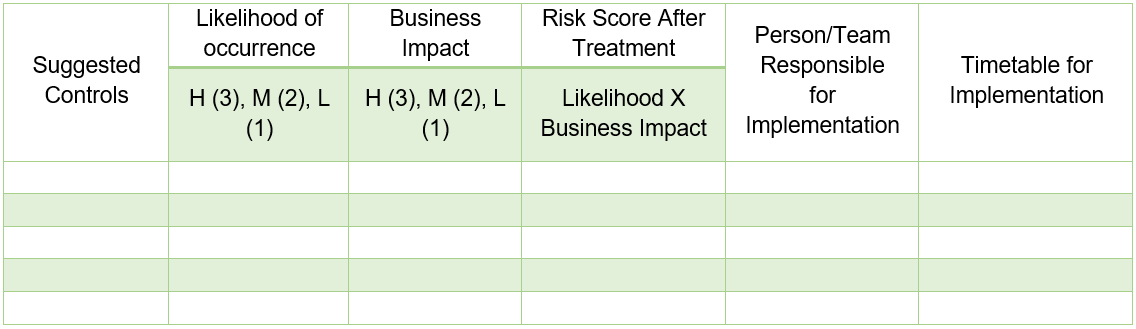
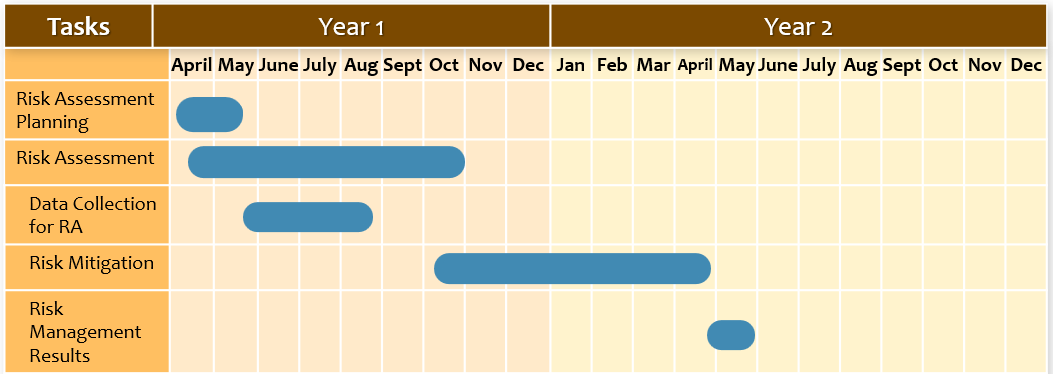


Figure 5 - NDANet Inc. Risk Treatment Sheet Sample

# Schedule for the Risk Management Planning Process



# Gap Analysis

The gap analysis will compare the current state of NDANet’s focus areas, such as regulatory laws, with the target state to determine the NDANet’s exploitable areas. The goal is to feature where there are exploits within the company and how they can be addressed to meet the legal requirements. This will also include an action plan which will serve as a guide for the corrective measures the Information Security must incorporate to bring the organization up to compliance.

The following table will demonstrate how the gap analysis will be performed by the Information Security team.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Focus Area | Current State | Target State | Gap | Action Plan |
| HIPAA Compliance | HIPPA training has not been reviewed or conducted in over a year. | HIPPA training must always be up to date and be conducted at least annually. | Training is not up to date to industry standards. | Conduct HIPPA Training this year. |
| GDPR | GDPR has not been integrated into the company since it passed legislation | Full compliance with GDPR regulations. | There has been no updates to policies regarding the GDPR. | Begin reviewing and integrate GDPR regulations this year. |

# References

Swinhoe, D. (2020, August 13). What is the cost of a data breach? Retrieved April 04, 2021, from https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

Wolford, B. (2019, February 13). What is GDPR, the EU's new data protection law? Retrieved April 04, 2021, from https://gdpr.eu/what-is-gdpr/

HIPAA Journal. (2021, March 05). Official 2021 HIPAA Compliance Checklist. Retrieved April 04, 2021, from https://www.hipaajournal.com/hipaa-compliance-checklist/

HHS Office of the Secretary, & Office for Civil Rights. (2017, June 16). HITECH act ENFORCEMENT Interim final rule. Retrieved April 04, 2021, from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

Darril Gibson, & Igonor, A. (2020). Managing Risk In Information Systems. (p. Ch 5 & 6). S.L.: Jones & Bartlett Learning.

Harris, S. (2019). CISSP All-in-One Exam Guide, Eighth Edition, 8th Edition. The Mcgraw-Hill Companies, Inc.

ISO/IEC 27001:2013. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Retrieved from ISO website: https://www.iso.org/standard/54534.html

ISO/IEC 27005:2018. (2019, January 10). ISO/IEC 27005:2018. Retrieved from ISO website: https://www.iso.org/standard/75281.html

Joint Task Force Transformation Initiative. (2012). NIST SP 800-30r2 - Guide for conducting risk assessments. https://doi.org/10.6028/nist.sp.800-30r1

Joint Task Force Transformation Initiative. (2012). NIST SP 800-30r2 - Guide for conducting risk assessments. https://doi.org/10.6028/nist.sp.800-30r1

NIST. (2011). Managing information security risk: https://doi.org/10.6028/nist.sp.800-39

Piney, C. (2003). Risk identification: Combining the tools to deliver the goods. Presented at the PMI® Global Congress 2003, EMEA, The Hague, South Holland, The Netherlands. Newtown Square. Retrieved from https://www.pmi.org/learning/library/risk-identification-life-cycle-tools-7784

Project Management Institute. (2017). A guide to the project management body of knowledge: (PMBOK® guide) (6th ed.). Newtown Square, Pennsylvania, Usa: Project Management Institute.

Swinhoe, D. (2020, August 13). What is the cost of a data breach? Retrieved April 04, 2021, from https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

Wolford, B. (2019, February 13). What is GDPR, the EU's new data protection law? Retrieved April 04, 2021, from https://gdpr.eu/what-is-gdpr/

HIPAA Journal. (2021, March 05). Official 2021 HIPAA Compliance Checklist. Retrieved April 04, 2021, from https://www.hipaajournal.com/hipaa-compliance-checklist/

HHS Office of the Secretary, & Office for Civil Rights. (2017, June 16). HITECH act ENFORCEMENT Interim final rule. Retrieved April 04, 2021, from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html