**Weekly Assignment 15**

Download the actual RMF documentation from NIST here:

<https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>

It should be a link like this: [SP 800-37 Rev. 2 (DOI)](https://doi.org/10.6028/NIST.SP.800-37r2)

Answer the following questions:

1. Review the Executive Summary. What was the purpose behind creating the RMF and requiring its use in the government sector?

The purpose of the Risk Management Framework (RMF) is to provide a structured process that integrates information security and risk management activities into the system development life cycle. The RMF was created to improve information security, enhance risk management, and ensure that the federal information systems are secure and resilient. It was required in the government sector to standardize the approach to risk management and ensure that all federal agencies follow a consistent process to manage and mitigate risks effectively.

1. Review the authorization package section starting on page 69. What is the purpose of an authorization package submission?

The purpose of an authorization package submission is to provide the authorizing official with the necessary information to make a risk-based decision on whether to authorize the operation of an information system. The authorization package includes documents such as the System Security Plan (SSP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M). These documents collectively demonstrate that the system has been properly assessed and that appropriate security controls are in place to mitigate risks to an acceptable level.

1. Review the section 3.7 Monitor on page 76. What would happen if this section was omitted from the document? Would this be a good or bad thing?

If the section 3.7 "Monitor" was omitted from the document, it would significantly impact the continuous monitoring and ongoing assessment of the information system's security posture. The monitoring section ensures that security controls are continuously monitored, assessed, and updated as necessary to respond to new threats and vulnerabilities. Omitting this section would be a bad thing because it would undermine the dynamic nature of risk management and leave the system vulnerable to emerging risks and changes in the threat landscape, potentially compromising the system's security and effectiveness.