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.

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

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

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. 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. [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.

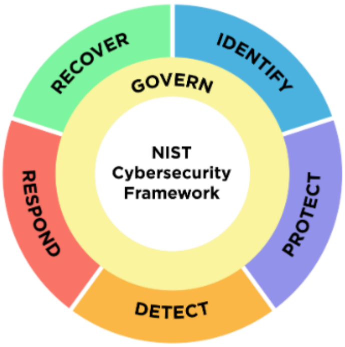

Figure 2: NIST CSF 2.0 and main functions

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, 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 steps, according to [1]:

- scope the Organizational Profile
- gather needed information
- create the Organizational Profile
- analyze gaps creating an action plan
- implementing action plan updating the Profile

3. Results

4. Conclusion

Bibliography

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