

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

**Completion:** MM/DD/YYY

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

**Applicability:** Organization Company-wide

BLANK PAGE

|  |  |
| --- | --- |
| SUMMARY | |
| The Information Security Team is pleased to present this overview of the annual Heath New England (HNE) NIST+ CSF 2.0 Risk Assessment. NIST Cyber Security Framework (CSF) is a framework that is used for the protection of sensitive health information, and our commitment to information security necessitates a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information (PHI).  This report provides insight into the objectives and methodology of our NIST CSF risk assessment. We aim to identify and analyze risks, ensuring our security measures align with HIPAA 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. | |
|  | Decorative |
| SUMMARY |
| The Information Security Team is pleased to present this overview of the annual Heath New England (HNE) NIST+ CSF 2.0 Risk Assessment. NIST Cyber Security Framework (CSF) is a framework that is used for the protection of sensitive health information, and our commitment to information security necessitates a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information (PHI).  This report provides insight into the objectives and methodology of our NIST CSF risk assessment. We aim to identify and analyze risks, ensuring our security measures align with HIPAA 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. |



SUMMARY

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

This report provides insight into the objectives and methodology of our NIST CSF risk assessment. We aim to identify and analyze risks, ensuring our security measures align with HIPAA 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.**



TOC



Introduction

The Information Security Team is pleased to present this overview of the annual NIST CSF 2.0 Risk Assessment. The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of sensitive health information, HNE uses the NIST CSF to identify risks and mitigation strategies to reduce that risk of adverse events. HNE requires a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information (PHI).

This report provides insight into the objectives and methodology of our NIST CSF risk assessment. We aim to identify and analyze risks, ensuring our security measures align with HIPAA 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. In addition, this document will roadmap the tactical and strategic plan.

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 privacy and security of health information.

# Objectives

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

* Discover and document potential risks to the security of PHI.
* Assess the potential impact and likelihood of each identified risk on the confidentiality, integrity, and availability of PHI.
* Ensure that the organization's policies and procedures align with HIPAA requirements.
* Identify gaps in the current security measures.
* Develop strategies and action plans to mitigate and manage identified risks effectively.
* Maintain thorough documentation of the risk assessment process, findings, and recommendations.
* Establish a framework for continuous monitoring, auditing, and updating security measures to adapt to evolving threats and changes in the organization's environment.

# Regulatory Framework

The HIPAA Security Rules are integral to the Health Insurance Portability and Accountability Act, designed to safeguard the confidentiality, integrity, and availability of protected health information (PHI). The Security Rule establishes standards for the security of electronic PHI, requiring healthcare organizations to implement measures such as access controls, encryption, and audit trails to protect sensitive data. This rule aims to ensure the security of PHI and maintain the trust and integrity of the healthcare system.

Though HIPAA does not explicitly require an *annual* risk assessment, it does mandate *regular* risk assessments as part of its security rule. The HIPAA Security Rule requires covered to conduct a risk analysis, which involves identifying and assessing potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI). This process must be ongoing and not just a one-time activity. While the frequency of these assessments is not specified, best practices suggest conducting them at least annually or whenever there are significant changes in the organization’s operations, systems, or environment Regular assessments help organizations identify new threats and vulnerabilities, ensuring that security measures remain effective and appropriate.

# Risk Assessment Methodology

In conducting the Annual NIST CSF risk assessment, information was gathered from several sources to understand and evaluate HNE’s security landscape against NIST CSF. The process began with identifying all information systems that process, transmit, or store ePHI, encompassing data repositories, systems, networks, hardware, software, and personnel. The assessment attempt so identify potential threats, malicious attacks, and technical failures (BCP/DRP). Simultaneously, vulnerabilities in systems and processes are assessed, often involving thorough reviews of configurations, penetration testing, 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 HIPAA Security Rule and NIST CSF for guidance in safeguarding PHI. Additionally, regulatory compliance requirements pertinent to HNE’s operations were considered, ensuring alignment with HIPAA/NIS TCSF. The process incorporated interviews with key stakeholders, documentation reviews, and analyses of historical data, including past security assessments. The culmination of this information allowed for a holistic understanding of HNE’s risk landscape, facilitating informed decision-making for risk prioritization and mitigation strategies.

Within the landscape of healthcare information security, the National Institute of Standards and Technology (NIST) has crafted a guide known as NIST 800-66. This guide, titled "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," serves as a comprehensive roadmap for ORGANIZATION to fortify their information technology security practices.

At its core, NIST CSF provides the overarching scope and purpose of the HIPAA Security Rule, emphasizing the safeguard electronic protected health information (ePHI). Acting as a foundational resource, the guide illuminates the security requirements mandated by HIPAA, paving the way for organizations to align their practices accordingly.

Emphasizing a holistic security management process, NIST CSF and NIST 800-66 delves into key components such as risk assessment, policy development, workforce training, and ongoing monitoring. The guide 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.

Additionally, NIST CSF and NIST 800-66 underscores the importance of incident response and contingency planning. It provides guidance on developing effective strategies to respond to security incidents and ensuring business continuity in the face of disruptions.

The guide also places significance on security awareness and training programs, recognizing their pivotal role in cultivating a culture of security within healthcare organizations. By offering guidance on educating staff to recognize and address security risks, NIST CSF and NIST 800-66 aims to fortify the human element in information security.

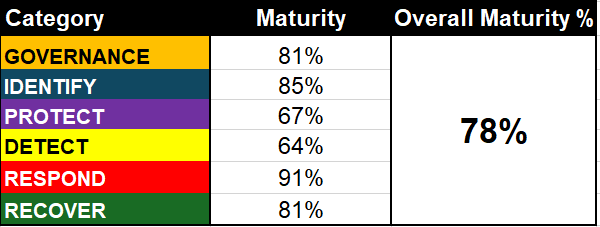
Finally, NIST CSF and NIST 800-66 advocates for ongoing compliance monitoring and evaluation of security controls. It encourages organizations to regularly assess and update their security measures, aligning them with evolving threats and technological advancements.

In essence, NIST CSF and NIST 800-66 emerges as a vital resources, guiding healthcare organizations through the intricate landscape of HIPAA compliance. Its practical insights empower entities to fortify their information technology security, ensuring the confidentiality, integrity, and availability of electronic protected health information.

| Risk Identification | | | | |
| --- | --- | --- | --- | --- |
| **Observation** | **Risk Statement** | **How to Mitigate** | **Current Mitigation Actions** | **Risk Level** |
| HNE has ePHI production data in the test environment | Using electronic protected health information (ePHI) production data in the test environment can lead to unauthorized access and exposure of sensitive patient information. This practice increases the risk of data breaches, violates regulatory compliance requirements, and can result in significant financial penalties, loss of patient trust, and reputational harm to the organization | Data de-identification is essential, involving techniques such as anonymization, pseudonymization, and data masking to ensure that data cannot be traced back to individuals. Alternatively, synthetic data that mimics the statistical properties of real data can be used. Access controls, including strict authorization measures and role-based access control (RBAC), should be established to limit access to ePHI. Additionally, isolating test environments from production environments and employing network segmentation can prevent data cross-contamination and control access effectively |  | **HIGH** |
| Flat network / Non-segmented network | Having a flat network with no network segmentation can lead to increased vulnerability to cyberattacks, as a single compromised device can provide attackers with unfettered access to the entire network. This lack of segmentation can result in widespread data breaches, unauthorized access to sensitive information, regulatory non-compliance, significant financial losses, and severe damage to the organization's reputation | Implement network segmentation. By dividing the network into smaller, isolated segments, organizations can limit the spread of cyberattacks and reduce the impact of a single compromised device. Each segment can be secured independently, ensuring that sensitive information and critical systems are protected even if one part of the network is breached. This approach not only helps in containing potential data breaches but also improves overall network performance and security | Micro-segmentation project | **MEDIUM** |
| MFA missing on some internet facing web applications | Absence of multi-factor authentication (MFA) on internet-facing applications significantly increases the risk of unauthorized access and cyberattacks. This vulnerability can lead to data breaches, exposure of sensitive information, regulatory non-compliance, substantial financial losses, and severe damage to the organization's reputation and trustworthiness | First and foremost, deploying MFA across all internet-facing applications is crucial. This added layer of security ensures that only authorized users can access sensitive information and critical systems |  | **HIGH** |
| HNE does not have an updated Business Continuity plan as per §164.308(a)(7)(i) which states, "Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information." In addition to prevention, the goal is to enable ongoing operations before and during the execution of disaster recovery. Business continuity is the intended outcome of properly executing business continuity planning and disaster recovery. With a Business Continuity Plan, HNE will know how to keep the business going during an adverse incident | Absence of a formal Business Continuity Program and a comprehensive Business Impact Risk Analysis may result in prolonged operational disruptions and an inability to promptly restore critical healthcare services during emergencies or disasters. This can lead to significant patient care delays, financial losses, non-compliance with regulatory requirements, and diminished organizational reputation | To ensure the effectiveness of a Business Continuity Program (BCP) and Business Impact Analysis (BIA), healthcare organizations must prioritize regular updates and revisions. This involves continuously monitoring and reviewing both the BCP and BIA to identify areas for improvement. Lessons learned from actual incidents and drills should be incorporated to enhance the plans. |  | **HIGH** |
| Logs are not being captured for all critical ePHI systems. Logs are being captured from security solutions. HIPAA §164.312(b) states that all required covered entities implement hardware, software and/or procedure mechanisms that record (log) and examine (audit) activity in information systems that contain or use electronic protected heath information (ePHI).  HNE’s security solutions do no contain ePHI. Log monitoring and regular reviews are part of ensuring compliance with this requirement to detect and address any unauthorized access to ePHI. | Not having centralized security logs can lead to fragmented and incomplete visibility of security events across the organization. This may result in delayed detection and response to security incidents, increased vulnerability to cyberattacks, compliance violations, and potentially severe financial and reputational damage due to undetected or unresolved security breaches | Implement a centralized logging system that aggregates security logs from all critical systems and applications. This centralized approach ensures comprehensive visibility of security events across the organization, enabling quicker detection and response to potential security incidents. By consolidating logs into a single system, security teams can more efficiently monitor, analyze, and correlate events, which helps in identifying patterns and anomalies indicative of cyberattacks. Regularly maintaining and auditing this centralized log system ensures that it remains effective and that logs are collected consistently from all relevant sources. |  |  |
| HIPAA §164.308(a)(6)(i) states that covered entities must implement policies and procedures to address security incidents. The standard specifically mandates the identification and response to suspected or known security incidents, mitigating their harmful effects, and documenting incidents and their outcomes in an orderly fashion. The incident response (IR) policy and procedure needs to be updated to include who needs to be notified, how to communicate, and when in the when in the event of an incident. In addition, the IR policy needs to be update to include guidelines that specify what information will be shared, with whom, under what circumstances, and through what channels. Furthermore, ensure there are logs or records that detail the information shared with stakeholders, including the date, the type of information, the recipient, and the purpose of sharing. Next, The IR policy, SOP, and playbooks, need documentation on how recovery actions are planned, including criteria for selecting, scoping, and prioritizing these actions. Finally, the IR policy should state when an incident is completed, communicated, and closed. | An incomplete incident response program can result in delayed identification, containment, and mitigation of security incidents. This may lead to prolonged data breaches, increased damage to information systems, non-compliance with regulatory requirements, significant financial losses, and erosion of stakeholder trust and organizational reputation | Update the incident response plan |  |  |
| HIPAA §164.308(a)(4) states that access to ePHI is formally granted to only those that have a need-to-know basis. Developers should not have access to ePHI. There is production (ePHI/PII) data in the test environment. There are privacy concerns with having production data in test. Production data often includes ePHI/PII. Using real user data in a test environment increases the risk exposure of sensitive information to workforce members that are not authorized to see the sensitive information. This could lead to potential breach and harm to individuals whose data is being used. | Unauthorized access to electronic protected health information (ePHI) can lead to the exposure of sensitive patient data, resulting in potential identity theft, financial fraud, and violation of patient privacy. This breach of confidentiality can incur substantial legal and regulatory penalties, damage the organization’s reputation, erode patient trust, and lead to significant financial losses |  |  |  |
| There is no 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 ORGANIZATION | Failure to regularly review and update access controls in electronic protected health information (ePHI) systems may result in unauthorized access, misuse, or data breaches. This can lead to compromised patient confidentiality, regulatory non-compliance, substantial financial penalties, loss of patient trust, and significant reputational damage to the organization |  |  |  |
| 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. | Failing to define appropriate data access requirements in job descriptions can lead to employees having unauthorized or excessive access to sensitive information. This oversight increases the risk of data exposure, misuse of information, regulatory non-compliance, potential financial losses, and damage to the organization's reputation and trust |  |  |  |
| Limited security architectural and data flow diagrams documentation | The absence of security architectural and data flow diagrams can result in an incomplete understanding of the system’s security posture and data movement. This lack of visibility may lead to undetected vulnerabilities, inefficient incident response, non-compliance with regulatory requirements, potential data breaches, and significant financial and reputational damage |  |  |  |
| Third Party Risk Management. §164.308(a)(1)(ii)(A) - Requires entities to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity or business associate Terms of Services are not reviewed. HNE does not review 3rd Party security certifications, if available. | Failure to conduct a comprehensive risk analysis on third-party vendors and business associates that handle protected health information (PHI) may result in unauthorized access, data breaches, and non-compliance with HIPAA regulations, potentially leading to significant financial penalties, reputational damage, and loss of patient trust. |  |  |  |
| Data retention and destruction process | Absence of a formal data retention and destruction process can lead to the improper handling of sensitive information, resulting in unauthorized access, data breaches, and non-compliance with regulatory requirements. This can cause significant legal and financial penalties, reputational damage, and loss of stakeholder trust. |  |  |  |
| Policy communication when updates are made | Failure to effectively communicate updates to policies and standards to employees can lead to non-compliance with current security protocols and regulatory requirements. This lack of awareness may result in increased risk of security breaches, operational inefficiencies, potential legal and financial penalties, and damage to the organization's reputation and trustworthiness. |  |  |  |
| Clear passwords in text file on network server | Storing clear text passwords in a text file on a shared server significantly increases the risk of unauthorized access to sensitive systems and data. This practice can lead to security breaches, data theft, non-compliance with regulatory standards, substantial financial losses, and severe reputational damage to the organization |  | Add the user IDs and password to Delinea Privileged Access Management (PAM) Tool | HIGH |
| Limited standards for consistent control implementation | Limited or no security configuration standards for managing can result in inconsistent application of security controls, leaving systems vulnerable to unauthorized access and data breaches. This inconsistency can lead to regulatory non-compliance, increased risk of security incidents, significant financial losses, and damage to the organization's reputation |  |  |  |
| There is no code scanning | Not implementing a code scanning review to detect potential vulnerabilities can result in the deployment of insecure applications. This lack of proactive vulnerability management increases the risk of security breaches, data exposure, regulatory non-compliance, substantial financial losses, and significant damage to the organization's reputation |  |  |  |
| The Customer Service Management system is running on an outdated and unsupported MS Access database | MS Access has reached end-of-life as of October 13, 2020. Using MS Access without access controls to store CSM information can lead to unauthorized access, data exposure, and misuse of potential sensitive customer data. This risk increases the possibility of regulatory non-compliance, substantial financial loses, loss of customer trust, and potential dame to the organizations reputation. |  |  |  |
| There is no role-based access control for the Amysis environment | Absence of role-based access control for an electronic protected health information (ePHI) system can result in unauthorized access to sensitive patient data. This lack of access control increases the risk of data breaches, misuse of information, regulatory non-compliance, substantial financial penalties, and significant damage to the organization's reputation and trust |  |  |  |
| 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 | Not providing targeted information security training for different roles within the organization can lead to inadequate understanding of security practices and procedures. This one-size-fits-all approach may result in inefficient use of training time, increased risk of security incidents, regulatory non-compliance, and potential data breaches. Ultimately, it can cause significant financial losses, operational disruptions, and damage to the organization's reputation |  |  |  |



# 2024 Maturity Result by NIST CSF Functions

In 2022, ORGANIZATION conducted a HIPAA risk assessment looking at 120 controls to create a baseline for the minimum level of security and privacy to identify risks. Physical Safeguards do not apply to ORGANIZATION as ORGANIZATION is 100% remote workforce. Physical safeguards are handled by ORGANIZATION third-party computing services. ORGANIZATION did not use a framework for the 2022 and past assessments.

In 2023, ORGANIZATION used NIST 800-66r1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.” NIST 800-66r1 summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. The publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule.

# Summary for each NIST CSF Functions

**Governance**

The organization demonstrates a commendable level of compliance with administrative controls, scoring at 85%. This reflects a robust implementation of measures governing security management processes, workforce training, and information access management. However, there may be areas for improvement to achieve full compliance. See Risk Register for more information on observations.

**Identify**

Given the organization's 100% remote nature, the HIPAA standard 164.310 for physical safeguards does not apply. Remote organizations are exempt from certain physical security requirements, acknowledging the unique operational context.

**Detect:**

The organization is 82% compliant with technical safeguards, indicating a substantial adherence to security measures related to access controls, audit controls, integrity controls, and transmission security. While a strong foundation is in place, there may be opportunities to enhance compliance in specific technical areas.

**Protect:**

The organization demonstrates exemplary compliance with organizational requirements, achieving a perfect score of 100%. This reflects a robust commitment to implementing policies and procedures to protect electronic protected health information (ePHI) and manage potential risks effectively.

**Respond:**

The organization is fully compliant with policies, procedures, documentation, and requirements, achieving a 100% score. This indicates a comprehensive and well-documented approach to maintaining and implementing policies that safeguard ePHI in accordance with HIPAA regulations.

Recover

Tactical Goal for 2024/2025

Remediation

**Key Steps in the Remediation Process:**

1. **Detailed Analysis:** Conduct an in-depth analysis of each finding to understand its root cause, potential impact, and the optimal path for resolution. Engage relevant stakeholders to gain diverse perspectives on the identified issues.
2. **Prioritization:** Prioritize the findings based on their criticality and potential risk to our organization.
3. **Action Plans:** Develop detailed action plans for each finding, outlining specific steps, responsible parties, and timelines for resolution. These plans should be comprehensive, addressing not only the immediate concerns but also establishing preventive measures for the future.
4. **Collaborative Efforts:** Remediation is a collective effort. Engage cross-functional teams, involving IT, security, compliance, and relevant business units to collaboratively work towards resolving the findings. Foster clear communication channels to ensure everyone is aligned on the remediation goals.
5. **Continuous Monitoring:** Implement continuous monitoring mechanisms to track the progress of remediation efforts. Regularly review and update the status of each finding to maintain transparency and accountability throughout the process.
6. **Documentation and Evidence:** Thoroughly document the remediation process, including evidence of corrective actions taken. This documentation is not only essential for audit purposes but also serves as a valuable resource for continuous improvement.
7. Training and Awareness: Consider the findings as opportunities for learning and improvement. Provide additional training and awareness pro

**Communication Plan:**

Maintaining open and transparent communication is paramount. Establish a communication plan to keep all stakeholders informed about the progress of remediation efforts. Regular updates, status reports, and any adjustments to the remediation plan should be communicated promptly to ensure everyone is on the same page.

**Continuous Improvement:**

As we address these findings, let's view this process as an integral part of our commitment to continuous improvement. Embrace the opportunity to strengthen our security posture, aligning it not only with HITRUST and SOC requirements but also with the ever-evolving landscape of cybersecurity threats.

Through a concerted and diligent effort, we aim to not only rectify the identified issues but to emerge from this process with a more resilient and secure foundation. Our collective dedication to these remediation efforts will undoubtedly contribute to our long-term success in maintaining a robust security framework.

Tactical Plan

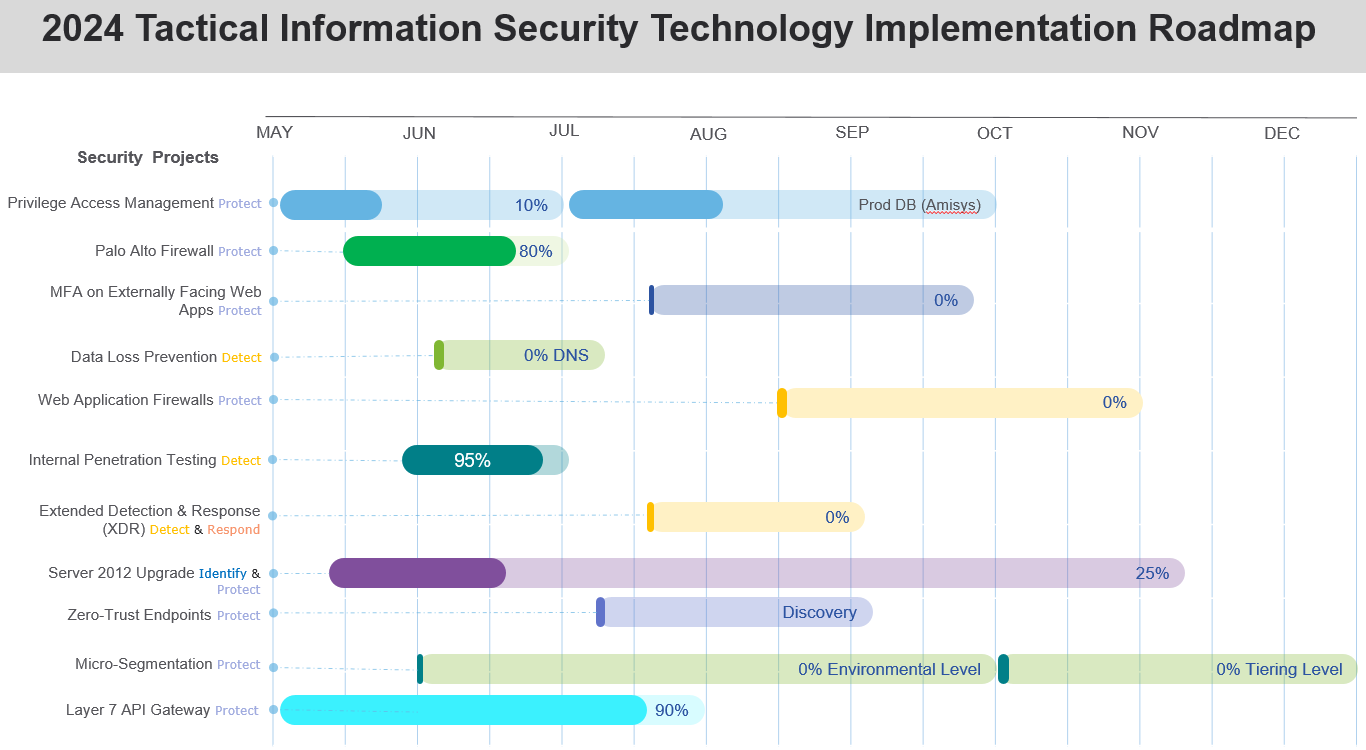


Figure 1 - 2024 Tactical Information Security Technology Implementation Roadmap

Strategic Goals for 2025/20