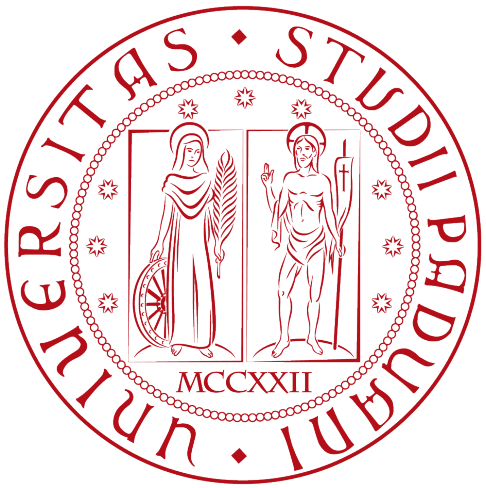

NIST CSF Assessment Report for Acme Healthcare Systems Using Generative AI

Security And Risk: Management and Certifications

Gabriel Rovesti - ID: 2103389

June 10, 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.

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 2: NIST CSF 2.0 and main functions

As evidenced by Figure 2, it consists of several elements:

- *Core*: it provides a set of desired cybersecurity activities and outcomes, being organized into five main Functions: Identify, Protect, Detect, Respond, and Recover;
- *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, objecti.ves 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]:

- *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 methdology employed in 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 implementation on the use case found, understanding how much it can suit;
- 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 aspect individually;
- 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

2.3. Protect

2.4. Detect

2.5. Respond

2.6. Recover

3. Conclusion

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."