

**2024 NIST CSF 2.0 Annual Risk Assessment**  
  
**Review Type:** 2024 NIST CSF 2.0 Annual Risk Assessment

**Completion:** July 11, 2024

**Policy Area:** Information Security Risk Management Policy and Procedure

**Applicability:** Company-wide

**Information Classification**: ***Confidential***



The Information Security Team is pleased to present this detailed overview of the annual Heath New England (HNE) NIST CSF 2.0 Risk Assessment. NIST Cyber Security Framework (NIST CSF) is a framework that is used for the protection of sensitive information (e.g., PHI, PII), and our commitment to information security necessitates a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information.

This report provides insight into the objectives and the methodology of our NIST CSF risk assessment. We aim to identify and analyze risks and ensuring our security measures align with applicable regulations. Through this assessment, we aim to not only meet regulatory requirements but also to fortify our organization's security posture and enhance the overall protection of PHI.

**We encourage all stakeholders to review this report, as it lays the foundation for ongoing efforts to mitigate risks, maintain compliance, and continuously improve our security measures. We appreciate your collaboration and commitment to safeguarding the privacy and security of health information.**



Contents

[Executive Summary 4](#_Toc171690056)

[Objectives 5](#_Toc171690057)

[Scope of the Assessment 5](#_Toc171690058)

[Risk Assessment Methodology 5](#_Toc171690059)

[Risk Scoring Methodology 6](#_Toc171690060)

[Report Summary 8](#_Toc171690061)

[Appendix A: Detailed Controls Gap Analysis 9](#_Toc171690062)

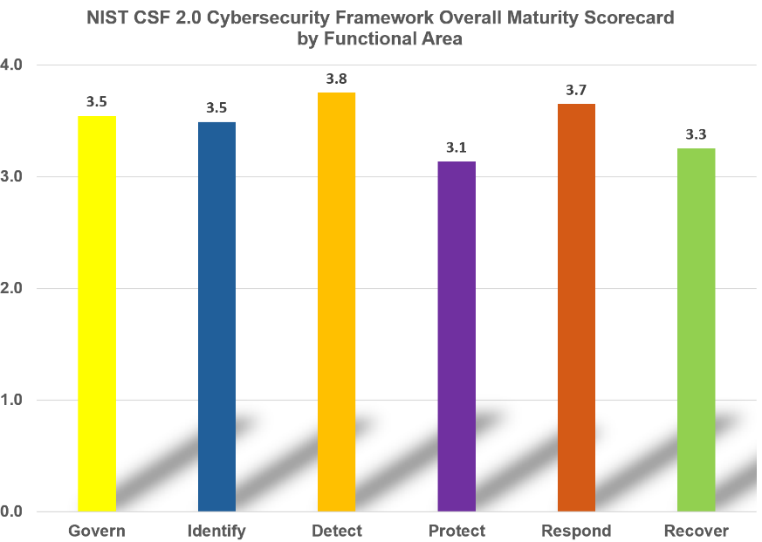
[Appendix B: Tactical Roadmap 28](#_Toc171690063)

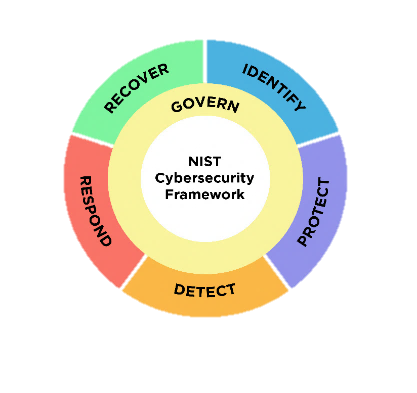
[Appendix C: Strategic Roadmap 29](#_Toc171690064)



# Executive Summary

From May to July of 2024, XXX conducted a NIST CSF risk assessment looking at 107 NIST CSF Subcategory controls to create a current baseline profile to determine information security risk. Maturity is based on a scale from 1 - 4 as defined on the NIST CSF Tiering definitions rubric. Overall, XXX scored an overall average of 3.4 out of 4. Though there are areas of improvement for some of the NIST CSF Subcategories, XXX illustrates an effective security program.

XXX's cybersecurity program is performing well compared to the broader healthcare sector as highlighted in both the [2023 HIMSS Healthcare Cybersecurity Survey](https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf) and the [Ponemon Institute Healthcare Cybersecurity Report 2023](https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf). XXX's focused and mature approach, with specific plans for addressing identified gaps and high alignment with NIST CSF 2.0 framework, puts it ahead in terms of structured cybersecurity risk management. The detailed NIST CSF 2.0 Risk Assessment for XXX indicates a robust and well-managed cybersecurity posture, with an average maturity score of 3.4 out of 4, and active mitigation of identified gaps such as MFA implementation and logging. In contrast, the HIMSS survey reveals ongoing challenges in workforce management and resource allocation across the sector, despite flat budgets. Additionally, the Ponemon report highlights significant financial impacts and patient care disruptions, with 88% of healthcare organizations facing an average of 40 attacks annually. This comparison suggests that XXX is performing better than the industry average in managing cybersecurity risks and maintaining a resilient cybersecurity framework.



There were eighteen (18) gaps noted: 1 Very High, 0 high, 10 Moderate, and 7 low. The identified gaps could impact systems that transmit, store, and/or process ePHI. Those systems are Edifecs, XXXDirect, Amisys, CARE, Change Healthcare, Claims Xten, ComCom, Cypress, Docustream, Enrollment HUB, MultiPlan, Northwood, OptumHealth, Amazon Web Services. (e.g., lack of logging)

This report provides insight into the objectives, methodology, identified gaps, tactical roadmap and strategic roadmap of our NIST CSF risk assessment. We aim to identify and analyze risks while ensuring our security measures align with NIST CSF 2.0 framework. Through this assessment, we aim to not only meet regulatory requirements but also to fortify our organization's security posture and enhance the overall protection of PHI. In addition, this document will address the tactical, strategic plan, metrics and continuous monitoring programs.

We encourage all stakeholders to review this report, as it lays the foundation for ongoing efforts to mitigate risks, minimize adverse impacts, maintain compliance, and continuously improve our security measures. We appreciate your collaboration and commitment to safeguarding the security of health information.

# Objectives

The primary objectives of the Annual XXX NIST CSF risk assessment are to:

* Discover and document potential risks to the security of PHI using an industry standard framework.
* Identify threats and vulnerability to each gap identified.
* Assess the potential impact and likelihood of identified gap.
* Ensure that the organization's policies and procedures align with HIPAA requirements.
* Identify gaps in the current security measures.
* Identify current mitigating security control strength
* Develop strategies and action plans to mitigate and manage identified risks effectively.
* Develop a tactical and strategic roadmap.

# Scope of the Assessment

The scope of the NIST CSF 2.0 analysis focuses on asset and data management, ensuring that inventories of hardware, software, and critical assets are up-to-date, implementing robust identity and access management controls, encrypting data both at rest and in transit, and securing all platforms, including cloud services, are necessary protective measures. Continuous monitoring for irregular activity, analyzing incidents to understand their impact, and recovery planning to ensure timely restoration of normal operations, with communication to relevant stakeholders. Furthermore, managing cybersecurity risks associated with suppliers, including contractual provisions for incident response, providing regular employee training on cybersecurity, and regularly auditing and assessing practices to ensure compliance and identify improvement areas are critical components of the scope

# Risk Assessment Methodology

In conducting the Annual NIST CSF risk assessment, information was gathered from several sources to understand and evaluate XXX’s security landscape against NIST CSF. The process began with identifying all ePHI information systems, networks, hardware, software, and personnel. The assessment attempts to identify potential threats and technical failures by a lack of proper security controls. Simultaneously, vulnerabilities in systems and processes are assessed, often involving thorough reviews of configurations, penetration testing results, and an analysis of existing security controls. The effectiveness of current security measures, such as access controls, encryption, and incident response procedures, is also evaluated.

The assessment followed the guidelines and standards outlined in the NIST CSF for guidance in safeguarding PHI. Additionally, regulatory compliance requirements pertinent to XXX’s operations were considered, ensuring alignment with NIST CSF. The process incorporated interviews with key stakeholders, documentation reviews, and analyses of historical data, including past security assessments and pen testing reports. The culmination of this information allowed for a holistic understanding of XXX’s information security risk landscape, and facilitating informed decision-making for risk prioritization and mitigation strategies.

Emphasizing a holistic security management process, NIST CSF dives into key components such as risk assessment, policy development, workforce training, and ongoing monitoring. NIST CSF sheds light on technical safeguards, including access controls, audit controls, and integrity controls, offering insights into their implementation and maintenance to secure electronic health information.

The methodology followed the following steps:

1. **Organizational Context**

* Gain an understanding of the business mission
* Gain an understanding of Stakeholder expectations
* Legal, regulatory, and contractual requirements
* Dependencies (critical objectives, capabilities, and services)

1. **Current Cybersecurity Profile**

* Document the current status of each subcategory, providing a detailed assessment of the organization’s current cybersecurity capabilities

1. **Gap Analysis**

* Compare the current and target profiles to identify areas needing improvement
* Document specific gaps in each function, category, and subcategory

1. **Mitigating Controls**

* Identify inherent risk and determine if mitigating controls exist
* Determine the strength of the mitigating controls

1. **Develop Plan of Action and Milestone (POA&Ms)**

* Outline steps to address the identified gaps
* Assign responsibilities, resources, and timelines for each action item

1. **Future Cybersecurity Profile**

* Define the desired outcomes for each function, category, and subcategory
* Prioritize these outcomes based on risk

1. **Continuous Monitoring**

* Ensure all POA&Ms are tracked to closure
* Ensure all current controls remain adequate

1. **Define Performance Measures and Metrics (KPIs/KRIs)**

* Define key performance indicators (KPIs) and metrics to track progress
* Establish a process for regularly reviewing and updating the profile

# Risk Scoring Methodology

We defined the scales for risk likelihood and impact. The likelihood scale ranges from 1 to 4, where 1 represents rare events that may happen once in many years, and 4 represents almost certain events that are very likely to occur frequently. Similarly, the impact scale ranges from 1 to 4, with 1 indicating minimal impact with negligible consequences and 4 indicating critical impact with catastrophic consequences such as significant financial loss and major reputational damage.

Next, we calculated the inherent risk, which is the risk present without any controls in place. This is done by multiplying the likelihood and impact scores. Since both scales are from 1 to 4, the inherent risk score ranges from 1 (1x1) to 16 (4x4).

Following this, we assessed the control strength using another 1-4 scale, where 1 signifies weak controls with minimal effectiveness and 4 signifies strong controls with high effectiveness.

Finally, we calculated the residual risk, which is the risk remaining after considering the effectiveness of the controls. This is done by dividing the inherent risk by the control strength. The residual risk score also ranges from 1 to 16, but it is scaled down based on the control strength.

For example, if a risk has a likelihood of 3 (likely) and an impact of 4 (critical), the inherent risk score would be 12. If the control strength is assessed as 3 (good), the residual risk would be calculated as 4 (12 divided by 3).

This process helps organizations to systematically evaluate, prioritize, and manage their cybersecurity risks by understanding both the inherent and residual risks associated with various scenarios

Example

1. **Define the Risk Likelihood and Impact Scales:**
   * **Likelihood Scale (1-4):**
     1. Rare: Extremely unlikely to occur (may happen once in many years)
     2. Unlikely: Possible but not expected to happen (may happen once every few years)
     3. Likely: Expected to happen occasionally (may happen annually)
     4. Almost Certain: Very likely to happen frequently (may happen multiple times a year)
   * **Impact Scale (1-4):**
     1. Low: Minimal impact, negligible consequences (e.g., minor inconvenience, no significant financial loss)
     2. Moderate: Noticeable impact, manageable consequences (e.g., some operational disruption, moderate financial loss)
     3. High: Significant impact, severe consequences (e.g., major operational disruption, substantial financial loss)
     4. Critical: Devastating impact, catastrophic consequences (e.g., complete operational halt, significant financial loss, major reputational damage)
2. **Calculate Inherent Risk:** Inherent Risk is determined by assessing both the likelihood and the impact of a risk occurring without any controls in place. This can be represented as:

*Inherent Risk(IR) = Likelihood (L) × Impact (I)*

Since both scales are 1-4, the inherent risk score will range from 1 (1x1) to 16 (4x4).

1. **Assess Control Strength:** Control strength will determine how effective existing controls are in reducing the risk. This also uses a 1-4 scale:
   * 1: Weak controls (minimal effectiveness)
   * 2: Fair controls (some effectiveness)
   * 3: Good controls (effective)
   * 4: Strong controls (highly effective)
2. **Calculate Residual Risk:** Residual Risk is the risk remaining after considering the effectiveness of controls. This can be represented as:

*Residual Risk (RR) = Control Strength (CS) / Inherent Risk (IR)*

The residual risk score will also range from 1 (1/1) to 16 (16/1), but since we divide by control strength (1-4), the effective range will be 1 to 16, scaled down depending on control strength.

# Report Summary

The 2024 NIST CSF 2.0 Risk Assessment Report for SAMPLE COMPANY (XXX) provides a comprehensive evaluation of the organization's cybersecurity posture, focusing on the protection of sensitive health information in compliance with HIPAA regulations. The report outlines the objectives, scope, and methodology of the risk assessment conducted between May and July 2024. It aims to identify, analyze, and mitigate potential risks to the confidentiality, integrity, and availability of protected health information (PHI). The assessment involved evaluating 107 controls based on the NIST CSF 2.0 framework, resulting in an overall maturity score of 3.4 out of 4. This score reflects an effective security program, though areas for improvement were identified.

The report highlights twenty-two gaps, categorized into critical, high, medium, and low risks, with none classified as critical. Key gaps include the presence of ePHI production data in the test environment, missing multi-factor authentication (MFA) on some internet-facing applications, and inadequate logging for critical ePHI systems. The report provides detailed mitigation strategies for each gap and emphasizes the importance of continuous monitoring and updating of security measures. The assessment's findings serve as a foundation for developing tactical and strategic roadmaps to enhance XXX's cybersecurity resilience and ensure compliance with regulatory requirements.

Overall, XXX's cybersecurity program appears to be performing better compared to the broader healthcare sector XXX's focused and mature approach, with specific plans for addressing identified gaps and high alignment with NIST CSF and HIPAA, puts it ahead in terms of structured cybersecurity risk management. The detailed NIST CSF 2.0 Risk Assessment for XXX indicates a robust and well-managed cybersecurity posture, with a maturity score of 3.4 out of 4, and active mitigation of identified gaps such as MFA implementation and logging.

# Appendix A: Detailed Controls Gap Analysis

| **Observation** | **Subcategory Impacted** | **Threats** | **Vulnerabilities** | **Likelihood of Threat or Vulnerability Attack Vector**  **(Inherent Risk with no Controls)** | **Impact of Threat or Vulnerability Attack Vector**  **(Inherent Impact with no Controls)** | **Inherent Risk [IR] Score** | **Strength of Compensating Control to Reduce Inherent Risk** | **Residual Risk Score** | **Observation** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **MFA missing on internet facing web applications** | **PR.AA-03**: Users, services, and hardware are authenticated  **ID.RA-05**: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization | Credential Theft, Brute Force Attack, Insider Threats, Man-in-the-Middle (MITM) Attacks, Phishing Attacks, Exploitation of Weak Authentication Protocols | Weak password policies, single factor authentication, unpatched software, Lack of MFA, inadequate user education, insecure storage credentials, lack of monitoring and logging | Almost Certain | Very High | 16 | Weak Control | 16 | Ensure MFA is enabled on internet facing web apps and critical systems.  Note: This observation is on the tactical roadmap to mitigate in 2024. |
| **XXX has ePHI production data in the test environment. This is inadequate process.** | **PR.DS-01**: The confidentiality, integrity, and availability of data-at-rest are protected  **PR.DS-02**: The confidentiality, integrity, and availability of data-in-transit are protected  **PR.AA-05**: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties | Data breaches, unauthorized access, malware attacks, insider threats, physical theft, ransomware, data tampering | Weak encryption, improper access controls, outdated storage solutions, lack of monitoring, inadequate backup, poor data management policies, insufficient incident response | Almost Certain | Very High | 16 | Fair Controls | 8 | Production data in test.  Note: There are mitigating controls in place, such as a workforce needs access to the network and access to the test environment. |
| **XXX’s network is flat, which means that if one device falls victim to malware, it could impact all other devices on the network.** | **PR.IR-01**: Networks and environments are protected from unauthorized logical access and usage | Unauthorized access, data breaches, malware, insider threats, network attacks, system compromise, exploitation of vulnerabilities | Weak access controls, insufficient network segmentation, poor monitoring, outdated security protocols, inadequate logging, lack of multi-factor authentication, insufficient training | Almost Certain | Very High | 16 | Fair Controls | 8 | There is limited segmentation on the network. Segmentation is important because is there is a malware outbreak it could impact the entire network instead of a segment.  Note: There is a micro-segmentation project in progress, so this still has to be called out |
| **XXX has limited access control reviews on ePHI systems.** | **PR.AA-04**: Identity assertions are protected, conveyed, and verified | Interception of identity assertions, replay attacks, man-in-the-middle attacks, forgery of identity assertions, credential stuffing, session hijacking, exploitation of weak verification protocols | Unencrypted transmission, lack of token expiry, weak encryption algorithms, insufficient validation checks, insecure storage, inadequate monitoring, poor session management | Unlikely | Moderate | 6 | Weak Control | 6 | There is limited comprehensive review of access control for systems that process, transmit, or store ePHI on a specified frequency. Lack of access control reviews could lead to a potential past employee or a current transfer employee having more access than they need or having access after they leave XXX  Note: Currently, there is no mitigating control. XXX should ensure that access to ePHI systems is reviewed on a determined frequency (Month, Quarterly). However, users are removed from ePHI systems upon termination of employment and that's what keeps this control to a medium residual risk. |
| **XXX does not have data de-identification in the test environment.** | **PR.DS-06**: Sensitive data is de-identified or masked as appropriate to protect its confidentiality and prevent unauthorized access or exposure. | Insider threats, unauthorized access, malware, data tampering, process hijacking, data leaks, exploitation of vulnerabilities | Insecure processing environments, lack of monitoring, insufficient access controls, outdated systems, weak application security, poor data handling practices, inadequate encryption | Almost Certain | High | 12 | Fair Controls | 6 | Data is not de-identified in the test environment. This leaves ePHI exposed to unauthorized access  Note: There are mitigating controls in place, such as a workforce needs access to the network and access to the test environment. |
| **There is limited RBAC in Amysis.** | **PR.DS-10**: The confidentiality, integrity, and availability of data-in-use are protected | Insider threats, unauthorized access, malware, data tampering, process hijacking, data leaks, exploitation of vulnerabilities | Insecure processing environments, lack of monitoring, insufficient access controls, outdated systems, weak application security, poor data handling practices, inadequate encryption | Almost Certain | High | 12 | Fair Controls | 6 | Amisys has PHI and there are only two roles in amisys. A user role and an admin role. PHI is not restricted to users that have a need-to-know basis. The CP038POL Confidentiality of System Security Information states, "It is XXX’s policy to limit access to and disclosure of XXX’s System Security Information to those who have a legitimate need to know the information in order to perform the specific functions of their jobs" In addition, there is prod data in test |
| **XXX has a limited manual source code review and training for developers.** | **PR.PS-06**: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle | Software vulnerabilities, unauthorized access, malware, code injection attacks, insider threats, supply chain attacks, software tampering | Inadequate secure development practices, insufficient code review, lack of security testing, poor version control, inadequate developer training, weak access controls, outdated development tools | Likely | Moderate | 6 | Weak Control | 6 | There is not a comprehensive guide provided to all developers that outlines required security practices, such as input validation, encryption of sensitive data, and error handling. There needs to be developer training on creating secure code. There is no DAST or SAST.  Note: Efforts are underway to find a solution for source code reviews. |
| **XXX does not have a process to test incident response plans with tier 1 vendors.** | **GV.SC-08**: Relevant 3rd Parties and other third parties are included in incident planning, response, and recovery activities  **GV.SC-09**: 3rd Party security practices are integrated into cybersecurity and enterprise information security programs, and their performance is monitored throughout the technology product and service life cycle  **DE.CM-06**: External service provider activities and services are monitored to find potentially adverse events  **GV.SC-01**: A cybersecurity 3rd Party information security program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders | Supply chain attacks, unauthorized access, data breaches, service disruptions, counterfeit products, insider threats, third-party vulnerabilities | Poor incident planning, lack of supplier involvement, inadequate response plans, insufficient communication, weak recovery strategies, inadequate training, insufficient resources | Likely | High | 12 | Fair Controls | 6 | There should be incident response testing with tier 1 vendors to ensure both parties are prepared for an adverse event.  Note: Current discussions with Vendor Management is underway to enhance the Vendor Management program. |
| **XXX has limited cyber threat intelligence gathering.** | **ID.RA-02**: Cyber threat intelligence is received from information sharing forums and sources | Emerging threats, sophisticated cyber-attacks, insider threats, data breaches, service disruptions, malware, unauthorized access | Lack of threat intelligence sources, inadequate information sharing, insufficient monitoring, poor access controls, outdated threat management processes, weak incident response plans, inadequate training | Unlikely | Moderate | 6 | Weak Control | 6 | Enhance cyber threat intelligence that could impact XXX.  Note: There are some intelligence gathering but further enhancements should be acquired. For example, H-ISAC, Feedly Threat Management. |
| **XXX has outdated BCP/BIA plans.** | **GV.OC-04**: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated | Service disruptions, loss of stakeholder trust, unmet stakeholder expectations | Inadequate understanding of critical services, poor communication of capabilities, insufficient service continuity planning | Likely | High | 9 | Fair Controls | 5 | BCPs Need to be updated. There is a project in progress that is working on updating the BCPs and BIAs |
| **XXX has limited logging, especially for ePHI systems.** | **DE.CM-01**: Networks and network services are monitored to find potentially adverse events | Unauthorized access, network attacks, malware, insider threats, data breaches, DDoS attacks, man-in-the-middle attacks | Inadequate monitoring tools, poor network visibility, lack of real-time monitoring, weak access controls, outdated security protocols, insufficient logging, lack of trained personnel | Likely | High | 9 | Fair Controls | 5 | There is limited logging and monitoring on key ePHI systems. For example, Amisys, Edifecs, XXXDirect, CARE, Claims Xten, ComCom, Cypress, Docustream, Enrollment HUB are not sending logs to Exabeam  Note: There are efforts underway to research the ePHI systems to determine if logging is technically feasible from these systems for input in the SIEM solution. |
| **CSM database is running on old MS Access technology that is no longer supported.** | **PR.PS-02**: Software is maintained, replaced, and removed commensurate with risk | Vulnerability exploitation, outdated software, malware, unauthorized access, insider threats, system failures, data breaches | Lack of update policies, inadequate patch management, insufficient monitoring, outdated software, poor inventory management, lack of testing, weak access controls | Unlikely | Low | 4 | Weak Control | 4 | The Customer Service Management system is running on an outdated and unsupported MS Access database. However, network access is required.  Note: Ensure access is limited to the CSM database to ensure data integrity. |
| **XXX does not have an exception management process.** | **ID.RA-07**: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked | Unauthorized access, data breaches, malware, insider threats, service disruptions, sophisticated cyber-attacks, data loss | Poor change and exception management, inadequate risk impact assessments, insufficient recording and tracking, weak access controls, lack of incident response plans, outdated risk management policies, inadequate training | Unlikely | Low | 4 | Weak Control | 4 | An exceptions policy needs to be documented. High & Critical need to go Casey.  Note: Create a policy exception process that reviews threats and likelihoods and compensating controls review. |
| **XXX uses generic and shared accounts.** | **PR.AA-01**: Identities and credentials for authorized users, services, and hardware are managed by the organization | Credential theft, unauthorized access, insider threats, brute force attacks, phishing attacks, man-in-the-middle attacks, social engineering attacks | Weak password policies, inadequate credential management systems, insufficient access controls, lack of multi-factor authentication, outdated identity management protocols, unpatched software vulnerabilities, poor user training | Unlikely | Medium | 4 | Fair Controls | 2 | Generic/Shared account should be prohibited unless there is an exception and there are technical controls to verify who is using the account.  Note: All shared/generic/application-to-application accounts should have an owner and those accounts should go into the PAM solution. |
| **XXX should update the incident response plans based on NIST CSF controls and best practices.** | **GV.SC-02**: Cybersecurity roles and responsibilities for 3rd Parties, customers, and partners are established, communicated, and coordinated internally and externally  **RS.MA-01**: The incident response plan is executed in coordination with relevant third parties once an incident is declared  **RS.CO-02**: Internal and external stakeholders are notified of incidents  **RC.RP-02**: Recovery actions are selected, scoped, prioritized, and performed  **RC.RP-03**: The integrity of backups and other restoration assets is verified before using them for restoration  **RC.RP-04**: Critical mission functions and cybersecurity information security are considered to establish post-incident operational norms  **RC.RP-05**: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed  **RC.RP-06**: The end of incident recovery is declared based on criteria, and incident-related documentation is completed  **RC.CO-03**: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders  **PR.AT-02**: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind | Role confusion, unmanaged supply chain risks, communication breakdowns | Undefined roles and responsibilities, poor communication, inadequate coordination | Unlikely | Medium | 4 | Fair Controls | 2 | Incident response plans need to be updated. The following components should be included:  1. How will XXX work with 3rd Parties before, during, and after an event  2. Update the policy or SOP about who needs to be notified and how notification will be sent (e.g., text, call)  3. Ensure IR Policy, SOP, and playbooks, have documentation on how recovery actions are planned, including criteria for selecting, scoping, and prioritizing these actions.  4. Ensure there are procedures in the SOP and Playbooks that outline how the integrity of backups and restoration assets is checked, including the tools and methods used.  5. Create a section in the IR SOP that mentions how policy and organizational adjustments will be made and add functions that verify the integrity of the restored assets and update the SOP  6. Create criteria that specify what conditions must be met to declare the end of an incident recovery, including system checks, security verifications, and business operations assessments in the SOP.  7. Develop guidelines that specify what information should be shared, with whom, under what circumstances, and through what channels.  8. There is no targeted training for certain job roles that could impact security. For example, and IT Admin should be trained on how to secure their systems or be able to identify anomalies |
| **XXX has limited security standards for configuration implementation** | **PR.PS-01**: Configuration management practices are established and applied | Unauthorized changes, misconfigurations, malware, insider threats, system failures, exploitation of vulnerabilities, data breaches | Lack of configuration policies, inadequate change management, insufficient monitoring, outdated systems, poor documentation, lack of training, weak access controls | Unlikely | Low | 2 | Fair Controls | 1 | Limited standards for consistent control configuration implementation.  Note: there are some procedures that act as standards. These should be broken apart so there is consistency with the implementation of controls. |
| **XXX’s JDs do not have which job role is allowed to access ePHI.** | **GV.RR-02**: Roles, responsibilities, and authorities related to cybersecurity information security are established, communicated, understood, and enforced | Role confusion, unmanaged risks, lack of accountability | Undefined roles and responsibilities, poor communication, inadequate enforcement | Unlikely | Low | 2 | Fair Controls | 1 | Job descriptions help identify particular skills or abilities necessary for a given position. There is a lack of Job Descriptions that specifically state what data a user can access, for example, ePHI. This will help IT determine what systems they are allowed to access. |
| **XXX should implement a communication plan when policies are updated.** | **GV.PO-01**: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced  **GV.PO-02**: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission  **ID.IM-03**: Improvements are identified from execution of operational processes, procedures, and activities | Non-compliance, unmanaged risks, policy violations | Lack of clear policies, poor communication, inadequate enforcement | Unlikely | Low | 2 | Fair Controls | 1 | There are no Policy communication when updates are made |

# Appendix B: Tactical Roadmap



# Appendix C: Strategic Roadmap

The following strategic plan builds on an already strong information security program.

A diagram of data retention

Description automatically generated

* Current Mitigation: Continue to follow through with the tactical information security plan.
* Logging & Monitoring Program: Develop a thorough logging and monitoring program to ensure threats and vulnerabilities are identified quickly to address risks such as ransomware attacks.
* Data Retention and Destruction Program: Develop a data retention and destruction program to identify data that needs to be kept for a certain timeframe and destroyed after that timeframe. For example, how long should we keep email?
* 3rd Party Risk Management: Enhance the vendor management program to include the review of applicable security certification, if feasible.
* Continuous Monitoring Program. Develop a continuous controls monitoring program to ensure controls stay adequate. This can be done through Governance, Risk and Compliance (GRC) platforms, such as ControlMap.
* Security Resources: Acquire an additional security analyst to ensure that the implementation of security controls is managed and monitored continuously.

**Metrics**

The security metrics program is in its infancy. Over the course of time, more metrics will be identified and measure, as needed. The following metrics will be the first metrics to capture

**Vulnerability Measure**

* **Metric**: Percentage (%) of high vulnerabilities mitigated within organizationally defined time periods after discovery / (Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period)\*100
* **Goal**: Ensure all vulnerabilities are identified and mitigated

**Security Training Measure**

* **Metric**: Percentage (%) of information system security personnel that have received security / (Number of information system security personnel that have completed security training within the past year/total number of information system security personnel) \*100
* **Goal**: Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities

**Risk Assessment Mitigation**

* **Metric**: Percentage (%) of risks remediated within organization-specified time frames / (Number of risks remediated according to POA&M schedule/total number of POA&M) \*100
* **Goal**: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems