KPMG

Our focus on delivering value

RMF Capabilities

February 2017

kpmg.com

Introduction

KPMG LLP's (KPMG) Federal Cybersecurity practice assists Federal organizations in transforming their security, privacy, and continuity controls, while maintaining the confidentiality, integrity, and availability of critical business functions. KPMG is a preferred choice for clients due to our distinct strengths which include:

Our **razor-sharp focus** on delivering **value** – coming in on time and on or below budget

Our ability to navigate technically and organizationally **complex** environments to help you achieve success

Our **ability to leverage the latest technology** – using the most advanced technology to provide faster time to value, support lower risk, and ultimately lower costs.

Our ability to handle **scale** – our largest engagement is more than $100 million

Our **multidisciplinary** approach – leveraging KPMG's breadth and depth across risk management, organizational change, and financial management services.

RMF challenge

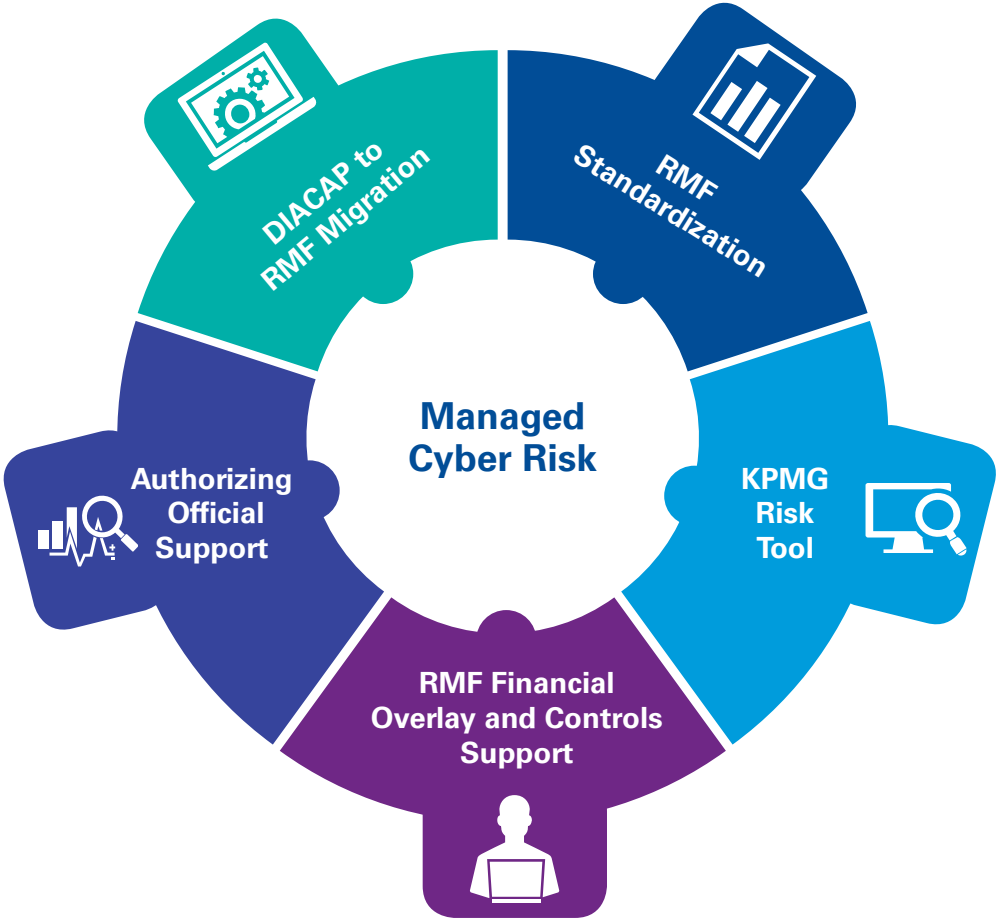
Same budget – increased level of effort (LoE)

While the Assessment and Authorization (A&A) program using the National Institute of Standards and Technology (NIST) RMF process reduces cybersecurity risk, it requires a larger level of effort establishing the program, migrate thousands of security authorization packages from the former Defense Information Assurance Certification and Accreditation Process (DIACAP), and then adding the new requirement for continuous monitoring. To compound the challenge, there are limited automated tools currently available to manage and sustain the RMF program, ultimately costing agencies more significantly time and funding.

Keep it simple – accessible, protected information

KPMG's approach to RMF is designed to be simple and effective, tailored to each agency and bringing experts in from both our federal and commercial sectors. Our approach follows NIST guidelines; includes industry best practices; and helps improve the risk-based culture towards cybersecurity. KPMG's capabilities help the security executive as well as the security engineer meet their responsibilities.

KPMG RMF core capabilities



RMF Information Systems Compliance (RISC) tool

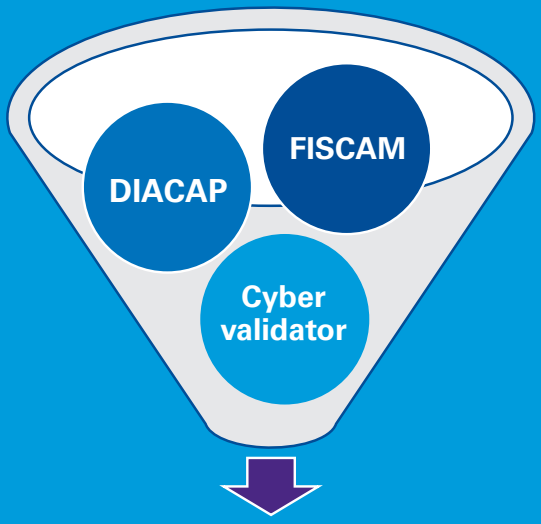
We are building a tool that automates and simplifies the workflows for complete process of RMF, significantly reducing the time and cost for package approval. Some of the major features include enterprise dashboards that continuously tracks status of every step in the RMF process in real-time, provides a complete audit history of every package, an interactive guide that simplifies data entry while making it more accurate and efficient, and a network discovery capability to quickly map the entire operating environment without referring to system diagrams.

KPMG

Key Differentiators by Step

RMF Financial Overlay and Controls Support

KPMG has been a leader in assisting Federal agency OIGs in implementing the CFO Act since its inception. Our Financial Audit Manual (FAM)/Federal Information System Controls Audit Manual (FISCAM) based audit approach has been successfully utilized at more than 50 annual Federal audits. KPMG utilized this IT audit experience to support the creation of the RMF FM Overlay to be applied as part of the RMF process to financial and financially relevant systems. The RMF Overlay maps audit-specific FISCAM control objectives to NIST SP 800-53 Rev 4 security controls and further defines how these controls should be implemented within systems to meet Financial Statement Audit requirements.



RMF ATO with FM Overlay

- Process for meeting multiple compliance work streams/requirements is consolidated to minimize the level of effort required by System Owners
- Meets objectives for FISCAM and Financial Statement Audit through the same process that is required to obtain your RMF ATO, with coordination of validation testing between the Cyber Validator and FM Validator

KPMG

RMF Standardization

While there is a standard process for implementing the RMF process at most organizations, there can be significant variance in executing a security package across the entire RMF process. KPMG provides a robust Internal Verification and Validation (IV&V) capability to understand and help minimize the variation that could occur with new or current RMF processes.

DIACAP to RMF Migration

KPMG provides strategic guidance for the CISO/ Information System Owners to develop a transition methodology based on an initial RMF Maturity Model assessment. We also have a repeatable and reproducible process for transitioning individual DIACAP packages to RMF packages.

Authorizing Official Support

Programmatic support to monitor RMF implementation progress, help manage delivery, and provide real time metrics to cyber executives.

Policy Development - Support for cyber policies and its supporting processes are developed based on security threat analysis and accepted recommendations to help reduce the risks posed by the threats. Our policies are written using the SMART rule: **S**pecific, **M**easurable, **A**greeable, **R**ealistic and **T**ime-bound.

Data Collection and Analysis – KPMG assist clients in sorting through the volume of data collected from all collecting points. Our methodology used sound knowledge management principles coupled with automated tools to provide actionable information.

Strategic Planning – KPMG assists with the development of strategy with a focused methodology that emphasizes close examination of the current and future strategic environment and consideration of alternative strategic concepts.

Cyber Risk Management – KPMG helps Federal Agencies and other government organizations identify and assess information security and privacy risks in order to develop associated actions and controls to mitigate risk to an acceptable level.

Incident Management and Response – KPMG assists clients in developing and implementing an effective and successful security incident response program through a comprehensive endeavor, which requires substantial enterprisewide planning, investment and resources.

Training - Training employees is a critical element of security. KPMG assists clients in communicating the value of protecting customer and colleague information and their role in keeping it safe. Our methodology involves putting practices and policies in place that promote security and training employees to be able to identify and avoid risks.

KPMG


Policy Development
Data Collection and Analysis
Training
AO Support
Strategic Planning
Incident Management and Response
Cyber Risk Management

KPMG Federal cybersecurity differentiators

Experience. For more than 100 years, KPMG has assisted the Federal Government. We understand the Federal Government and its business and technology challenges, including cybersecurity.

Knowledge. We possess the knowledge, insight, and awareness of cybersecurity standards, legislation and regulatory implications needed to address the needs of the Federal Government, notably the Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST), and Federal Risk and Authorization Management Program (FedRAMP).

Tailored Approach. We help transform Federal Government cybersecurity challenges into opportunities by combining our global KPMG cybersecurity commercial practice with cross-functional public sector knowledge, past lessons learned, open collaboration, leading practices and an insightful approach that is tailored to each Federal Agency's situation and needs.

Advanced Tools. KPMG's extensive network of alliances with the latest technology companies provide the most advance technology solutions available on the market today.

KPMG

KPMG cybersecurity recognition

KPMG is recognized as a **GLOBAL LEADER** for its Cybersecurity Services

Forrester, 2016 leader in **CYBER SERVICES**

Kennedy Vanguard, **"INFORMATION TECHNOLOGY"** Consulting to the Energy and Utility Industries (2014)

Kennedy Vanguard, **"Consulting to Public Healthcare 2015: Cybersecurity"**

Leader Quadrant: "Gartner Magic Quadrant for **Global RISK MANAGEMENT Consulting Services**

SailPoint, "2015 GLOBAL PARTNER of the Year"

"Cyber Investigation **TEAM OF THE YEAR** – USA" Acquisition International

According to "Information Security Consulting Services, Q1 2016," Forrester Wave

Key contacts

Tony Hubbard
Principal, Federal Cyber Lead
O: 703-286-8320
E: thubbard@kpmg.com

Anser Chaudhary
Director
O: 703-286-8660
E: anchaudhary@kpmg.com

Ken Adams
Director
O: 703-286-8102
E: kennethadams@kpmg.com

Stu Wharton
Manager
O: 571-635-4116
E: swharton@kpmg.com

KPMG

kpmg.com/socialmedia