KPMG

Becoming Audit Ready...

through Dynamic Cybersecurity Risk Management

May 2018

kpmg.com

Cybersecurity is a top concern for any Federal government organization, coupled with rapid technological advances and ongoing awareness of evolving vulnerabilities and threats to support organizational risk management decisions. Information Security Continuous Monitoring (ISCM) of federal information systems, including systems in-scope for a financial statement audit which facilitate financial transactions and business processes, utilizes the security controls assessment and authorization process to support a dynamic risk mitigation program where risks are evaluated on a continuous basis. The concept for the Authorization to Operate (ATO) through the application of a Risk Management Framework (RMF) for federal information systems is used to confirm that entities comply and require independent monitoring, and that they consider future threats and technologies. A key piece of becoming audit ready through dynamic cybersecurity risk management is to continuously monitor risks by applying the Financial Management (FM) Overlay to information systems which synchronizes the Federal Information System Controls Audit Manual (FISCAM) guidance with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, security controls catalog for unified security control management and implementation.

Challenge

CFO perspective

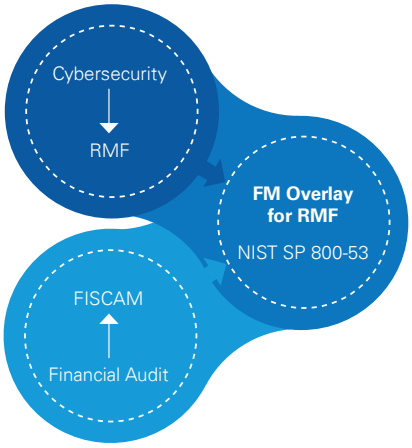
Federal agencies are inundated with multiple audit and compliance requirements across the board. As a Chief Financial Officer (CFO)/comptroller, you want to optimize compliance activities, reduce costs and respond to risks quicker and holistically. One of your primary duties is the stewardship of American taxpayer's dollars which includes the use of accurate and reliable financial data. Modern finance heavily depends on information systems to facilitate financial transactions and business processes with significant levels of automation. Do you have a control framework to help ensure proper reporting by those information systems? How do you synchronize and integrate the audit compliance requirements and needs with IT governance?

CIO perspective

Your agency relies on cybersecurity every day to both safeguarding information systems against threats and vulnerabilities while seamlessly delivering critical financial functions and business processes. Each stakeholder may have different priorities when it comes to IT. While the CFO community may prioritize the integrity and accuracy of the financial data and the business operations need continual availability to support e-commerce functions, secure systems are essential to achieve these priorities. How do you address those circumstances within your organizational cybersecurity program? What unique program requirements need to be implemented within your environment?

Solution

The Financial Management (FM) Overlay is a complimentary control framework that aims to seamlessly integrate audit readiness through cybersecurity risk management. The framework is based upon the NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* which contains a catalog of security controls required for Federal agencies. The FM Overlay which is applied to financial systems through the RMF process takes the NIST SP 800-53 and incorporates the Government Accountability Office's (GAO) *Federal Information Systems Control Audit Manual* (FISCAM) guidance along with KPMG's extensive experience in auditing Federal agencies in order to manage and implement unified security controls for continuous risk management.



Audit Readiness and Cybersecurity Risk Management Overlap
Manage and Implement Security Controls **ONCE** by applying the FM Overlay to satisfy both cybersecurity and financial audit requirements.

The FM Overlay's integration and supplementation with cybersecurity allows for the increased confidence of a Federal agency's information systems in undergoing audits, such as the financial statement audit. Using NIST SP 800-53 as the basis for securing information systems provides for a common reference for the CIO and CISO in implementing relevant security controls along the rigor for the audit with their cybersecurity risk management program.

Case Study

A major Federal agency early realized that their business systems are required to adopt a new cybersecurity framework and are most likely in-scope for the financial statement audit. The audit is also a new experience for the agency's personnel having questions such as:

1. How do I prepare my systems for the audit?
2. What could the auditor look at in my systems?
3. What documents the auditor may request for?

Solution

The agency decided to implement the FM Overlay on their business systems in conjunction with the mandated new cybersecurity RMF. They realized the FM Overlay is complementary and seamless with the RMF by allowing them to implement, assess, and monitor controls to better meet both cybersecurity and audit requirements. The FM Overlay enlightened them on what the audit could entail in regard to their systems' control environment, governance, and documentation. KPMG worked side by side with this agency throughout the implementation of the FM Overlay offering our insights into the realms of Federal audit and cybersecurity risk management.

End Result

The Federal agency came out better prepared and confident for the audit with the adoption of the FM Overlay. It is a key driver for their enterprise risk management and mitigation program by helping them integrate their efforts of enforcing security controls and mitigating deficiencies within the existing IT governance process. They applied the FM Overlay on their first information system to undergo this transformation, which then led to a chain of other successful implementations to support the adoption of the cybersecurity risk management framework. Senior leadership approved the continued operation of the system even with noted deficiencies knowing that with the FM Overlay, there is a path towards audit readiness along with a secure system where security controls are dynamically monitored for risk management.

KPMG's team of audit and cybersecurity professionals can offer insight and assist with the implementation and tailoring of the FM Overlay to better prepare your information systems and organization for audit and cybersecurity compliance in a changing information technology (IT) landscape defined by diverse service providers delivering a multitude of services in the larger enterprise. Lessons learned from our collaboration with federal partners in building a robust information security program, which meets audit requirements, include the critical need for the FM Overlay as a framework to manage, implement, and monitor the security risks for information systems within an organization. Our KPMG team has significant experience in dealing with regulatory compliance issues and developing processes that meet the expectations and requirements of the inspector general and independent oversight communities. In addition, our KPMG team has experience in identifying future risks, measuring the impacts of those risks and developing plans to mitigate them to support audit and cybersecurity compliance. Having an effective dynamic cybersecurity risk management program in place, one that utilizes the FM overlay, business processes, people, and technology to facilitate compliance with federal laws and regulations and to identify and prioritize issues associated with an organization's IT environment, helps to provide effective audit and cybersecurity posture for continuous sustainment.

Contacts:

Ginger Bonin
Managing Director
T: 703-286-8247
E: gbonin@kpmg.com

Anser Chaudhary
Managing Director
T: 703-622-5233
E: anchaudhary@kpmg.com

Nirali Chawla
Director
T: 703-286-6694
E: niralichawla@kpmg.com

Peichi Sopko
Manager
T: 703-962-5672
E: peichisopko@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia