RA Framework Comparisons

Megan Leonard

ISEC 475

6/4/2023

When it comes to security there are always going to be risks that you need to consider moving forward. The best way is to create a risk assessment as you need to understand just how important a risk is and the impact it will have on your company. To make this process easier, there have been many risk assessment frameworks that were made available for companies to use.

The first framework we can look at is SERA or Security Engineering Risk Analysis. SERA looks at the software systems and creates a model approach to understanding the risks while most other frameworks focus on the brainstorming side. As systems are growing and their connections widening, SERA looks at the larger scale and the risk that is found in these multi-layered systems. SERA looks more for gaps within the systems and works on trying to fix them than the individual risks. Their main focus is where the system needs fixed than what could happen during those attacks. We look at this as a castle that is working on upping its security. The castle sees that people could just scale the side of the building to get in. Instead of worrying about the damage they could cause, the castle focuses on fixing its security by building a moat.

FAIR or Factor Analysis of Information Risk is another framework that looks at risks using a model. This framework looks more at the risk impact to IT and works on understanding the frequency and magnitude of possible data loss. While SERA focuses on the software systems, FAIR looks at the risks themselves and works on understanding just how the risk will affect them. To use the castle once more, the framework as the castle will look at the possibility of people climbing the walls. They will take this risk into account and look into how it could affect the castle should they breach the wall and how often this could happen.

NIST Risk Assessment Framework is another that has its own focus, this being in the system development life cycle. NIST has a seven-category approach when it comes to risks which is to start with preparing the organization for the risk management. Next is to categorize the system and information for an impact analysis. Then they select the NIST controls to use to protect the system. After they implement the controls then assess the impact of those controls and their results. Then the system is authorized and constantly monitored. To use the castle analogy, NIST would take place while they are working on building the castle. They focus on laying out the bricks and making sure they follow the rules that are set in place for building and look at the best way to protect the castle while they are working. This could be building a moat to add that layer of separation or adding controls to the castle door so it cannot open from the outside. NIST has its own views and looks more at the laws and policies they need to follow. This is understandable as NIST as a group has made their own policies and standards to follow.

The three frameworks are each a risk assessment framework, but they are only alike in name. Frameworks are never going to be the exact same and their focus will lie on what the creator deems important at that time. This is why when deciding to implement a framework for an organization, it is best to look over the different ones that are available as one may fit your needs better than the other.

Citations:

*(FAIR) factor analysis of information risk management*. RSI Security. (2022, August 2). <https://www.rsisecurity.com/fair-risk-assessment/>

Computer Security Division, I. T. L. (n.d.). *About the RMF - NIST risk management framework: CSRC*. CSRC. <https://csrc.nist.gov/projects/risk-management/about-rmf>

Mead, N. R., & Woody, C. C. (2017). *Cyber Security Engineering: A practical approach for systems and software assurance*. Addison-Wesley.

Pros and cons of the Fair Framework — riskoptics - reciprocity. (n.d.-a). <https://reciprocity.com/pros-and-cons-of-the-fair-framework/>

Security Engineering Risk Analysis (SERA) - Carnegie Mellon University. (n.d.-b). <https://resources.sei.cmu.edu/asset_files/Brochure/2015_015_001_447211.pdf>

Security Engineering Risk Analysis (SERA) threat archetypes - DTIC. (n.d.-c). <https://apps.dtic.mil/sti/pdfs/AD1116716.pdf>

Zola, A. (2022, February 28). *What is a risk assessment framework, and how does it work?*. CIO. <https://www.techtarget.com/searchcio/definition/risk-assessment-framework-RAF>