NIST RMF Applicability in Healthcare Sector

By: Gerald Rigdon - 2023

Assumptions:

For this analysis I assume the companies or organizations in the Healthcare Sector are not bound by the Federal Information Security Modernization Act or FISMA, meaning they do not provide any services identified by federal law for government entities.

Discussion:

The purpose of the NIST Risk Management Framework or RMF is to promote the development of security and privacy capabilities into information systems throughout the System Development Life Cycle or SDLC. Hence, although developed specifically for government entities, the SDLC is a universal process control concept applied in risk management and used in international standards, especially related to use cases in the Healthcare Sector. I believe any organization in healthcare should be open to RMF given the following recent events:

- WannaCry ransomware that affected hospital systems and devices around the world
- Vulnerabilities in URGENT/11 (TCP/IP) and SweynTooth (Bluetooth Low Energy) third-party components
- The 2020 Duesseldorf University Clinic's systems disruption that led to patient death

The seven steps (*Risk Management Framework for Information Systems and Organizations*, 2018) recommended in the RMF are as follows:

1. **Prepare**: The purpose of this step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.
2. Categorize
3. Select
4. Implement
5. Assess
6. Authorize
7. Monitor

In the previous version of RMF there were only 6 steps and then in Revision 2 a "Step 0" was added. Per (*NIST RMF: The "Prepare Step" of Implementation*, 2023) the main goals of the new **Prepare** step are:

- Facilitate better communication surrounding security and risk between leadership, business process levels and system owners.
- Identify common security controls and baselines in place at the organization.
- Identify where security resources will go according to risk appetite, prioritizing high-value assets and high-impact systems requiring increased levels of protection.

Considering the many cybersecurity challenges in the Healthcare Sector, RMF, especially with the additional focus on "Step 0", would be an effective way to bring harmonization to the Healthcare Sector and the need to do all the upfront work in thinking about security from the start. In fact, in the most recent FDA guidance on medical device cybersecurity (*Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, 2023), the NIST Cybersecurity Framework or CSF is already recognized as something that can be employed to fulfill the FDA requirements for a Secure Product Development Framework or SPDF. Furthermore, the RMF addresses the CIA confidentiality, integrity, and availability triad which are sound governing general-purpose principles applicable to healthcare.

Although the ISO standards have long been used for risk management in healthcare, many of them are historically heavily focused on safety. For example, in the medical device arena, ISO 14971 was eventually complemented by TIR57 which was security focused. Given the NIST RMF was created to address information systems, the primary focus has always been on security. Since much of healthcare is driven by the management of data, NIST RMF can most certainly be a practical framework for multiple industries, including the Healthcare Sector.

References:

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. (2023, September). fda.gov. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurityLinks to an external site.

NIST RMF: The "Prepare Step" of Implementation. (2023, April). intraprisehealth.com. https://intraprisehealth.com/implementing-the-nist-rmf-step-zero/Links to an external site.

Risk Management Framework for Information Systems and Organizations. (2018, December). NIST Special Publication 800-37 Revision 2. nvlpubs.nist.gov. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdfLinks to an external site.