As a security analyst, I intend to comprehensively assess EPIC Systems Corporation’s security practices, evaluating them within the framework provided by the National Institute of Standards and Technology (NIST). The following points outline the objectives and scope of my analysis:

1. Name of company – EPIC Systems Corporation (EPIC)

2. Context – EPIC is a prominent provider of EHR (Electronic Health Records) systems and healthcare software solutions. Many major healthcare organizations rely on EPIC as their primary software platform for managing patient records, coordinating care, and facilitating seamless communication among healthcare professionals. EPIC’s software is widely adopted by hospitals, clinics, and healthcare organizations globally, playing a vital role in digitizing and modernizing healthcare delivery. With its widespread usage and critical position in healthcare systems, EPIC’s software handles a vast amount of sensitive patient information, including medical records, treatment plans, and personally identifiable information. The software enables healthcare providers to streamline workflows, improve patient care, and enhance operational efficiency, making it an essential component of modern healthcare systems.

3. Motivation – EPIC handles sensitive patient information, making security a paramount concern. Given the increasing digitization of healthcare and the need to protect patient privacy, EPIC must employ strategic risk and security management to safeguard patient data, ensure the confidentiality and integrity of health records, and mitigate potential vulnerabilities in its software and systems. The healthcare industry in the United States is subject to various privacy and security regulations, such as HIPPA. EPIC must comply with these regulations to avoid legal and financial consequences, protect patient rights, and maintain the integrity of the healthcare system. EPIC’s software operates in a complex and evolving technological landscape, where new threats and vulnerabilities constantly emerge, and trust between organizations and patients is necessary.

4. Framework used – NIST Framework (National Institute of Standards and Technology)

a. Key Components:

b. Identify

c. Protect

d. Detect

e. Respond

f. Recover