Using RMF to Improve Audit Results

Fortifying cybersecurity & financial management audit priorities.

BACKGROUND

The Department of Defense (DoD) has been under some level of financial statement audit for the last several years. The majority of information technology (IT) Notification of Findings and Recommendations (NFRs) are coming from areas that could have been detected and corrected during the Risk Management Framework (RMF) process. As a result, auditors are finding significant control deficiencies and material weaknesses for systems authorized under RMF. With the scope of the audit expanded to full financial statements, additional IT systems will be audited leading to more findings. **RMF can be used as a tool to enforce compliance with audit requirements and decrease the volume of IT NFRs.**

WHAT IS RMF?

The RMF is a six-step methodology prescribed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 that replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) to authorize information systems for operation in the DoD IT environment. The change was made to improve information security, strengthen risk management processes, and encourage reciprocity among organizations. organizations. The RMF six step lifecycle is illustrated in the figure below.

RMF LIFECYCLE

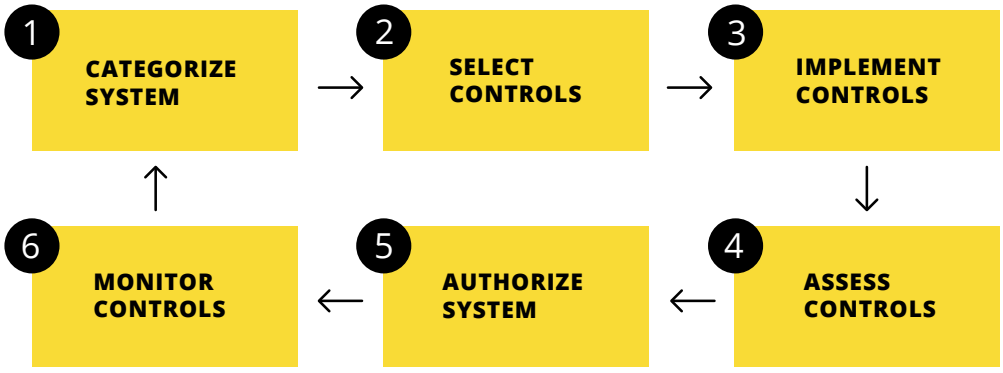

Fig. 1: RMF Six Step Lifecycle

WHY DOES MY ORGANIZATION NEED TO IMPLEMENT THE RMF?

In support of the DoD Fiscal Year 2014 Information Resources Management Strategic Management Plan, the Department of Defense Chief Information Officer (DoD CIO) updated DoD Instruction 8510.01, "RMF for DoD Information Technology," to facilitate meeting the Financial Improvement and Audit Readiness (FIAR) requirements for relevant systems.

Guidehouse

Implementing RMF also aligns the cybersecurity initiatives of the DoD CIO with financial management initiatives. The figure below demonstrates how the RMF-related NIST and DoD guidance is relevant to both cybersecurity and financial management audit priorities.

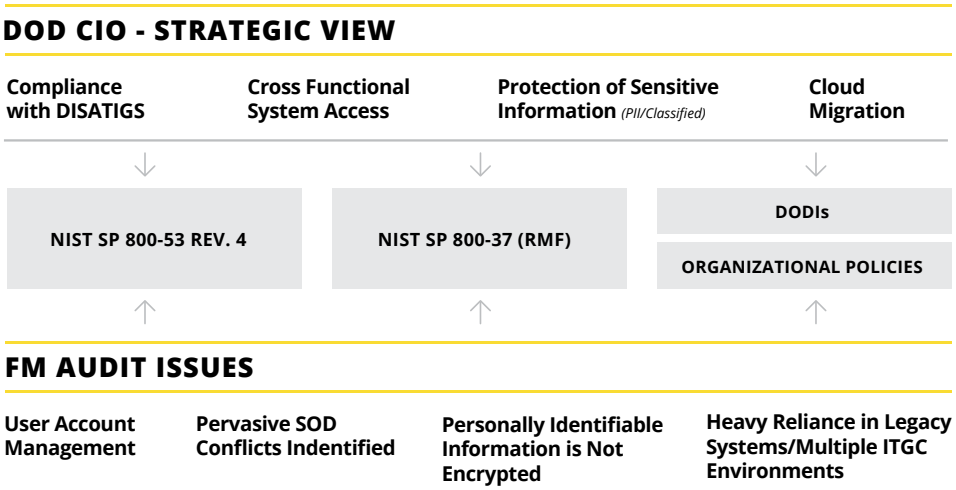

Fig. 2: Common Guidance for Cybersecurity and Financial Management

HOW CAN RMF HELP ME WITH THE FINANCIAL STATEMENT AUDIT?

By utilizing RMF and NIST controls, system owners are now required to implement controls using the same criteria financial auditors use for NFRs. Additionally, these controls have a stronger relationship to the Federal Information System Controls Audit Manual (FISCAM) methodology auditors follow to perform their testing. Organizations can utilize the RMF methodology to develop one process to address both compliance requirements. By adding the following necessary actions for all audit-relevant systems, organizations can close the gap even more between RMF and audit standards:

- Document internal controls,
- Test the design and operating effectiveness of controls using appropriate assessment procedures, and
- Utilize comprehensive risk acceptance process including approval by the business/data owner.

HOW CAN GUIDEHOUSE PUBLIC SECTOR HELP?

Guidehouse Public Sector has supported organizations within the DoD to develop a RMF Overlay that requires all NIST controls tested by the auditors for audit-relevant systems. Guidehouse Public Sector 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:

Tom Rhoads
Managing Director
(703) 918-1002
trhoads@guidehouse.com

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

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

Guidehouse

Follow us on Twitter @guidehouse_us