Risk Management: What is it, Why is it Important, and How to do it?

Richard Parker

ABSTRACT

Risk Management is the process whereby an organization identifies the risk, makes an assessment of the risk, identifies any mitigation that can be done to control the risk, and then decides to accept the risk or not to accept the risk. It applies to everything we do such as our personal lives, financial institutions, organizational operations, and information security. It is important in order to ensure the protection of the organization, it's assets, and more specifically the organization's Information Technology environment. There are a few variations of the risk management process which have been developed by both commercial and government organizations. All these processes may differ in implementation and labeling but have the same essential core steps. Those steps include identification of the risk, analysis and evaluation of the risk, mitigation of the risk, acceptance of the risk that can't be mitigated, and monitoring. When done properly, risk management can greatly reduce the amount of risk taken on by an organization and the effects of the risk.

Risk Management: What is it, Why is it Important, and How to do it?

Over the years, several processes have been developed by both government and commercial entities to handle the task of Risk Management and Assessment and Accreditation of new software being put on the network. The goal of such endeavors is to standardize the process and requirements so that everyone in the Cyber Security field will be able to use similar processes, documents, and steps to document, assess, and approve software. The common term for these sets of processes is Risk Management Framework (RMF). It is also important to note that there is more than one model for RMF. Popular RMF models include but are not limited to: NIST (National Institute of Standards and Technology) RMF, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), TARA (Threat Agent Risk Assessment), and FAIR (Factor Analysis of Information Risk) (Joshi & Singh, 2017). The various RMF models are either quantitative or qualitative (Dobrynin, Radivilova, Maltseva, & Ageyev, 2019). Choosing the appropriate scanner to use in the RMF process being used is also an important aspect of RMF.

Before diving into the various models and what they are it is important to cover some basic information that, will apply to all or most of the models such as what is the RMF? RMF as defined by NIST is "a disciplined and structured process that integrates information security and risk management activities into the system development life cycle" (Glossary of Terms). The goal of any RMF model/process should be to improve security, make the processes stronger, and encourage reciprocity (What is RMF, n.d.).

Of all the Risk Management models to choose from, most of them can be broken down into two types: qualitative method or quantitative method (Dobrynin et al, 2019). Qualitative methods attempt to assess risk on some sort of scale such has critical, high, medium, or low

(Dobrynin et al, 2019). Quantitative methods attempt to assess risk on some sort of numerical scale such annual losses or amount of gains by doing the process (Dobrynin et al, 2019). Quantitative methods are used when the threats and risks can be compared to values such as money and percentages (Dobrynin et al, 2019). Due to the complex and sometimes hard to calculate values, some use a qualitative approach in which risks are expressed on a numerical scale or descriptive scale (Dobrynin et al, 2019). The major drawback to a qualitative method is that the conclusion is subjective and does not provide the complete damage picture (Dobrynin et al, 2019). Which one you use will depend on the model you use as well as how easy it is to define risk and rewards.

Another important part of any RMF model is vulnerability scanning (Joshi & Singh, 2017). Which scanner to use is about as hard to answer as which RMF model to choose. There are many scanners on the market. Network vulnerability scanners include Nessus by Tenable, Retina by eEye, Fusion VM by Critical Watch, and Core Impact by Core Security (Holm, 2012). Web vulnerability scanners include: IBM Security AppScan, HP webInspect, and Acunetix web vulnerability scanner (Alsaleh et al, 2017). Which one to choose depends on your situation.

The first RMF model to be discussed is the NIST RMF model. There are seven steps involved in the NIST process: “Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor” (“Risk Management”, 2018). The first step in the process is Prepare. This step is new with revision 2 of NIST SP 800-37. While this is the first step, it is also included at the beginning of each of the other steps (“Risk Management”, 2018). In this step, the organization carries out the needed steps to prepare the organization to manage security and privacy risks using RMF (“Risk Management”, 2018). Individuals are identified and roles are assigned (“Risk Management”, 2018). A strategy is determined which includes risk tolerance for the organization. Organization tailored control baselines are established (“Risk Management”, 2018). Controls are identified as applicable or non-applicable (“Risk Management”, 2018). A continuous monitoring strategy is established (“Risk Management”, 2018).

The second step in the process is to Categorize. In this step, the impacts to organization operations and assets is determined (“Risk Management”, 2018). The categorization is based on loss of confidentiality, integrity, and availability of systems and the data stored or transmitted by those systems (“Risk Management”, 2018). Tasks include describing the system, coming up with the security categorization, and doing the security categorization review and approval (“Risk Management”, 2018).

The third step in the NIST process is to Select. In this step the controls needed to ensure confidentiality, integrity, and availability of the organizations systems and data in relation to the risk to those systems and data are selected, tailored, and documented (“Risk Management”, 2018). Tasks in the step include: “control selection, control tailoring, control allocation, documentation of planned control implementations, continuous monitoring strategy for the system, and plan review and approval” (“Risk Management”, 2018).

The fourth step in the NIST process is to Implement. In this step, the controls in the security and privacy plans for the system are implemented as well as documented in the baseline configuration (“Risk Management”, 2018). There are only two tasks in this step: “Control implementation and update control implementation information” (“Risk Management”, 2018).

The fifth step in the NIST process is Assess. In this step, the system is evaluated to determine if the controls that were selected were implemented correctly, that the system and controls operate normally, and are meeting the security and privacy requirements for both the system and the organization ("Risk Management", 2018). In this step, tasks include selecting an assessor to assess the controls and system, coming up with and documenting the assessment plan, conducting control assessments, producing assessment reports, performing remediation actions, and developing a Plan of Action and Milestones (POAM) for the items that cannot be remediated at the time of the assessment ("Risk Management", 2018).

The sixth step in the NIST process is to Authorize. In this step, organizational accountability is established by having a senior management official determine if the security and privacy risk to the organization operations and assets, individuals, and other entities is acceptable in relation to system operation or use of the controls ("Risk Management", 2018). Tasks include developing an authorization package, performing a risk analysis and determination, providing risk responses to the risks identified, performing the authorization decision, and reporting the authorization decisions, critical vulnerabilities, and risks ("Risk Management", 2018).

The seventh and final step in the NIST process is to Monitor. In this step, sometimes referred to as continuous monitoring, the system is monitored to ensure it maintains the security and privacy posture that was approved ("Risk Management", 2018). Tasks in this step include: monitoring the system and environment changes, performing ongoing assessments, performing risk response, updating authorization packages, reporting security and privacy changes, performing continuous authorization based on changes to the system, and developing a system disposal plan if needed ("Risk Management", 2018). A good example of this step is a system running on the Windows 2016 server platform being approved. At the start it is a good system, but a month later a vulnerability in Windows 2016 is discovered by Microsoft. A company such a Tenable writes a plugin to detect if a system has that patch and releases it to the organization.

The organization then scans the system they approved the previous month and it is determined that it needs the patch published by Microsoft. The organization applies that patch and re-evaluates the system. The remediation is documented in the authorization package update and the senior management official re-approves the system. But what if a patch or fix is not available? The organization must decide whether to accept the new risk or not to accept the new risk.

Several of the steps mentioned involve access controls. What are access controls? Where do access controls come from? The Access Controls come from NIST Special Publication 800-53 Revision 4. The controls listed in NIST SP 800-53 deal with security and privacy. The list of controls used can be tailored to meet the needs of the organization ("Security and Privacy", 2013). For example, if the system does not deal with Privacy Act information, some or all privacy controls can be tailored out of the list. In order to select the appropriate controls, an organization must determine the type of information they have and the sensitivity of the information ("Security and Privacy", 2013). If using an automated system, such as XACTA, for completing the project, overlays can be created and tailored from these control sets.

Reciprocity is a key component in any RMF process. It is also the biggest problem area. Reciprocity, or as NIST SP 800-37 revision 2 calls it, reciprocal acceptance is accepting the assessment results and authorization decisions from other agencies and organizations ("Risk Management", 2018). It is NIST's hope that as both public and private sectors adopt a standard framework, that sharing and acceptance of others work will become more common, thereby reducing the need for each entity to expend man hours accrediting the same system or software

(“Risk Management”, 2018). Reciprocity in its purest form means trusting the work others have done to accredit software or a system.

Up to now, a lot has been dedicated to the NIST RMF model. It is important to know this is not the only RMF model that an organization can use. The NIST RMF model is not for every organization. There are several other risk assessment models to choose from. Some are qualitative and some are quantitative with the goal of eliminating risk (Joshi & Singh, 2017). OCTAVE is a model developed by CERT (Joshi & Singh, 2017). Unlike most of other models, which simply focus on the software threat, it defines assets as people, hardware, software, information, and systems (Joshi & Singh, 2017). OCTAVE provides the framework for assessment and planning, however it complex and does not allow the ability to quantitatively model risk (Joshi & Singh, 2017). OCTAVE was derived from three primary sources: Information Security Evaluation (ISE), software risk management expertise, and surveying current practices being done in information security risk management (Alberts, Behrens, Pethia, & Wilson, 1999).

OCTAVE provides the methodology to look at both organizational and technology issues and put together the security needs for the organization (Alberts et al, 1999). It has 3 phases: “build enterprise-wide security requirements, identify infrastructure vulnerabilities, and determine security risk management strategy” (Alberts et al, 1999). Unlike the NIST RMF process which evaluates a specific thing and what its impact on the enterprise will be, OCTAVE takes a higher-level approach and looks at the overall infrastructure and evaluates both good and bad practices throughout the enterprise (Alberts et al, 1999). Another key difference is that NIST RMF focuses on the impact of new software and systems, whereas OCTAVE seems to focus on the existing architecture in the enterprise (Alberts et al, 1999).

Another RMF model that can be used is TARA (Joshi & Singh, 2017). TARA is a risk assessment framework model developed by Intel (Joshi & Singh, 2017). TARA assists organizations with managing risk by breaking down the information related to security attacks (Joshi & Singh, 2017). The thought process behind this model is that it would be too expensive to fix all vulnerabilities, therefore an organization should focus on only attacks and vulnerabilities that are likely to occur (Rosenquist & Casey, 2009).

TARA consists of three references: "Threat Agent Library (TAL), Common Exposure Library (CEL), and Methods and Objectives Library (MOL)" (Rosenquist & Casey, 2009). The TAL contains a list of threat agents as was already in use at Intel, therefore it seemed to be a good fit into the TARA model (Rosenquist & Casey, 2009). The CEL contains known vulnerabilities and exposures (Rosenquist & Casey, 2009). The MOL contains the known objectives of threat agents as well as the methods most likely to be used by those threat agents (Rosenquist & Casey, 2009). There are six steps in the TARA model: Measure current threat agent risks to Intel, Distinguish threat agents that exceed baseline acceptable risks, Derive primary objectives of those threat agents, Identify methods likely to manifest, Determine the most important collective exposures, and Align strategy to target the most significant exposures (Rosenquist & Casey, 2009). TARA was adopted by the United States Department of Homeland Security in 2007 (Rosenquist & Casey, 2009).

Yet another approach is FAIR (Joshi & Singh, 2017). FAIR "provides the framework for understanding, analyzing, and measuring information risk" (Joshi & Singh, 2017). Unlike some of the other RMF models, FAIR is quantitative, not qualitative (Institute, F. A. I. R.). It was developed in a way that provides a common language that everyone can understand, use a portfolio view of organization risk, allow challenges and defenses to risk decisions, and develop and understanding of how time and money will impact security (Institute, F. A. I. R.). FAIR provides scales in which to measure risk factors (Institute, F. A. I. R.). It also allows for analysis of complex situations through its models (Institute, F. A. I. R.). Of note is that The Open Group chose FAIR as the RMF model to use for the international standard (Institute, F. A. I. R.).

While these models are four of the most mentioned models, some organizations, such as MITRE develop their own model. MITRE uses Threat Assessment and Remediation Analysis, also called TARA. It is used to “identify and assess cyber vulnerabilities and select countermeasures effective at mitigating those vulnerabilities” (Wynn, 2015). It relies on the use of “a catalog of attack vector and countermeasure data” (Wynn, 2015). It incorporates web-based tools to search the catalog (Wynn, 2015). From the Catalog, a vulnerability matrix is created (Wynn, 2015). The vulnerability list is then combined with a mitigation map to create a list of countermeasures (Wynn, 2015). It is then ranked based on cost, thus creating a mapping table (Wynn, 2015). A countermeasure is then selected based on cost and risk tolerance (Wynn, 2015).

No matter which RMF model is used, a major problem with any of them is lack of knowledge about the risks and the processes as well as a lack of sharing within the community of Cyber Security professionals. This problem seems to compounded by the fact that many smaller companies that might not have Cyber Security or Information Technology staff might not have the knowledge and skills to perform good risk management (Alhawari, Karadsheh, & Nehari, 2012). Research has shown that RMF models don’t make good use of Knowledge Management (KM) practices (Alhawari et al, 2012). The KM framework operates under the premise that knowledge is created, transferred, and reused whenever an individual performs any kind of task (Alhawari et al, 2012). KM principles can and should be used to share information regarding an

RMF project between employees and senior leadership (Alhawari et al, 2012). Three KM principles related to RMF can be used to help generate risk knowledge (Alhawari et al, 2012). These principle lead into five steps. The three principle in play are: “business focus, accountability, and operational support” (Alhawari et al, 2012). The five steps that they spawn are: “start with key business risks, prioritize the business risks based on their importance to the business strategy, identify information sources for the high business risk areas, identify at risk information sources through establishing what information is critical to the business process, and establish risk mitigation strategies” (Alhawari et al, 2012). This combination of KM and RM yields a methodology called KBRM (Knowledge-Based Risk Management) (Alhawari et al, 2012). With this KBRM methodology at all steps in risk management, information is captured, reused, and even created and added to the knowledge base (Alhawari et al, 2012). Additionally, not only is good KM practices important within an organization, it is important among the community of cyber security professionals. If RMF and KM are combined properly, and trust is established, then reciprocity, mentioned earlier, can be established.

So why is it important to have a good RMF process for software and system accreditation? Many outside vendors adopt processes to be used during development that introduce or don’t catch all vulnerabilities and risk. For example, some software companies use Distributed Agile Development to get quality, speed, and cost benefits to complete a project. However, this induces risks and vulnerabilities that could be detrimental to an organizations network if not caught during assessment, accreditation, and authorization process (Shrivastava & Rathod, 2017). Another reason is that increasingly, more and more software is being created by reusing existing code either from previous projects owned by the software company or from open source software which may contain vulnerabilities (Kulkarni & Varma, 2017).

Which RMF model is right for an organization? That depends on several factors. One factor to consider is if this is a closed or open network (Joshi & Singh, 2017). Due the network being open at universities, OCTAVE seemed to be a good fit (Joshi & Singh, 2017). Additionally, the RMF model an organization uses might be mandated by policy. For example, government agencies and contractors may be required to use the NIST RMF model. There is no one thing to help an organization choose the model that is right for them (Joshi & Singh, 2017).

In conclusion, the common RMF models in use are: NIST RMF, OCTAVE, TARA, and FAIR. RMF models and processes are needed to ensure our networks stay secure and to reduce the risk and vulnerabilities being introduced into our networks. RMF models can be quantitative or qualitative in nature. There is no easy button guide to help organizations choose which model is best for their organization, however some good guidelines to follow is to know whether you have an open or closed network. Another good indicator is to know how well variables and impacts can be articulated. Lastly, the RMF model an organization uses might be mandated by policy. Just as important to choosing the right RMF process is the choosing the right vulnerability scanner. Effective KM practices can help with sharing information across and organization as well as sharing information with other organizations (reciprocity).

References

Glossary of Terms. (n.d.). Retrieved from https://csrc.nist.gov/glossary/term/risk-management-framework.

What is RMF? (n.d.). Retrieved from https://rmf.org/what-is-rmf/.

Dobrynin, I., Radivilova, T., Maltseva, N., & Ageyev, D. (2019). Use of approaches to the methodology of factor analysis of information risks for the quantitative assessment of information risks based on the formation of cause-and-effect links. doi:10.1109/INFOCOMMST.2018.8632022

*Holm, H., Industriella informations- och styrsystem, Skolan för elektro- och systemteknik (EES), & KTH. (2012). Performance of automated network vulnerability scanning at remediating security issues. *Computers & Security, 31*(2), 164-175. doi:10.1016/j.cose.2011.12.014

*Alsaleh, M., Alomar, N., Alshreef, M., Alarifi, A., & Al-Salman, A. (2017). Performance-based comparative assessment of open source web vulnerability scanners. *Security and Communication Networks, 2017*, 1-14. doi:10.1155/2017/6158107

Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy (2018). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Security and Privacy Controls for Federal Information Systems and Organizations (2013). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

*Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, *35*, 128–137. doi: 10.1016/j.jisa.2017.06.006

Alberts, Christopher., Behrens, Sandra., Pethia, Richard., & Wilson, William. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0* (CMU/SEI-99-TR-017). Retrieved November 09, 2019, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=13473

Rosenquist, Matt & Casey, Timothy. (2009). Prioritizing Information Security Risks with Threat Agent Risk Assessment (TARA). Retrieved November 09, 2019, from https://www.researchgate.net/profile/Matthew_Rosenquist/project/Threat-Agent-Risk-Assessment-TARA/attachment/5b63874644cde265cb6538675/AS:655309425094656@1533249350237/download/Prioritizing+Informatoin+Security+Risks+with+Threat+Agent+Risk+Assessment+-+M.Rosenquist+2009.pdf?context=ProjectUpdatesLog

Institute, F. A. I. R. (n.d.). The Importance and Effectiveness of Quantifying Cyber Risk. Retrieved from https://www.fairinstitute.org/what-is-fair.

Wynn, J. E. (2015, July 27). Threat Assessment and Remediation Analysis (TARA). Retrieved from https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara.

*Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management, 32*(1), 50-65. doi:10.1016/j.ijinfomgt.2011.07.002

*Shrivastava, S. V., & Rathod, U. (2017). A risk management framework for distributed agile projects. *Information and Software Technology, 85*, 1-15. doi:10.1016/j.infsof.2016.12.005

*Kulkarni, N., & Varma, V. (2017). Perils of opportunistically reusing software module. *Software: Practice and Experience, 47*(7), 971-984. doi:10.1002/spe.2439