KPMG

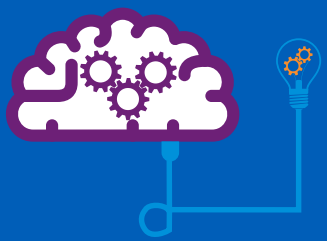
Security Program Management (SPM)

Build, enhance, manage information security programs

Overview

Security Program Management (SPM) helps enable agencies to be strategically aligned, resource optimized, controlled for risks, and built to achieve their goals. SPM provides agencies with insight on the risks present in the organization, how to develop plans to mitigate those risks, and the tools, services, and oversight needed to implement processes and technologies into their environment in a sustainable manner.

KPMG methodology



KPMG's Security Program Management (SPM) Methodology is based on leading information security frameworks, combined with our global insight of leading practices in risk management and cyber security. KPMG's Security Program Management framework/ methodology is primarily based on the Cyber Security Framework (CSF), National Institute of Technology (NIST) SP-800 series of publications, including the Federal Information Security Modernization Act of 2012, Defense Federal Acquisition Regulation Supplement (DFARS), Health Insurance Portability and Accountability Act (HIPAA) Security Rule, The Federal Risk and Authorization Management Program (FedRAMP) in order to provide to provide business-driven, risk-based security assessments in line with regulatory requirements and industry best practices. KPMG's Security Program Management methodology is flexible and can be tailored to meet organizational needs and internal requirements.

KPMG approach

KPMG Security Program Management focuses on risk assessments, incident reports, maturity assessments, gap analyses, and baseline assessments in order to align support security program operation, procedures, privacy, and security engineering with industry leading practices. We provide clients with management, guidance, and resources in support of a robust security management program.

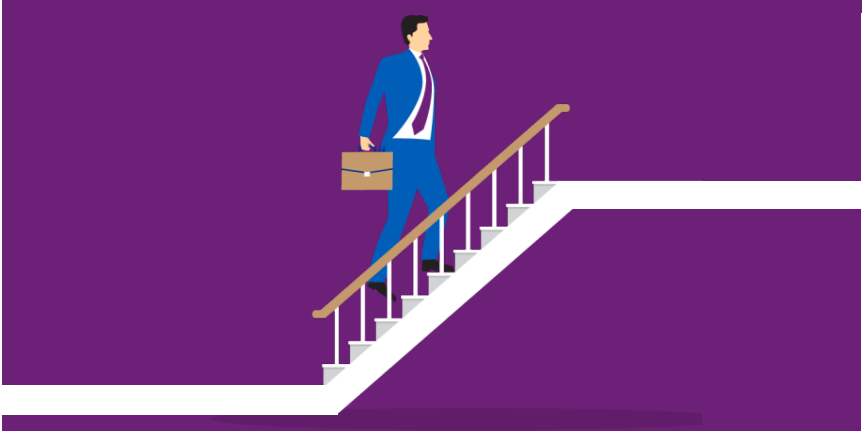
- ***Cyber maturity assessment (CMA):*** incorporate our insight into leading cyber practices from the public and private sectors. The assessment is targeted at Boards and senior executives to provide appropriate Board-level reporting and communications. The CMA framework leverages the NIST Cybersecurity Framework (CSF) and can be tailored to the specific requirements of our clients, yet is wide-ranging in its ability to address six key dimensions that together provide an in-depth view of an organization's cyber maturity.
- ***Compliance assessment:*** By assessing current-state security control processes, we assist clients in identifying needs, strengths, and weaknesses in the current environment as compared to peers and determining future business processes and technology that will be needed in order to mature the cyber security function.
- ***Technical security assessments:*** KPMG assists agencies in identifying vulnerabilities present in their wired / wireless network or application infrastructure and developing actionable remediation recommendations. KPMG can also assist agencies in the assessment or development of a vulnerability management program, aligned to your industry and investment appetite, or assess your service provider or approach to address the changed threat landscape and new technology platforms

Client challenges

KPMG Continuous Diagnostics and Mitigation (CDM) services deliver integration and architecture support to assist Federal Agencies in realizing value and achieving the goal of continuous compliance and authorization from their investments in CDM.

Today many Government agencies face a common set of security challenges:

1. **Lack of personnel trained in cyber security disciplines**
2. **Ever-evolving security frameworks and requirements**
3. **Limited alignment with organizational goals and objectives**
4. **Minimal or unstructured long-term security strategy**
5. **Inconsistent security solutions with limited or no standardization**
6. **Organizational reluctance to embrace new technologies, such as cloud services, due to security concerns**
7. **Inability to standardize or leverage knowledge from previous security projects**



SPM drivers

Some of the drivers for a SPM assessment for any organization include:

- ***Changing Threat Landscape*** drives to improve Security based on new threats and information provided by threat feeds.
- ***Evolving Technologies*** drives decision makers to seek to improve agency security posture due to ever-changing technologies and capabilities.
- ***Legal and Regulatory Requirements*** demand structured security program management to address the security needs based on Federal regulatory changes.
- ***Business Requirements*** motivate the organization in meeting business technical security needs.
- ***Risk Management and Compliance*** promotes the need for structured security program management ensuring IT security risks are mitigated with security solutions.

Benefits and outcomes

Potential client enhancements by adopting a Security Program Management framework:

01	Understanding and experience with relevant SPM implementation
02	Key vendor alliances (Sailpoint, Okta, RSA Archer, CyberArk, ServiceNow, ForeScout)
03	Over 100 years of Federal Government consulting proficiency
04	Technical and management niche experience
05	Strategic alignment with business goals
06	Value-added spend on Cyber security
07	Effectively protect from cyber attacks
08	Continuous monitoring of security posture
09	Business risk-focused security strategy
10	Auditable compliance
11	Sustainable protection and identification of ongoing security risks
12	Ongoing assessments of agency-defined policies (NIST, FIPS, etc.)
13	Broad knowledge of all SPM capabilities and requirements

Conclusion

KPMG Security Program Management (SPM) successfully aligns the focus for agencies to strategically optimize their security programs and effectively mitigate the ever present risks faced bvy organizations. The continued enhancement and building of a strong security program is paramount in the ability to sustain the effective mitigation of risk.

KPMG ensures that the sustainable management of risk through security program management through the delivery of baseline risk and maturity assessments, which enables agencies and organizations to shift its focus to identifying forward leaning strategies in operations, procedures, privacy, and engineering in alignment with industry best practices. Specifically, KPMG enhances the ability to drive agency security programs from initial maturity assessments to leading forward thinking strategic positioning for agencies and organizations to prepare and harden against an ever evolving threat landscape.

The ability to strategically optimize a security program at a high level allows for a clear direction in building and maintaining a robust and sustainable risk mitigation strategy. KPMG's Security Program Management enhances the strategy at a high level to promote the organic growth of security operations at a more foundational and granular level. KPMG provides the foundational support needed to develop the tools, services, and oversight required to implement a foundational level of processes and technologies to ensure risks are mitigated in a sustainable manner.

Helps enable agencies to be strategically aligned, resource optimized, controlled for risks, and built to achieve their goals. SPM provides agencies with insight on the risks present in the organization, how to develop plans to mitigate those risks, and the tools, services, and oversight needed to implement processes and technologies into their environment in a sustainable manner.

Contacts

If you have questions or want more details regarding KPMG's Security Program Management services, please contact us:

Tony Hubbard
Principal, Advisory
T: 703-286-8320
E: thubbard@kpmg.com

Kevin Bauer
Manager
T: (845) 313-0088
E: kbauer1@kpmg.com

kpmg.com/socialmedia