Using RMF to Improve Audit Results

Revolutionizing supply chain management and health financing through a decentralized database and peer-to-peer networks

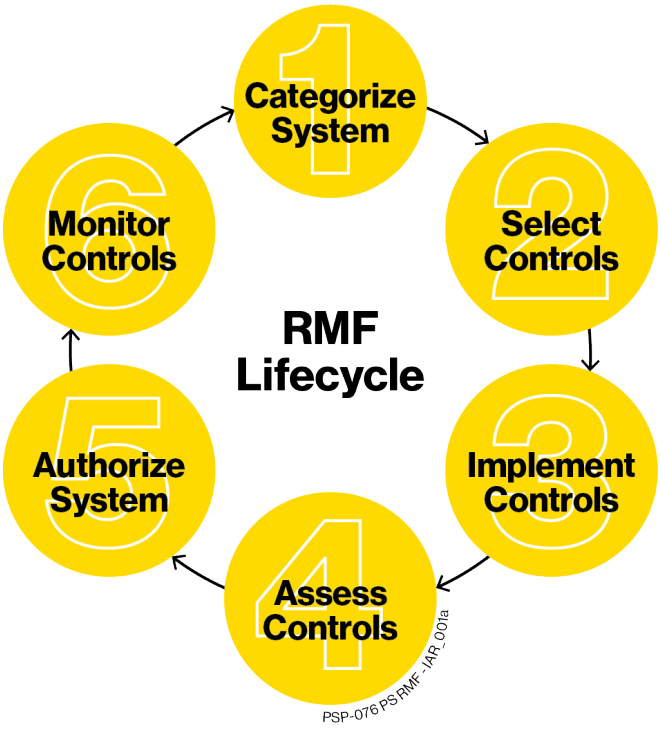
Background

Since the implementation of the Chief Financial Officers Act, auditors continue to report a significant number of IT related findings. Often times the number and the significance of these IT related finds are aggregated into significant deficiencies or material weaknesses in a financial statement audit or in other audit reports which address operations and compliance. The Risk Management Framework (RMF) can be used as a tool to enforce compliance with IT related policies and procedures - and effectively reduce the volume and significance of IT related findings.

What is RMF?

The RMF is a six-step methodology prescribed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 to authorize information systems for operation in the DoD IT environment. The RMF six step lifecycle is illustrated in the figure below.

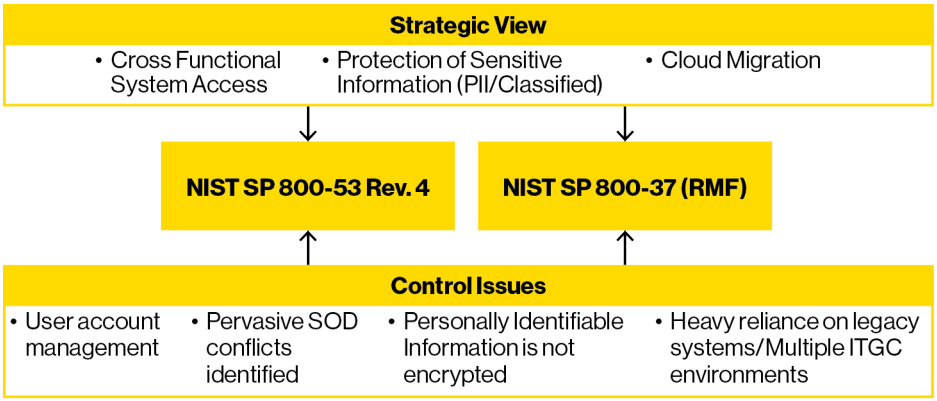
Figure 1: RMF Six Step Lifecycle



Why does my organization need to implement the RMF?

As more and more systems are integrated to support mission, finance and compliance areas, it will become more important than ever to effectively harden the IT environment to ensure compliance with IT policies and procedures and to help mitigate cybersecurity risks. Migration toward cloud environments have also increased the need to ensure that the entire IT environment has been designed and built using a standardized framework which addresses the integration required to operate in today's world.

Figure 2: Common Guidance for Cybersecurity and Financial Management



PSP-076 PS RMF - IAR_002B

So RMF is more than just a financial statement audit issue?

By utilizing RMF and the NIST guidance, systems may be designed, built and monitored in a structured way across the entire organization. Beyond the preparation of th!,! financial statements or other key financial reports, systems used to support mission delivery or used to demonstrate compliance with non-financial laws and regulations can benefit from the use of RMF. With the issuance of GAO's Green Book, and the evolving gllidance being issued by 0MB for agencies to implement enterprise wide controls, we believe that agencies would benefit from implementing RMF throughout the organization. Once implemented, RMF can be used to help:

- Document comprehensive risk acceptance processes;
- Document internal controls; and,
- Test the design and operating effectiveness of controls using appropriate assessment procedures.

How can Guidehouse help?

Guidehouse has supported organizations to develop a RMF Overlay that requires all NIST controls tested by the auditors for audit-relevant systems. Guidehouse works with Chief Information Officers (CIOs) to develop and communicate an enhanced risk acceptance process to incorporate reviews from the business and data owners. Our teams work with the systems in the field to implement the above steps to avoid or remediate audit issues. We provide feedback on implementation challenges to the CIO to improve the process or focus training efforts. This produces a sustainable plan for audit improvement using the RMF process enforced by the CIO.

For more information, please contact:

Craig Atkinson
Managing Director
(540) 454-8760
catkinson@guidehouse.com

Bradley Keith
Director
(804) 304-7005
bkeith@guidehouse.com

David Koondel
Director
(703) 918-1499
dkoondel@guidehouse.com

Follow us on Twitter
@guidehouse_us