

**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

<b>1. Company Overview .....</b>	<b>3</b>
<b>2. NIST CSF Risk Analysis .....</b>	<b>3</b>
2.1. Methodology and Generative AI Usage .....	3
2.2. Govern .....	5
2.2.1. Organizational Context (GV.OC) .....	5
2.2.1.1. AI-Driven Risk Analysis .....	5
2.2.1.2. Human Risk Analysis .....	5
2.2.2. Roles, Responsibilities, and Authorities (GV.RR) .....	5
2.2.2.1. AI-Driven Risk Analysis .....	5
2.2.2.2. Human Risk Analysis .....	5
2.3. Identify .....	6
2.3.1. Asset Management (ID.AM) .....	6
2.3.1.1. AI-Driven Risk Analysis .....	6
2.3.1.2. Human Risk Analysis .....	6
2.3.2. Risk Assessment (ID.RA) .....	6
2.3.2.1. AI-Driven Risk Analysis .....	6
2.3.2.2. Human Risk Analysis .....	6
2.4. Protect .....	6
2.4.1. Identity Management, Authentication, and Access Control (PR.AC) .....	6
2.4.1.1. AI-Driven Risk Analysis .....	6
2.4.1.2. Human Risk Analysis .....	6
2.4.2. Awareness and Training (PR.AT) .....	7
2.4.2.1. AI-Driven Risk Analysis .....	7
2.4.2.2. Human Risk Analysis .....	7
2.4.3. Data Security (PR.DS) .....	7
2.4.3.1. AI-Driven Risk Analysis .....	7
2.4.3.2. Human Risk Analysis .....	7
2.5. Detect .....	7
2.5.1. Continuous Monitoring (DE.CM) .....	7
2.5.1.1. AI-Driven Risk Analysis .....	7
2.5.1.2. Human Risk Analysis .....	7
2.5.2. Adverse Event Analysis (DE.AE) .....	7
2.5.2.1. Human Risk Analysis .....	8
2.6. Respond .....	8
2.6.1. Incident Management (RS.MA) .....	8
2.6.1.1. AI-Driven Risk Analysis .....	8
2.6.1.2. Human Risk Analysis .....	8
2.6.2. Incident Analysis (RS.AN) .....	8
2.6.2.1. AI-Driven Risk Analysis .....	8
2.6.2.2. Human Risk Analysis .....	8
2.7. Recover .....	8
2.7.1. Incident Recovery Plan Execution (RC.RP) .....	8
2.7.1.1. AI-Driven Risk Analysis .....	9
2.7.1.2. Human Risk Analysis .....	9
2.7.2. Incident Recovery Communication (RC.CO) .....	9
2.7.2.1. AI-Driven Risk Analysis .....	9
2.7.2.2. Human Risk Analysis .....	9
<b>Bibliography .....</b>	<b>9</b>

## 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:

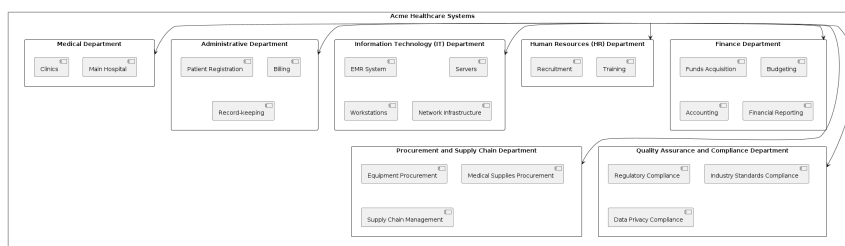


Figure 2: Company organisational chart

## 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* [1]. 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. [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 follows (referring also to the laboratory done in this course as reference in [5]):

- 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, 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 [6]. 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 possible 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.

## **2.2. 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 organiza-

tion'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**

### **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 faces 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**

## **2.4. Protect**

### **2.4.1. Identity Management, Authentication, and Access Control (PR.AC)**

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

#### **2.4.1.2. Human Risk Analysis**

## **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**

## **2.4.3. Data Security (PR.DS)**

### **2.4.3.1. AI-Driven Risk Analysis**

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).
- *PR.DS-2*: Protect the confidentiality, integrity, and availability of patient data in transit (e.g., during transmission over networks).
- *PR.DS-10*: Ensure the secure handling of data in use, such as within the EMR system or other applications processing patient information.

### **2.4.3.2. Human Risk Analysis**

## **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**

### **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**

## **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.

To reach Tier 3 (Repeatable), Acme should ensure that the incident response plan is regularly tested, reviewed, and updated based on lessons learned and changes in the threat landscape. The incident management process should be formally documented and consistently applied across the organization, with clearly defined roles and responsibilities for all involved parties.

#### **2.6.1.2. Human Risk Analysis**

### **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**

## **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

### 2.7.2. Incident Recovery Communication (RC.CO)

#### 2.7.2.1. AI-Driven Risk Analysis

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.

#### 2.7.2.2. Human Risk Analysis

## 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] 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](https://stem.elearning.unipd.it/pluginfile.php/841940/mod_resource/content/0/M6.5-%20Nist%20CSF%20Framework.pdf).
- [6] S. Soderi, “NIST CSF Resources - Security and Risk 2023-2024,” <https://stem.elearning.unipd.it/mod/folder/view.php?id=485546>.