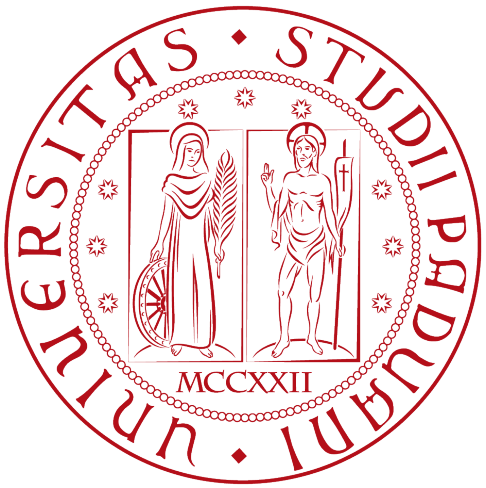

NIST CSF Assessment Report for Acme Healthcare Systems Using Generative AI

Security And Risk: Management and Certifications

Gabriel Rovesti - ID: 2103389
Prof. Simone Soderi - Prof. Antonio Belli

10/06/2024

Table of contents

1. Company Overview

In this assessment, we will give a brief description of Acme Healthcare Systems, describing its core functioning, its infrastructure and organization to have a high-level view of its functions. The company is a leading healthcare services provider serving a metropolitan area, offering a wide range of facilities and utilities through many clinics and a main hospital.

The organization has a workforce of around 500 professionals, including doctors, nurses, administrative staff, an efficient administrative personnel and a specialized IT team. The organization's operations deal daily with private patient information like medical records, insurance details, and payment data and the commitment towards keeping information confidential has to be ensured, in order to deliver high-quality patient care and being respectful to existent standards.

In this assessment, the NIST Framework will be applied, ensuring this goal will be properly respected, considering the type of data the organization deals with. All potential vulnerabilities will be analyzed, serving as guide for anomalous or harmful events of other kind.

1.1. IT infrastructure

The company's IT infrastructure is critical in supporting its operations and has to ensure sensitive handling of data present. It includes the following components:

- a centralized data center hosting the organization's Electronic Medical Records (EMR) system, billing software and critical applications for the whole system. This data center is the primary repository for storing and processing confidential patient information, records, insurance details and financial data related to them;
- each of Acme's clinics is equipped with local servers and workstations, interconnected through a private Wide Area Network (WAN) to the central data center. This allows for real-time access and updates to all operations, ensuring the information is always up-to-date, regardless of the location, making collaboration faster;
- to facilitate collaboration among staff and employees, Acme leverages a cloud-based suite and file-sharing platform, such as Microsoft 365. This enables a centralized solution, allowing for virtual meetings and document management in a simple way between departments and its staff;
- authorized personnel has remote access capabilities to the EMR system, ensuring patient records and administrative staff can perform necessary tasks from outside the organization's premises, ensuring continuity of operations and efficiency.

1.2. Company organization

To best frame the context of the organization analyzed, Acme Healthcare Systems is structured according to the following departments:

1. *Medical Department* oversees the clinics and the main hospital, where medical staff provide healthcare services to patients;
2. *Administrative Department* manages administrative tasks such as patient registration, billing, and record-keeping;
3. *Information Technology (IT) Department* ensures the functioning and maintenance of the organization's IT infrastructure, including the EMR system, servers, workstations, and network infrastructure;

4. *Human Resources (HR) Department* is in charge of recruiting, screening and finding job applicants, training the personnel in an accurate way, suitable for their role internal to the organization;
5. *Finance Department* oversees the organization's financial operations, acquring funds, redistributing them according to budgeting operations and doing accounting, while reporting for the financial year accordingly;
6. *Procurement and Supply Chain Department* is responsible for procuring equipment, medical supplies and resources able to make the internal supply chain work continuously for all operations of the organization;
7. *Quality Assurance and Compliance Department* ensures that the organization adheres to regulatory requirements, industry standards, and best practices related to patient care and data privacy.

This assessment is based on conducted on these units, better refining and giving a comprehensive analysis and overview, for all units and subunits alike. Such can be seen from the following figure:

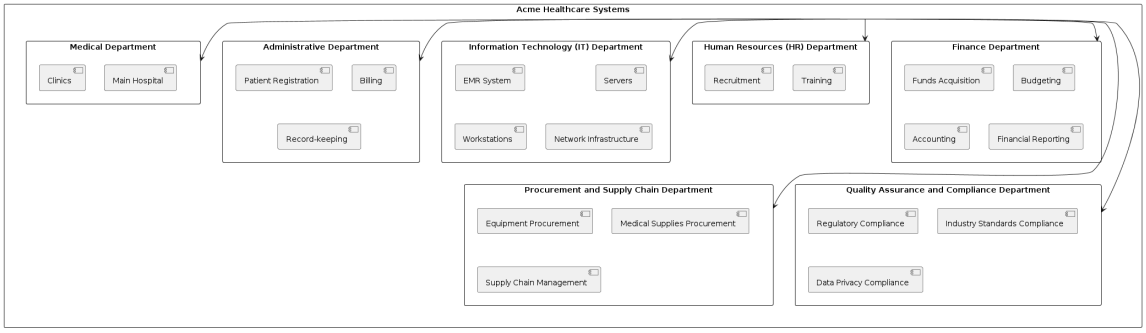

Figure 2: Company organisational chart

2. NIST CSF Risk Analysis

2.1. Methodology and Generative AI Usage

This assessment is prepared with the use of the generative AI model of Claude.ai, provided by Anthropic, in its free model Sonnet [1]. This particular model was chosen out of the others for its precision in its answers and the possibility to attach multiple files in answers. This allows for more fine-grained analysis over the controls applicable to the analyzed organization, complying with the use of NIST CSF 2.0 Framework. [2]

The NIST Cybersecurity Framework (CSF) 2.0 is a risk-based framework designed to help organizations improve their cybersecurity posture and manage cybersecurity risks and it provides a comprehensive view for mitigating risks, providing an ideal foundation for Acme's operations.

Figure 3: NIST CSF 2.0 and main functions

As evidenced by [2], it consists of several elements:

- *Core*: it provides a set of desired cybersecurity activities and outcomes, being organized into five main Functions, which will be explained in detail shortly;
- *Implementation Tiers*: these ones describe the degree to which the organization's practices exhibit the characteristics present in the Core;
- *Profiles*: they represent the alignment of the organization's requirements, objectives and resources, according to the Core and the Profiles selected.

Given this brief introduction, in the following subsections, NIST guidelines will be applied using the selected model, collecting relevant information, doing a current state analysis of the current posture and following these functions, according to [2] and Figure 3:

- *Identify*: Managing risks by identifying assets, vulnerabilities or threats inside of the organization ecosystem;
- *Protect*: Implementing safeguards to ensure confidentiality and security of data and systems;
- *Detect*: Establishing mechanisms for incidents detections;
- *Respond*: Developing and implementing plans to respond and mitigate incidents, containing them;
- *Recover*: Establishing procedures and processes to restore systems and operations to normal after a cybersec incident.

As [3] and [4] present and discuss, AI is definitely a good tool, if adequately used and prepared to do such tasks. The methodology employed in its usage for this assessment is composed as follow:

- dataset preparation and model training: list of materials regarding NIST CSF applying all the Core functions detailed in [2], describing how its patterns apply complying to NIST specifications, guidelines and case studies, understanding the core functions and implementation guidelines. With this material, the model is adequately ready to discuss and answer possible implementations on the use case found, gathering a good understanding via progressive refinement over prompts of this assessment's company relevant controls, as present in [5];

- generating the assessment report: this involves providing the model with specific prompts or inputs related to each core function, then reflecting guidelines and requirements, then addressing each single function and subcategory found individually to describe the specific application and importance of the considerations it made;

- analyzing the results: contextualizing the effects produced by the AI and the single mitigations employed, understanding if in the possible future this can be used suitably for this kind of scenarios and deternmining the potential as a tool to conduct cybersec assessments in real-world scenarios, identifying inconsistencies, inaccuriacies or misleading interpreations.

2.2. Identify

2.2.1. Asset Management (ID.AM)

As an important healthcare services provider, Acme relies heavily on its physical and software assets to ensure the delivery of high-quality patient care while safeguarding sensitive information. Inadequate management of such assets can result in unauthorized access, data breaches and disruptions, posing important risks to the patients. Controls suitable for this function are:

- *ID.AM-1*: Maintain an inventory of hardware assets, including servers, workstations, network equipment, and medical devices. This ensures visibility to the organization infrastructure.

- *ID.AM-2*: Maintain an inventory of software assets, including the EMR system, billing software, and other critical applications. This helps identifying and addressing vulnerabilities inside of software components.
- *ID.AM-5*: Prioritize assets based on their criticality, sensitivity (e.g., patient data), and impact on the organization's mission. This enables the allocation of resources and implementation of security controls based on risk prioritization.

2.2.2. Risk Assessment (ID.RA)

This function holds a big importance inside of Acme's operations framework. Given its role, the organization aces a myriad of risks, including operational, financial, and cybersecurity-related threats. Understanding these risks and their potential impact on the organization is imperative for developing effective mitigation strategies. To do so, the following controls are identified:

- *ID.RA-1*: Identify and document vulnerabilities in Acme's systems, applications, and IT infrastructure. This entails conducting regular assessments and audits to identify weaknesses that could be exploited by malicious actors.
- *ID.RA-2*: Leverage threat intelligence sources to stay informed about potential cyber threats targeting the healthcare sector. This includes monitoring industry-specific threat reports, participating in information sharing forums, and collaborating with cybersecurity organizations.
- *ID.RA-5*: Assess the likelihood and potential impact of threats exploiting vulnerabilities, considering the sensitivity of patient data and regulatory requirements. This involves conducting risk assessments to quantify the probability and severity of potential incidents.
- *ID.RA-6*: Prioritize and communicate risk responses based on the assessed risks. This includes developing mitigation strategies, allocating resources for risk treatment, and communicating risk decisions to relevant stakeholders.

2.3. Protect

2.3.1. Identity Management, Authentication, and Access Control (PR.AC)

Acme must implement robust measures to authenticate users, manage access permissions, and monitor physical access to its facilities and critical assets. Safeguards compliant to the following controls is identified:

- *PR.AC-1*: Acme Healthcare Systems is required to implement strong authentication mechanisms, such as multi-factor authentication (MFA), for all users accessing its systems and patient data. MFA adds an additional layer of security beyond traditional passwords, reducing the risk of unauthorized access.
- *PR.AC-5*: Define and regularly review access permissions based on the principles of least privilege and separation of duties. This ensures that users have only the necessary access rights to perform their job functions, reducing the risk of unauthorized access and data breaches.
- *PR.AC-6*: Manage and monitor physical access to Acme's facilities and critical assets.

2.3.2. Awareness and Training (PR.AT)

Acme must ensure that all personnel, including medical staff, administrative employees, and IT teams, are equipped with the knowledge and skills necessary to identify and mitigate cybersecurity risks effectively. Compliance to the following controls is required:

- *PR.AT-1*: Provide cybersecurity awareness and training programs for all personnel, including medical staff, administrative employees, and IT teams. This includes educating employees on common cyber threats, best practices for safeguarding sensitive information, and the importance of cybersecurity in protecting patient data and organizational assets.

- *PR.AT-2*: Offer specialized training for personnel in roles directly handling sensitive patient information or critical systems. This training should focus on the unique security challenges and compliance requirements associated with handling sensitive data.

2.3.3. Data Security (PR.DS)

Ensuring robust data security measures is imperative for Acme Healthcare Systems to safeguard the confidentiality, integrity, and availability of patient data. As a leading healthcare services provider, Acme must implement comprehensive strategies to protect patient information at rest, in transit, and during processing. The following controls are found as most suitable:

- *PR.DS-1*: Implement encryption and access control measures to protect the confidentiality, integrity, and availability of patient data at rest (e.g., in databases). Encryption ensures that sensitive information remains unreadable to unauthorized users, while access control measures restrict access to authorized personnel only.
- *PR.DS-2*: Protect the confidentiality, integrity, and availability of patient data in transit (e.g., during transmission over networks). ecure transmission protocols, such as Transport Layer Security (TLS), should be employed to encrypt data in transit and prevent unauthorized interception or tampering.
- *PR.DS-10*: Ensure the secure handling of data in use, such as within the EMR system or other applications processing patient information. This involves implementing access controls, audit trails, and data loss prevention measures to prevent unauthorized access or leakage of sensitive data.

2.3.4. Platform Security (PR.PS)

By implementing comprehensive security controls, Acme can ensure consistent configurations, timely software updates, and effective monitoring to detect and mitigate security incidents. The following controls are required:

- *PR.PS-1*: Implement configuration management practices to ensure consistent and secure configurations across Acme's systems, servers, and workstations. Consistent configurations help reduce the attack surface and minimize the risk of security vulnerabilities resulting from misconfigurations.
- *PR.PS-2*: Regularly update and patch software, operating systems, and applications to address vulnerabilities and security flaws. Timely patching is crucial for mitigating the risk of exploitation by malicious actors and preventing potential security breaches.
- *PR.PS-4*: Enable logging and continuous monitoring of systems and applications to detect potential security incidents. Logging and monitoring provide visibility into system activities and facilitate the timely detection of anomalous behavior indicative of security breaches.

2.4. Detect

2.4.1. Continuous Monitoring (DE.CM)

By monitoring personnel activity, technology usage, and computing environments, Acme can proactively identify and mitigate security threats, including insider threats and unauthorized activities. The following are identified as controls to use:

- *DE.CM-1*: Implement continuous monitoring mechanisms to detect potential security incidents or anomalies in Acme's networks, systems, and applications. Continuous monitoring provides real-time visibility into system activities and helps identify deviations from normal behavior indicative of security breaches.

- *DE.CM-3*: Monitor personnel activity and technology usage to detect potential insider threats or unauthorized activities. Monitoring user behavior helps identify abnormal patterns and unauthorized access attempts that may indicate malicious intent or security breaches.
- *DE.CM-9*: Monitor computing hardware, software, and runtime environments to detect potential adverse events. Monitoring these components helps identify hardware failures, software errors, and configuration issues that may impact system performance or security.

2.4.2. Adverse Event Analysis (DE.AE)

Thorough analysis of detected anomalies or indicators of compromise is imperative for Acme Healthcare Systems to better understand associated activities and mitigate potential security threats effectively. By estimating the impact and scope of adverse events, integrating cyber threat intelligence, and promptly declaring incidents when necessary, Acme can enhance its incident response capabilities and minimize the impact of security incidents. The following controls are required:

- *DE.AE-2*: Analyze detected anomalies or indicators of compromise to better understand associated activities. Analysis of anomalies helps identify the root cause of security incidents and develop appropriate mitigation strategies.
- *DE.AE-4*: Estimate the impact and scope of detected adverse events. Understanding the potential impact of security incidents helps allocate resources effectively and minimize disruption to business operations.
- *DE.AE-7*: Integrate cyber threat intelligence and contextual information into the analysis process. Leveraging threat intelligence sources provides valuable insights into emerging threats and adversary tactics, enabling proactive defense measures.
- *DE.AE-8*: Declare incidents when detected adverse events meet the defined incident criteria. Timely incident declaration ensures swift response and containment of security incidents, minimizing their impact on business operations.

2.5. Respond

2.5.1. Incident Management (RS.MA)

By executing the incident response plan in coordination with relevant stakeholders, categorizing and prioritizing incidents based on severity, and escalating incidents as needed, Acme can minimize the impact of security breaches and maintain trust in its services. Compliance to the following controls is required:

- *RS.MA-1*: Execute the incident response plan in coordination with relevant third parties (e.g., law enforcement, regulatory bodies) once an incident is declared. Collaboration with external stakeholders enhances incident resolution efforts and ensures compliance with legal and regulatory requirements.
- *RS.MA-3*: Categorize and prioritize incidents based on their severity and potential impact. Categorizing incidents enables efficient resource allocation and ensures that response efforts are commensurate with the level of risk posed by each incident.
- *RS.MA-4*: Escalate or elevate incidents as needed, involving appropriate personnel and stakeholders. Escalation procedures facilitate communication, decision-making, and resource mobilization during incident response efforts.

2.5.2. Incident Analysis (RS.AN)

Accurate incident analysis to understand the root causes of security incidents, preserve the integrity of incident data, and accurately assess the impact on operations. By performing detailed analysis to establish the root cause and timeline of incidents, collecting and preserving incident data and

metadata, Acme can derive valuable insights to inform response efforts and prevent future incidents. The following controls are identified:

- *RS.AN-3*: Perform analysis to establish the root cause and timeline of the incident. Identifying the root cause helps address underlying vulnerabilities and prevent recurrence, while establishing a timeline enables accurate reconstruction of events for incident response and reporting purposes.
- *RS.AN-7*: Collect and preserve the integrity and provenance of incident data and metadata. Preserving data integrity and provenance helps maintain the trustworthiness and credibility of incident findings and conclusions.
- *RS.AN-8*: Estimate and validate the magnitude of the incident's impact. Validating the impact of security incidents enables informed decision-making, resource allocation, and prioritization of response efforts to mitigate adverse consequences effectively.

2.6. Recover

2.6.1. Incident Recovery Plan Execution (RC.RP)

Executing the recovery portion of the incident response plan is crucial for Acme Healthcare Systems to restore systems and operations affected by cybersecurity incidents efficiently. By adhering to the compliance controls outlined below, Acme can minimize downtime, mitigate data loss, and restore normal operations promptly. The following controls are identified for this function:

- *RC.RP-1*: Execute the recovery portion of the incident response plan to restore systems and operations affected by the cybersecurity incident. This involves following predefined procedures and protocols to systematically recover IT assets, data, and functionalities while minimizing disruption to operations.
- *RC.RP-3*: Verify the integrity of backups and other restoration assets before using them for restoration. This involves validating the integrity, completeness, and accuracy of backups and restoration assets to prevent data corruption, loss, or compromise during the recovery process.
- *RC.RP-5*: Verify the integrity of restored assets, systems, and services, and confirm their normal operating status. This involves conducting post-recovery testing, validation, and monitoring to assess the effectiveness of the restoration efforts and identify any issues that require further attention.

2.6.2. Incident Recovery Communication (RC.CO)

In the aftermath of a cybersecurity incident, effective communication is essential to keep stakeholders informed about recovery activities and progress in restoring operational capabilities. Acme Healthcare Systems must adhere to the compliance controls outlined below to ensure transparent and timely communication with both internal and external stakeholders. Acme must be compliant to the following:

- *RC.CO-3*: Communicate recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders. This involves providing regular updates on the status of recovery efforts, including key milestones achieved, challenges encountered, and expected timelines for restoration.
- *RC.CO-4*: Share public updates on incident recovery using approved methods and messaging, as necessary. This involves providing regular updates on the status of recovery efforts, including key milestones achieved, challenges encountered, and expected timelines for restoration.

3. Conclusion and critical thoughts

The AI-generated content produced by Claude.ai's Sonnet model offers valuable insights into the NIST CSF assessment for Acme Healthcare Systems. While the analysis reveals as precise and

relevant, comprehensively this could be applied for Acme Healthcare Systems and other organizations, but some critical conclusions should be engrained.

The main strengths come from its rapid generation and the ability to provide recommendations aligned with relevant NIST CSF framework material, while at the same time giving advices on points a security engineer might possibly miss. The most relevant limitations comes from the contextual understanding, which requires many iterations but also a good if not complete understanding of the context to correctly evaluate if such functions can be applied to the use case found.

To mitigate these limitations and associated risks, organizations should implement best practices such as human oversight, continuous training, and peer review. Human experts can provide critical contextual insights and validate the AI-generated content to ensure its accuracy and relevance. While it's useful, it definitely lacks in many aspects, for example focusing on some functions instead of other ones

Ethically, organizations should carefully evaluate the potential impact on stakeholders, including patients whose data may be at risk due to inaccurate assessments. By adopting ethical guidelines and frameworks, such as those outlined by industry associations and regulatory bodies, organizations can ensure responsible use of AI in cybersecurity assessments. By integrating human expertise with AI capabilities and leveraging emerging technologies, organizations can enhance the reliability and effectiveness of cybersecurity assessments while upholding ethical standards and industry best practices, enhancing both the cybersecurity posture of an organization while retaining caution and strengths.

Bibliography

[1] Anthropic, "Claude AI," *https://claude.ai/*.

[2] NIST, "NIST CSF 2.0," *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*.

[3] R. K. Pan Dhoni, "Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity."

[4] K. A. E. P. L. P. Maanak Gupta CharanKumar Akiri, "Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity."

[5] S. Soderi, "NIST CSF Resources - Security and Risk 2023-2024," *https://stem.elearning.unipd.it/mod/folder/view.php?id=485546*.