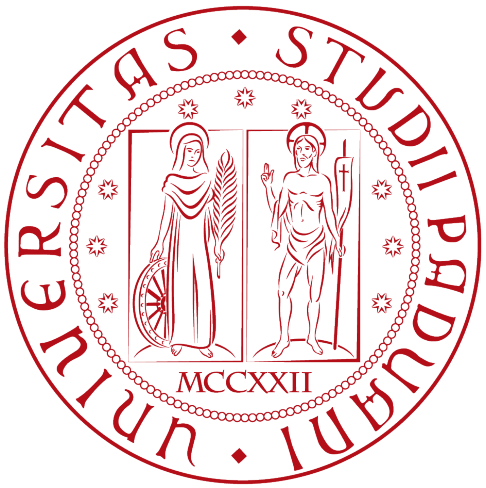

NIST CSF Assessment Report for Acme Healthcare Systems Using Generative AI

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. 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, acquiring 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:

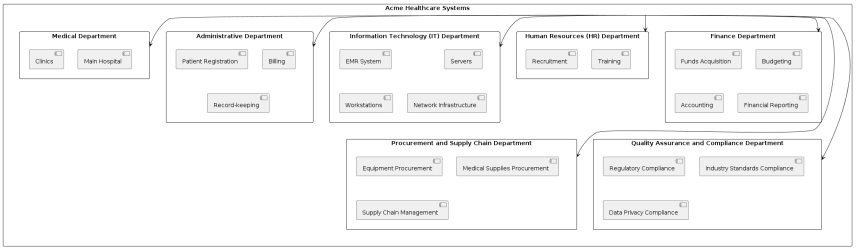

Figure 2: Company organisational chart

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* and its paid model *Opus*. This particular model was chosen out of the others for its precision in its answers and the possibility to attach up to 5 files/images for answers retaining

refined results. 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. [1]

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 [1], 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 [1] and Figure 3:

- *Govern*: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
- *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 [2] and [3] 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 follows (referring also to the laboratory done in this course as reference in [4]):

- dataset preparation and model training: list of materials regarding NIST CSF applying all the Core functions detailed in [1], describing how its patterns apply complying to NIST specifications, using its functions, categories and subcategories. With this material, the model is adequately ready to discuss and progressively refine its results over prompts of this assessment's company relevant controls, as present in [5]. To allow for a broader analysis, the subcategories used are up to 2/3, allowing to better scope the "human" analysis after each AI-driven production;

- 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 likely future this can be used suitably for this kind of scenarios and determining the potential as a tool to conduct cybersec assessments in real-world scenarios, identifying inconsistencies, inaccuracies or misleading interpretations.

2.1.1. Organizational Context and Industry Specifics

As a healthcare provider, Acme Healthcare Systems must ensure the protection of sensitive data, including patient information. In the context of the NIST CSF, this means safeguarding against threats that could compromise the confidentiality, integrity, and availability of critical data and systems. Within the healthcare industry, the organization must be prepared to respond to various threats, such as:

- Data breaches leading to privacy violations
- System outages disrupting patient care
- Cyber-attacks that could jeopardize operations

2.2. Govern

2.2.1. Organizational Context (GV.OC)

2.2.1.1. AI-Driven Risk Analysis

Acme Healthcare Systems operates in a highly regulated industry, dealing with sensitive patient information and critical healthcare services. The organization's mission is to provide high-quality patient care while ensuring the confidentiality, integrity, and availability of patient data. Key stakeholders include patients, healthcare providers, regulatory bodies, and insurers. The following controls are essential for understanding the organizational context:

- *GV.OC-01*: The organizational mission of providing high-quality patient care while safeguarding sensitive information is clearly understood and informs cybersecurity risk management decisions.
- *GV.OC-03*: Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy obligations under HIPAA and other applicable regulations, are well-understood and managed.
- *GV.OC-04*: Critical objectives, capabilities, and services that external stakeholders, such as patients and healthcare partners, depend on or expect from Acme Healthcare Systems are clearly defined and communicated

2.2.1.2. Human Risk Analysis

The AI-driven risk analysis accurately identifies the essential controls for understanding Acme Healthcare Systems' organizational context. However, additional risks and controls should be considered, particularly those related to GV.SC (Cybersecurity Supply Chain Risk Management) and GV.PO (Policy). Given the sensitive nature of patient data and strict regulations like HIPAA, any breach could result in severe consequences. Acme must prioritize data protection, ensure compliance, and maintain the availability and resilience of its systems to prevent interruptions in critical healthcare services. To strengthen its organizational context controls, Acme should develop a comprehensive cybersecurity strategy, regularly assess its legal and regulatory requirements, and foster a culture of cybersecurity awareness among all employees.

2.2.2. Roles, Responsibilities, and Authorities (GV.RR)

2.2.2.1. AI-Driven Risk Analysis

To effectively manage cybersecurity risks, Acme Healthcare Systems must establish clear roles, responsibilities, and authorities for cybersecurity risk management. This includes ensuring that the organization's leadership is accountable for cybersecurity and fosters a risk-aware culture. The following controls are essential for defining roles, responsibilities, and authorities:

- *GV.RR-01*: Organizational leadership, including the board of directors and senior executives, are responsible and accountable for cybersecurity risk and foster a culture that is risk-aware, ethical, and continuously improving.

- *GV.RR-02*: Roles, responsibilities, and authorities related to cybersecurity risk management are clearly defined, communicated, understood, and enforced across the organization.
- *GV.RR-03*: Adequate resources, including budget, personnel, and technology, are allocated commensurate with the organization's cybersecurity risk strategy, roles, responsibilities, and policies.

2.2.2.2. Human Risk Analysis

The AI-driven risk analysis correctly highlights the importance of establishing clear roles, responsibilities, and authorities for effective cybersecurity risk management at Acme Healthcare Systems. However, there are additional considerations and potential risks that should be addressed. Firstly, without clearly defined and communicated roles and responsibilities, there is a risk of accountability gaps, which can lead to critical cybersecurity tasks being overlooked or poorly executed. This can result in increased vulnerability to cyber threats and a weakened overall cybersecurity posture. Moreover, if the organization's leadership does not actively demonstrate a commitment to cybersecurity and foster a risk-aware culture, employees may not prioritize cybersecurity in their daily activities. This can lead to increased risk of human error, such as falling victim to phishing attacks or failing to follow security protocols, which can compromise sensitive patient data.

2.3. Identify

2.3.1. Asset Management (ID.AM)

2.3.1.1. AI-Driven Risk Analysis

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.
- *ID.AM-2*: Maintain an inventory of software assets, including the EMR system, billing software, and other critical applications.
- *ID.AM-5*: Prioritize assets based on their criticality, sensitivity (e.g., patient data), and impact on the organization's mission.

2.3.1.2. Human Risk Analysis

What the AI focused most upon were general classification aspects, giving an overview on some controls which can be applied in order to be consistent with the business purposed to be achieved. It's also important to actually focus on the management of data throughout the whole lifecycle and keep attention to the supplier maintenance, which is another fundamental aspect in keeping the inventory controlled and assessed. Additionally, while the AI-driven analysis mentions maintaining asset inventories, it does not stress the importance of regularly updating and patching these assets to address known vulnerabilities and should have more processes in place to ensure control over those - while at the same time, ensuring secure disposal of the present ones.

2.3.2. Risk Assessment (ID.RA)

2.3.2.1. AI-Driven Risk Analysis

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.
- *ID.RA-2*: Leverage threat intelligence sources to stay informed about potential cyber threats targeting the healthcare sector.

- *ID.RA-5*: Assess the likelihood and potential impact of threats exploiting vulnerabilities, considering the sensitivity of patient data and regulatory requirements.
- *ID.RA-6*: Prioritize and communicate risk responses based on the assessed risks.

2.3.2.2. Human Risk Analysis

Firstly, while the AI-driven analysis mentions identifying vulnerabilities and leveraging threat intelligence, it does not address the importance of internal/external threats while managing changes or trying to respond to tracked communications. Also, the processes for receiving/analyzing/responding vulnerability disclosures should be defined prior to the acquisition of the assets. Another aspect not touched by the AI is the Improvement category, which considers all of the tests/processes and activities affecting everyday operations; these observations should be key in order to create adequate prevention planning.

2.4. Protect

2.4.1. Identity Management, Authentication, and Access Control (PR.AA)

2.4.1.1. AI-Driven Risk Analysis

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.AA-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.
- *PR.AA-5*: Define and regularly review access permissions based on the principles of least privilege and separation of duties.
- *PR.AA-6*: Manage and monitor physical access to Acme's facilities and critical assets.

2.4.1.2. Human Risk Analysis

The AI overall tries to bound the credentials controls and hardware while safely authenticating users, but more fine-grained control should be employed in order to effectively authenticate the users and define precise policies of access. In particular, authentication factors should be precisely controlled and monitored, in order to define a global policy and proof-check identity access for each kind of operation. Overall, different safeguards are present to generally control the operations overall.

2.4.2. Awareness and Training (PR.AT)

2.4.2.1. AI-Driven Risk Analysis

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.
- *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.

2.4.2.2. Human Risk Analysis

In this case, the AI has applied precisely the subcategories present. In particular, the training should be complying with awareness programs, so to continually inform all personnel about existing policies and making them aware and trained according to their different level of skills and knowledge, necessary to correctly handle sensitive data.

2.5. Detect

2.5.1. Continuous Monitoring (DE.CM)

2.5.1.1. AI-Driven Risk Analysis

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.
- *DE.CM-3*: Monitor personnel activity and technology usage to detect potential insider threats or unauthorized activities.
- *DE.CM-9*: Monitor computing hardware, software, and runtime environments to detect potential adverse events.

2.5.1.2. Human Risk Analysis

Several considerations must be added on the AI analysis, for example ensuring existing systems can continuously integrated in a seamless way, for example adding some SIEM systems or some IDS detection systems, allowing to pose a baseline for the systems activities, possibly new baselines for incident management. Continuous monitoring should be also held in terms of privacy, while using some more fine-grained analysis tools in order to understand and recognize patterns/anomalies inside of breaches and other incidents,

2.5.2. 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, 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.
- *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.
- *DE.AE-8*: Declare incidents when detected adverse events meet the defined incident criteria. Timely incident declaration ensures minimizing their impact on business operations.

2.5.2.1. Human Risk Analysis

Acme should also establish, apart from the general points given here, clear incident criteria aligned with risk appetite and regulatory requirements, adding consistent timely incident declaration. Leveraging automation is also important, understanding how to streamline data collection and correlation to enable faster incident triaging and response. Collaboration with cross-functional teams is essential to gather a comprehensive understanding of impact and implications, while capturing lessons and updating response plans and control matrices.

2.6. Respond

2.6.1. Incident Management (RS.MA)

2.6.1.1. AI-Driven Risk Analysis

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.

2.6.1.2. Human Risk Analysis

The analysis effectively outlines the essential incident management controls for Acme Healthcare, including executing the response plan, categorizing incidents and escalating as needed. However, Acme should also consider the following:

1. Involve legal and regulatory teams immediately for incidents involving sensitive healthcare data to ensure compliance with HIPAA and other privacy laws.
2. Factor in reputational damage and patient trust impact when prioritizing incidents, as even minor public incidents can be costly in healthcare.
3. Ensure well-documented escalation procedures and conduct regular tabletop exercises to identify gaps and improve preparedness.
4. Perform thorough post-incident analysis to identify lessons learned and implement controls to prevent recurrence.

2.6.2. Incident Analysis (RS.AN)

2.6.2.1. AI-Driven Risk Analysis

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.
- *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.

2.6.2.2. Human Risk Analysis

The AI perspective of incident analysis controls is on the right track but lacks depth in a few key areas when compared to the NIST framework. While it touches on root cause analysis, data preservation, and impact assessment, it fails to emphasize the importance of collaboration across teams, contextual analysis specific to Acme's environment, and the need for a strong forensic readiness plan. The AI also misses the mark on highlighting continuous improvement based on lessons learned and timely reporting to stakeholders. To fully align with NIST standards, the analysis should provide a more comprehensive view of incident analysis that goes beyond just the basic controls mentioned.

2.7. Recover

2.7.1. Incident Recovery Plan Execution (RC.RP)

2.7.1.1. AI-Driven Risk Analysis

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.
- *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.
- *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.

2.7.1.2. Human Risk Analysis

The above analysis of incident recovery plan execution touches on important aspects such as following predefined procedures. However, it misses some critical elements that are essential for alignment with the NIST framework. The analysis should place more emphasis on prioritizing recovery efforts based on the criticality of affected systems and their impact on patient care and business continuity. Additionally, it fails to stress the importance of clear and timely communication with stakeholders throughout the recovery process. Furthermore, the AI should highlight the need for thorough documentation of the recovery process, including any deviations from the plan, to facilitate future improvements and audits.

3. Conclusion and critical thoughts

The AI-driven analysis highlighted most critical aspects, while aligning with the organization's mission of providing high-quality patient care. The assessment identified key areas where Acme can strengthen its controls and processes, such as risk assessment, access management, continuous monitoring, and incident response planning. However, as a healthcare provider operating in a highly regulated industry, Acme must go beyond the AI-generated recommendations and ensure full compliance with relevant regulations, such as HIPAA and HITECH. This requires a holistic approach that considers the unique challenges and requirements of the healthcare sector, including maintaining patient trust, ensuring data privacy, and minimizing disruptions to critical care services.

Moving forward, Acme should leverage the insights provided by this AI-assisted assessment as a starting point and further refine its cybersecurity strategy through collaboration with subject matter experts, stakeholders, and regulatory bodies. Continuous improvement, ongoing risk assessments, and regular employee training are essential to maintain a robust cybersecurity posture and adapt to evolving threats and industry standards. While generative AI can be a valuable tool for conducting comprehensive assessments and identifying potential areas of improvement, it should be viewed as a complementary resource rather than a complete solution. The expertise and guidance of cybersecurity professionals, combined with a deep understanding of the organization's specific context and requirements, are crucial for developing and implementing effective cybersecurity measures that meet the unique needs of the healthcare industry.

Bibliography

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

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

[3] 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."

[4] A. Belli, "M6.5 – Nist CSF Laboratory," *https://stem.elearning.unipd.it/pluginfile.php/841940/mod_resource/content/0/M6.5-%20Nist%20CSF%20Framework.pdf*.

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