Risk Management Plan

Keith M. Hall

College of Science and Technology, Bellevue University

CYBR610-T301 Risk Management Studies

Professor Steven Maestas

November 18, 2023

Revision History

Version #	Approval date	Implemented by	Approved by	Reason
1.0	11/17/2023	K. Hall		

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

A risk is an incident or event that, if it takes place, could have a detrimental effect on daily operations, corporate goals, and the overall mission. Because existing threats and vulnerabilities put company assets in immediate jeopardy, steps must be taken to detect, assess, mitigate, and monitor them. This risk management plan defines the framework within which the project team will identify risks and create mitigation or avoidance strategies for handling them. It also outlines the methods for monitoring and documenting risks.

1.2 OBJECTIVES

Risk carries the potential for serious losses to occur. Many of these losses are avoidable by developing a comprehensive risk management plan with clear objectives. The goals of this plan are:

- Identify the essential risk management roles and responsibilities of individuals and departments within the organization.
- Identify Procedures and Tools for Identifying and Categorizing Assets
- Explain the Process for Risk Identification, Assessment, and Mitigation
- Identify Procedures for Risk Prioritization
- Provide a Structure for Reporting
- Deliver a Security Plan for Business Continuity
- Provide Recommendations for Improvement

- Create a suggested timetable for the risk management planning process.

1.3 SCOPE STATEMENT

The scope of this risk management plan is limited to activities and processes that assure the completion of stated plan objectives, as well as any adjustments to those objectives that ensure all levels of risks within the company are identified and effectively managed.

2 RISK MANAGEMENT ORGANIZATION

2.1 ROLES AND RESPONSIBILITIES

2.1.1 Risk Manager

The Risk Manager is primarily responsible for overseeing risk management for the organization, ensuring strict adherence to the whole process established by the RMP and identifying and updating new risks and opportunities.

Duties:

- Developing and updating the RMP.
- Project pricing estimation based on risk assessment, identification of potential opportunities, and evaluation of necessary measures.
- Optimizing the procedure for locating R&O (Risk and Opportunity) and their corresponding care plans.
- Assisting individuals responsible for managing risks in articulating potential dangers and their associated expenses.

- Reporting involves the creation of indicators, the dissemination of information, and communication with partners.
- Ensuring that the project's risk and opportunity management has a comprehensive worldwide approach and effectively aligning the project's many stakeholders.
- Assessing and informing important stakeholders, including directors and, if needed, the Risk and Audit Committee, on the overall risk exposure of the organization's projects and operations.

2.1.2 Risk Coordinator

The RC is responsible for the overall success of the plan, ensuring that it is implemented correctly throughout the project, analyzing trends and metrics, finance, and training. Unless this responsibility is given to a team member, the Risk Manager is also in charge of generating and maintaining the Risk Register (or Log).

Duties

- Ensure that the project remains on schedule.
- Make sure that the project is finished on schedule.
- Keep track of and handle all project issues.
- Ensure information is accessible to all interested parties

2.1.3 Risk Officer

Every risk discovered is the sole responsibility of its respective owner. Furthermore, they possess comprehensive technical expertise about risks and opportunities, in addition to collaborating with the risk manager. They are likely the individuals who initially observed it and subsequently explained it by identifying the source or reasons for the risk and its consequences. Subsequently, they ensure that they possess the latest information regarding their vulnerabilities. In addition, they articulate the approach and delineate the steps required for the treatment plan, ensuring collaboration among the individuals responsible for executing these tasks.

2.1.4 Team Leader

Appointed by the Risk manager to supervise team meetings and manage small work groups to complete all assigned responsibilities.

2.1.5 Steering Committee

Overall accountability for ensuring that the Risk Management Plan is adequately implemented rests with the project's steering committee. The following actions are examples of specific duties.

- Approve the reduction of hazards with an extremely high severity level.
- Encourage the use of mitigation.

- Assist in cross-organizational and contentious risk mitigation, including assessing Senior management and other organizational resources' participation.
- Change Management and Auditing

3 RISK MANAGEMENT ASSESSMENT

3.1 RISK ASSESSMENT PLAN

The purpose of a risk assessment is to identify, evaluate, and prioritize potential risks to information systems. These systems are comprised of data, assets, people, and processes that must be safeguarded against persistent internal and external threats. An assessment is necessary to identify areas for improvement and assist management in making informed decisions regarding resource allocation and risk reduction. This risk assessment seeks to modify the current plan based on the efficacy of the current security controls in place.

3.1.1 Scope & Boundaries

This plan provides an outline that will help lead the assessment process by deciding the exact steps that need to be taken. The scope of the plan focuses on Health Network's services delivery and the IT (Information Technology) infrastructure and personnel supporting it. The assessment is limited to informing decisions regarding the selection, tailoring, or supplementation of security controls pertaining to the systems and assets shown in **(Appendix B).** To that end, it seeks to pinpoint the current (i) threats to specific assets, systems, and

processes; (ii) identify internal and external vulnerabilities; (iii) determine the adverse impact that may happen given the possibility of threats exploiting vulnerabilities; and (iv) the likelihood a particular exploit will occur. The policies, infrastructure, operations, and assets to which the risk assessment and the resulting risk-based decisions apply are limited to the following:

- The HNetExchange service policy, operations, and infrastructure that handles secure electronic medical messages between Health Network's customer facilities.
- The HNetPay web portal which is used by many of the company's HNetExchange customers to support the management of secure payments and billing. The HNetPay web portal, hosted at Health Network production sites, accepts various forms of payments, and interacts with credit-card processing organizations.
- The HNetConnect online directory listing of doctors, clinics, and other medical facilities which allow Health Network customers to find the right type of care at the right locations.
- The HTTPS connection which enables customers to access all three of Health Networks' product services, including the HTTPS website accessible via the internet.
- Health Network's Data centers, corporate laptops, and company-issued mobile devices for its employees.

3.1.2 Risk Model

The key terminologies used in risk assessments are defined by risk models together with the risk factors that need to be evaluated and how they are related. Because risk assessments depend on well-defined aspects of threats, vulnerabilities, and other risk factors to accurately calculate risk, it is crucial for companies to establish these definitions before performing risk assessments. Figure 2 shows an illustration of the adversary-based threat model utilized for this assessment together with the main risk factors connected to the model and their relationships.

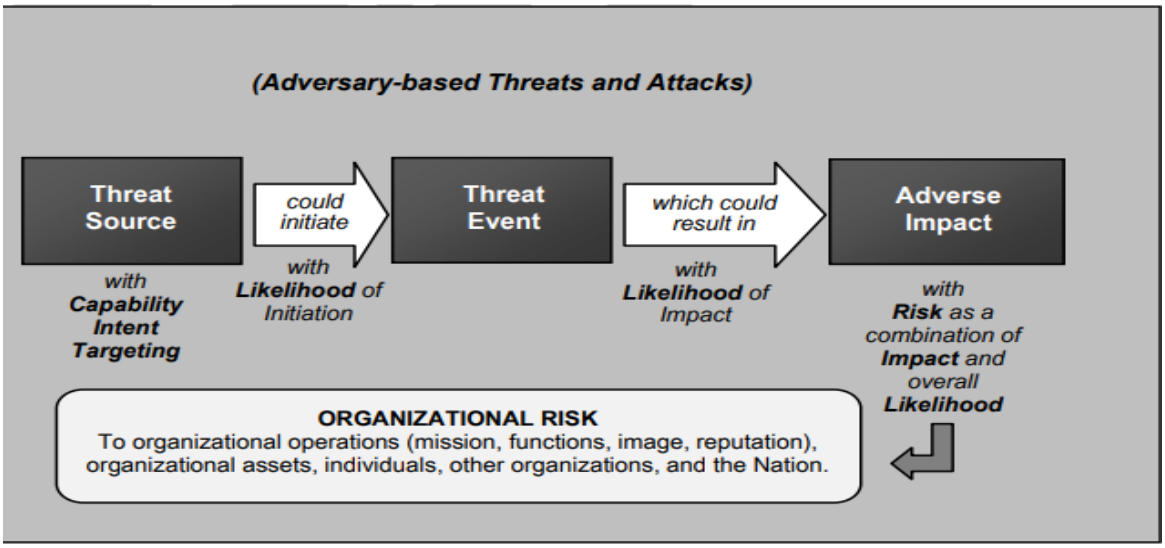


Fig 2: Risk model with key risk factors for adversarial threats (image from NIST.gov)

Threats

A threat is any situation or occurrence that has the potential to have a negative impact on an organization's operations and assets, people, and partner organizations, through an information system, such as through

unauthorized access, information destruction, disclosure, or modification, and/or service denial.

Vulnerabilities

A vulnerability is a built-in weakness in an information system, security protocols, internal controls, or implementation that a threat source could exploit. Security measures that have not been applied or have been applied but still have weaknesses can be used to identify most information system vulnerabilities.

Threat Source and Threat Event

A threat source is an actor who intends to exploit a vulnerability and uses a specific technique to accomplish their objective. Threat sources can be broadly categorized as (i) hostile cyber/physical attacks, (ii) human errors of commission or omission, (iii) structural failures of resources under the control of the organization (such as hardware, software, and environmental controls), and (iv) natural and human-caused disasters, accidents, and failures that are beyond its control.

Likelihood

The likelihood of occurrence of a threat event combines an estimate of the likelihood of initiation or occurrence of the threat event with an estimate of the likelihood of impact (i.e., the chance that the threat event has negative effects). An evaluation of the likelihood of initiation for adversarial threats

typically considers the following factors: (i) adversary purpose; (ii) adversary capabilities; and (iii) adversary targeting. The likelihood of occurrence can be calculated using empirical data, historical information, or other considerations for events other than hostile threat events.

Impact

The level of impact from a threatening event is the magnitude of harm that can be expected to result from the unauthorized disclosure, modification, disruption, destruction, or loss of information and/or denial of service.

3.1.3 Risk Assessment Team

Personnel from the IT department will be assigned ownership of the risk assessment plan. The IT department Manager will be the primary head under the direction of the Chief Information Officer. Key staff members will assist the manager in conducting the assessment and implementing any recommendations. Personnel should be assigned responsibilities in close alignment with their skills and normal job duties. Personnel roles include:

- Risk Assessment Manager
- Coordinator
- IT Staff
- Compliance Staff
- Team Leaders

3.2 RISK ASSESSMENT PROCESS

3.2.1 Assets

Only assets within this assessment's scope will be identified for risk evaluation. The assets identified by Senior Management and Stakeholders as the most critical are:

Information Assets

- Electronic messages in transit between client hospitals and clinics
- Doctors and patient personally identifiable information
- Credit card and billing information
- Doctor and Patient Credentials
- Sensitive corporate data
- Patient medical records

Network Infrastructure

- Corporate Laptops
- Company-issued mobile devices
- Hardware
- Web Portals
- Internet connections (HTTPS)
- Web, email, and database servers
- Security components
- Gateways and credit card processing

- Network devices

Physical Infrastructure

- Buildings
- Equipment
- Power & water supply
- Cable
- Data center facilities

3.2.2 Risk Identification

Risk identification is the process of identifying and evaluating the magnitude of prospective threats and vulnerabilities and the likelihood they will result in losses. Understanding the relationship between threats and vulnerability is crucial. Threats trigger attacks (exploits) that target vulnerabilities. When the threat/vulnerability duo manifests, loss happens. Threats and their associated vulnerabilities should be identified based on information obtained through interviews, a review of historical data, and threat modeling.

3.2.3 Vulnerability Assessment

A vulnerability assessment is a method for identifying weak points in a system. The vulnerability assessment will next prioritize the weaknesses to identify which flaws are pertinent. We have identified the following low to high priority weaknesses that should be checked during every risk assessment:

- Data encryption is lacking.
- Inadequate security cameras
- Unlocked business doors.
- Unrestricted upload of potentially hazardous files
- Downloads of code without integrity checks
- Using faulty algorithms
- URL redirection to dubious websites
- Passwords that are both weak and unchanged
- SSL-free website
- Firewalls and antivirus protection are missing.

3.2.4 Threat Identification

Following is a list of threats associated with the vulnerabilities discovered and prioritized by the Assessment team:

- Loss of company data due to hardware being removed from production systems.
- Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops
- Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on
- Internet threats due to company products being accessible on the Internet.
- Insider threats

- Changes in regulatory landscape that may impact operations.

3.2.5 Controls to be Assessed

Technical Controls

- Input Validation
- Firewalls
- Encryption
- Anti-virus
- System Logs
- Intrusion Detection
- Continuous Monitoring

Physical Controls

- Video Cameras
- Guards and Access Logs
- Locks

Procedural Controls

- Policies and procedures
- Awareness and training
- Personnel Screening checks

3.2.6 Prioritization & Categorization

The following list of threats and vulnerabilities were identified, analyzed, and placed in order of importance by the Assessment Team:

- Loss of information assets due to hardware being removed from production systems and lost or stolen company-owned assets, such as mobile devices and laptops.
- Loss of network infrastructure
- Exposure of sensitive information such as patient and employee records, PII, and credit card information
- Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable applications, and software.
- Internet threats due to company products being accessible on the Internet.
- Insider threats
- Fines and/or imprisonment due to noncompliance to federal law and industry regulations
- Downloads of code without integrity checks
- Using faulty algorithms
- threat/vulnerability duo manifests, loss happens.
- Data encryption is lacking.
- Inadequate security camera coverage
- Unlocked business doors.
- Unrestricted upload of potentially hazardous file

- URL redirection to dubious websites
- Passwords that are both weak and unchanged
- SSL-free website

4 RISK MITIGATION

4.1 PREPARAION & GUIDELINES

Today's technologically oriented businesses are constantly bombarded with threats coming from cybercriminals who are fiercely determined to search the internet for companies with vulnerabilities they can exploit. An organization must maintain an awareness of these threats and implement security measures to counteract them. This Risk Mitigation Plan includes details on how and when to implement countermeasures. It suggests countermeasures for each, and every threat and vulnerability identified in the risk assessment and offers solutions for selecting and implementing security controls which will lower the likelihood an adversary will obtain any reasonable success in exploiting vulnerabilities in the Health Network. It is essential that the selection is based on how well they accomplish either of the following two goals: 1) lowering or neutralizing the identified risks to an acceptable level, or 2) lowering the vulnerability to an acceptable level. The plan also offers several methods for calculating each risk's impact so that resources can be prioritized and allocated according to that impact. However, it is critical to acknowledge that not all disasters can be completely averted. Mitigation deals with the aftermath of a disaster and the

actions that can be taken before the event occurs to decrease negative and, potentially, long-term repercussions.

4.1.1 Risk Reduction Strategy

Health Network, Inc. should incorporate a policy statement in its corporate documents prohibiting it from engaging in business initiatives when the risks of doing so are judged to be excessive compared to the potential benefits. In addition, specific procedures should be developed and adopted to determine acceptable risk levels and identify real-time threats via continuous monitoring.

4.1.2 Controls in Place

It is vital to assess the effectiveness of current security measures in meeting company objectives to prevent, detect, or recover from attacks. When a control is determined to be ineffective, it must be replaced. Some controls will concentrate on a single objective, whereas others on several goals. To be considered an effective countermeasure it must satisfy at least one security objective.

4.1.3 Planned Controls

Controls that have been approved but not yet installed are considered planned. A list of planned controls should be kept on file. The list should include the purpose for which the control was purchased, any supporting documentation, and a target implementation date. Planned controls should be accounted for before other controls are approved, so that an additional control is not purchased if one is already planned to address the same vulnerability.

4.3 IDENTIFYING AND EVALUATING SECURITY CONTROLS

To address the threats and vulnerabilities identified, assessed, and prioritized by the Assessment Team, this mitigation plan recommends the following countermeasures.

4.3.1 Recommendations

Data Encryption

- Use the IKEv2/IPsec protocol to implement VPNs (Virtual Private Networks). When properly configured, IPsec employs asymmetric and symmetric encryption everywhere to deliver speed and the highest degree of security during data transfer.
- When using FTP to share sensitive files internally or with remote users, run it on top of TLS (Transport Layer Security) to establish a secure, encrypted connection. Consider using a cloud solution like Dropbox for storing and moving massive files or entire directories.
- Use TLS to enable encryption on top of HTTP to create an encrypted connection (HTTPS) whenever our computers connect to the internet or the HNetPay Web Portal via an online server.
- Consider encrypting databases that store your most sensitive information assets to defend against both internal and external attacks.
- Use S/MIME for an added layer of security when transmitting extremely sensitive email. In addition to encrypting emails, S/MIME

uses public key infrastructure to ensure emails are legitimate, undamaged, and come from the intended sender.

Patch Management

- Implement a patch management solution that can automate patching of all network appliances, software, drivers, firmware, and servers.
- Upgrade or discontinue use of unsupported software and any internal apps that rely on them. Instead, upgrade to the most recent version of Windows and look for equivalent applications that work with the latest version. Consider replacing any servers that are more than 4 years old.
- Begin migrating to IP6, which is faster and more secure

Firewalls, Routers, Anti-virus

- Configure firewalls and routers to enable rules, which will allow administrators to specify which traffic is allowed and which is banned.
- Install anti-virus/malware protection on all virtual servers.
- Use an email appliance (Proofpoint) to guard against spyware and social engineering. Choose an appliance that can function as an email firewall, enforcing a set of guidelines that restrict which emails are permitted to access or leave our email network.

Access Control

- Adopt and enforce separation and least privilege policies to control access to systems and data. Give users no more access or permissions than are necessary to do their jobs.
- Employ multifactor authentication for access to all networks operated by Health Network, Inc.
- Use an Active Directory (AD) as the main gateway to the network and require a two-step verification process for all access.
- Create additional AD organizational units (OU) then configure AD to grant permissions that decide which resources each OU can access. Require a second login for access to the most sensitive resources.
- Changing password and complexity required to gain access.
- Lock out accounts after a defined number of incorrect password attempts.
- For access to the most sensitive resources use least privilege, activity logs, Security Information and Event Management data, device health, and other parameters.

Monitoring

- Install an intrusion detection/prevention appliance on the network core that will continually monitor the entire network for malicious

activity, take steps to prevent it, and alert incident response teams if necessary.

- Next generation firewalls can also add visibility by monitoring user device behavior and interactions with network applications.
- Install endpoint detection and threat response software on workstations and other endpoints to monitor user behavior and assess security threats in real time.
- Implement User Behavior Analytics (UBA) and monitor or alert any abnormal activity of the employee or partner networks.
- Implement a software platform like Splunk that will let you monitor, search, analyze, and visualize machine-generated logs in real time.

Security Awareness Training

- Establish a minimum 8-hour security awareness training requirement for all workers, with a focus on phishing and password management.

Physical Security Controls

- Digital CCTV (closed circuit television) cameras with full pan, tilt, and zoom should be installed to monitor movement inside and outside of the building(s) and on entrances and exits from secured or critical areas of the company.

- Use card access that will allow only the appropriate people in/out of secured areas.
- Radio frequency identification (RFID)
- Global positioning satellite locator chip

4.3.2 Evaluation

Countermeasures must also be tested to ensure they are effective. Because a countermeasure's goal is to reduce risk, it should either lessen the impact of a threat or reduce vulnerability. The only way to determine the effectiveness of a countermeasure is to test and evaluate it. For example, after implementing the countermeasure, the same vulnerability scan should be performed. If the scan does not discover the risk, the countermeasure has obviously closed the security gap. However, if the scan still discovers the risk, it is apparent that a security gap exists and that more precautions must be taken.

4.4 IMPLEMENTATION AND TRACKING

4.1.1 Selecting Controls

The Change Control Board will select appropriate countermeasures from this list of recommended controls using the Risk Assessment and NIST Special Publication 800-53 to identify security gaps. Controls will be selected to fill those gaps with engagement from management and pertinent stakeholders in an organization-generated approach.

4.1.2 Prioritizing and Tracking Countermeasures

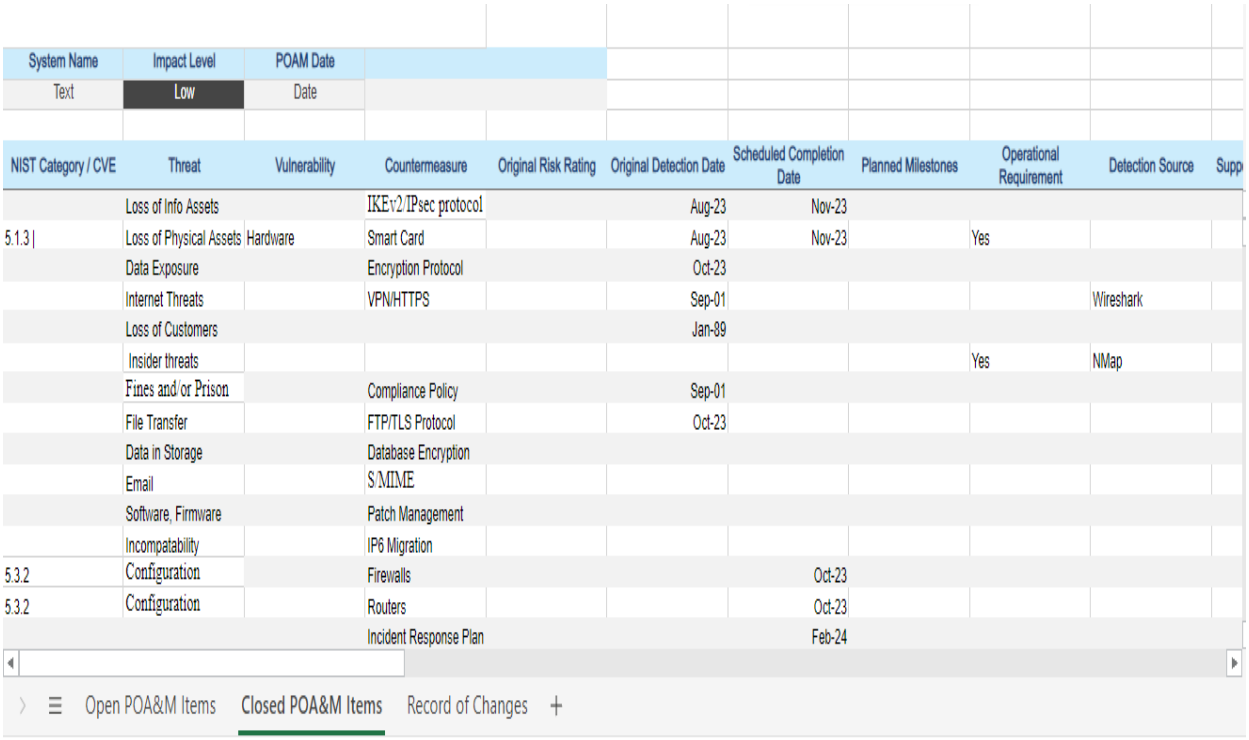
While some of these recommendations can be delayed a brief time, others should be implemented immediately. How should these controls be ranked in order of importance so that the most crucial ones are implemented first? We have adopted a risk-based strategy that makes use of a risk register to rank countermeasures. Controls must be put into place in a manner that is linked to business risk; otherwise, the company is unlikely to derive the most benefit from them. The impact on the business of each control if it is not in place may be determined using the same methodology, and the controls can then be prioritized according to the impact on the company. The Change Control Board will conduct a **Cost Benefit Analysis** for each recommended control to help determine whether a countermeasure should be used. The board can place all controls that qualify in the **Risk Register** below as a template for prioritizing controls.

Enterprise Risk Rgister

Date of last review: Health Network, Inc

ID	Countermeasure	Impact (score/1-5)	Likelihood (score/1-5)	Risk Level (I +L)	Risk Owner (s)	Implementation Date
1	IKEv2/IPsec protocol					
2	FTP/TLS					
3	HTTPS					
4	Encrypting databases					
5	S/MIME					
6	Patch management automation					
7	Upgrade software and Servers					
8	Migrate to IP6					
9	Configure firewalls and routers					
10	Anti-virus/malware					
11	Email appliance					

4.1.3 Ensuring Countermeasures Have Been Implemented



System Name	Impact Level	POAM Date
Text	Low	Date

NIST Category / CVE	Threat	Vulnerability	Countermeasure	Original Risk Rating	Original Detection Date	Scheduled Completion Date	Planned Milestones	Operational Requirement	Detection Source	Supp
	Loss of Info Assets		IKEv2/IPsec protocol		Aug-23	Nov-23				
5.1.3	Loss of Physical Assets	Hardware	Smart Card		Aug-23	Nov-23		Yes		
	Data Exposure		Encryption Protocol		Oct-23					
	Internet Threats		VPN/HTTPS		Sep-01				Wireshark	
	Loss of Customers				Jan-89					
	Insider threats							Yes	NMap	
	Fines and/or Prison		Compliance Policy		Sep-01					
	File Transfer		FTP/TLS Protocol		Oct-23					
	Data in Storage		Database Encryption							
	Email		S/MIME							
	Software, Firmware		Patch Management							
	Incompatability		IP6 Migration							
5.3.2	Configuration		Firewalls			Oct-23				
5.3.2	Configuration		Routers			Oct-23				
			Incident Response Plan			Feb-24				

Open POA&M Items | Closed POA&M Items | Record of Changes | +

5 PRPOSED SCHEULE FOR IMPLEMENTATION

	Owner	**Approval Date**					
Asset Identification							
Vulnerability Assessment							
Threat Identification							

Assessing Controls							
Risk Mitigation Preparation							
Recommended Controls							
Selection of controls							
Approval and Implementation							
Tracking							
Review							
BIA							
Business Continuity							

PLAN APPROVAL

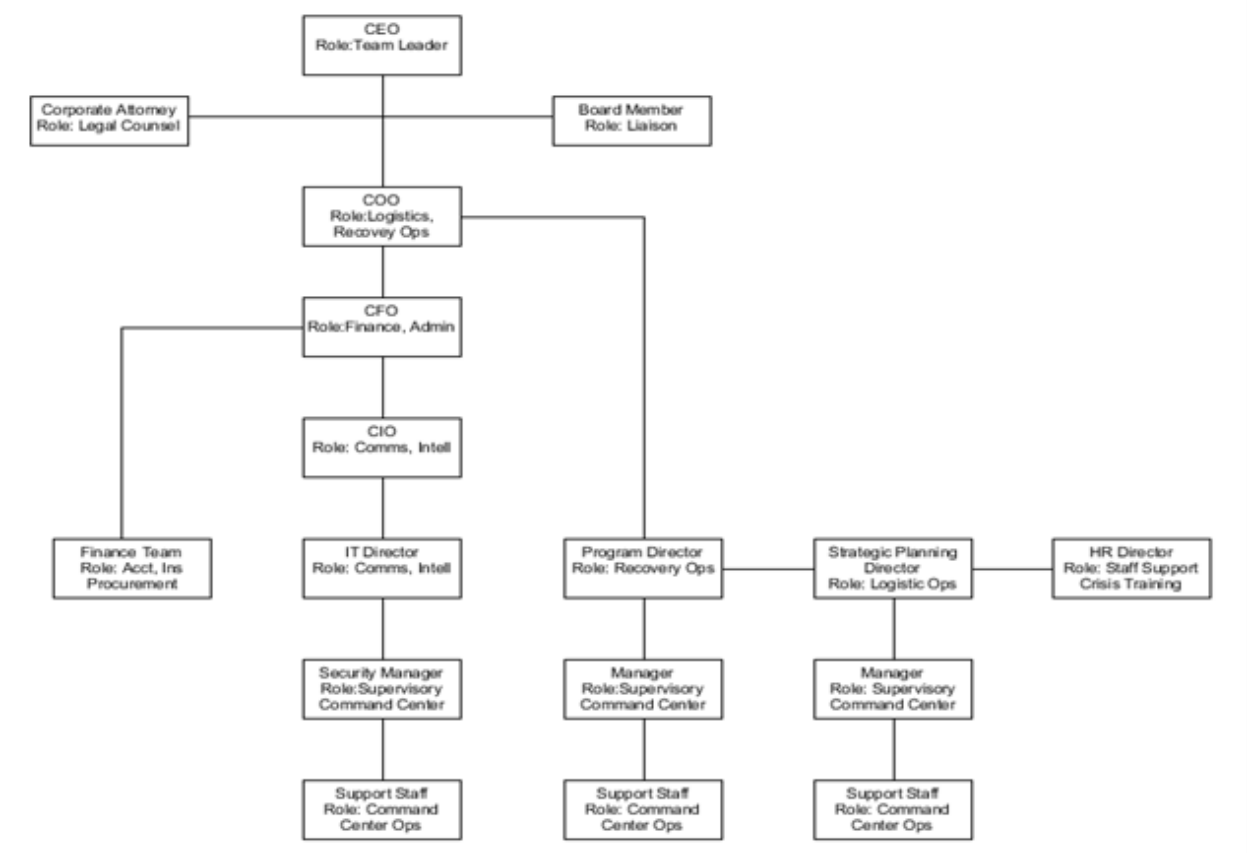
_____ _____

Signature and Title Date

_____ _____

Signature and Title Date

Appendix I Order of Succession and Delegation of Authority



Appendix II: Resources

The list is not all-inclusive, but it will get us started in the right direction.

Resources		Yes	No	
Computers/Laptops				
Printer & Paper				
Pens/Pencils				
Flip Charts				
Landline				
Wi-Fi				
Generators				
Portable Battery Power Banks				
Portable Televisions				
32' Monitors				
Radio				
DVD/VCR, CCTV (Closed circuit television) camera				
Cabinets				
Conference Table/Chairs				

Projectors				
Hard Hats & Boots				
Thumb Drives				
Compact Disks				
Wall clocks				
Break Room Supplies				
Inflatable Airbeds				
ICS Go Kits				
ICS position vests				
Maps and charts as needed				
Dry-erase boards and Markers (multiple colors)				
T-card racks to support				
Administrative support kits				
Fire Extinquishers				
Light Bulbs				
Countertops				
Bottled Water				
Safety Vests				
Shareholder Agreementts				
Supplier Contracts				
Benefits Information				
Business Plan				

References

Definition of Business Impact Analysis (BIA) - Gartner Information Technology Glossary. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/bia-business-impact-analysis

How to prioritize security controls implementation. (n.d.). ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/how-to-prioritize-security-controls-implementation

Managing Risk in Information Systems: Gibson & Igonor; 3rd edition; Jones & Bartlett Learning; 2022

Akdeniz, C. (2015). Risk management explained. Can Akdeniz.

Chapman, C., & Ward, S. (2003). *Project risk management processes, techniques, and insights*. John Wiley & Sons Ltd.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30.

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of applied corporate finance*, *18*(4), 8-20.

Hopkin, P. (2018). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. India: Kogan Page.

Paul Hopkin is an internationally recognized risk management professional and was previously Technical Director at the Institute of Risk Management (IRM) and held the same role at Airmic for nine years previously.

Hodge, B. (2004). Developing risk management plans. *University of Waterloo*.

Managing Risk in Information Systems: Gibson & Igonor; 3rd edition; Jones & Bartlett Learning; 2022

Scavetta, A. (2023, September 12). *How to make a risk management Plan*. ProjectManager. https://www.projectmanager.com/blog/risk-management-plan

(Credible Website)

Risk management fundamentals: Homeland security risk management doctrine (2011) https://www.dhs.gov/publication/risk-management-fundamentals (Accessed: 03 September 2023).

Threat Modeling - The Penetration Testing Execution Standard. (n.d.). http://www.pentest-standard.org/index.php/Threat_Modeling#High_level_threat_modeling_process