KPMG

Security Architecture

A business-aligned security design

Overview

- The President issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* on May 11, 2017, seeking to improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats. EO 13800 focuses Federal efforts on modernizing Federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure.

- In response to this tasking, the Department of Defense (DoD) working in concert with the Department of Homeland Security (DHS) began an effort to evolve the Federal Enterprise Architecture Framework (FEAF) to create implementation roadmaps for the DoD and Federal Agencies based on an end-to-end holistic review of the existing security architecture along with current implementations and plans. The results were two related frameworks – the Department of Defense Cybersecurity Analysis and Review (DoDCAR), and .gov Cybersecurity Architecture Review (.govCAR). These threat-based architecture frameworks provide the basis to discuss and assess cybersecurity architecture choices, empowering Departments and Agencies to make informed, threat-based risk management decisions.

Security architecture services

Security Architecture delivers business-aligned security design to support an organization's security strategy and target operating model. Security Architecture also aligns with Enterprise Architecture with necessary security components to support business needs.

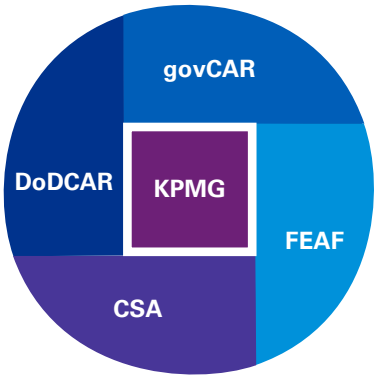
There are two (2) types of Security Architecture services:

1. **Enterprise Security Architecture** provides an end-to-end security design of an entire organization and aligns with the Enterprise IT Architecture.

2. **Security Solution Architecture** helps to create a design of one or more security solutions and how those solutions fit with the rest of the security environment.

KPMG methodology

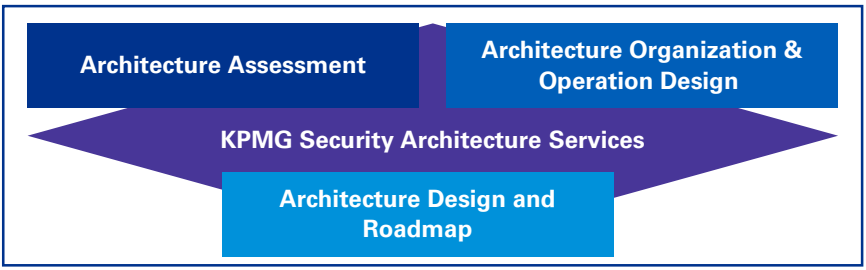
KPMG's Security Architecture framework/methodology is primarily based on the Federal Enterprise Architecture Framework (FEAF), Department of Defense Cybersecurity Analysis and Review (DoDCAR), and Cybersecurity Architecture Review (.govCAR) to provide business-driven, risk-based security architecture. It is further customized and enhanced using the Sherwood Applied Business Security Architecture (SABSA) to align with client's overall enterprise architecture. To drive a cloud strategy, KPMG Security Architecture methodology includes the capabilities of CSA (Cloud Security Alliance) Reference Architecture.



In keeping with the Federal Enterprise Architecture Framework (FEAF), Cloud Security Alliance (CSA), and threat-based assessment frameworks, DoDCAR, and .govCAR, KPMG's Security Architecture methodology is flexible and can be tailored to meet organizational needs and internal requirements. This also allows for an alignment with an organization's current security framework, such as, National Institute of Standards and Technology (NIST), Cyber Security Framework (CSF), or others, and/or regulatory requirements, such as, Health Insurance Portability and Accountability Act (HIPAA).

KPMG approach

KPMG Security Architecture Service offers three (3) areas of focus to assist our clients. These include assessment of security architecture, establishment of an architecture organization, and development of security architecture design.



Architecture Assessment: The objective is to develop an initial understanding of an organization's current state security architecture. KPMG identifies key business and regulatory drivers, conducts a deep-dive of the current security solutions, reviews security policies and architecture documentation, performs a Security Architecture Maturity Assessment, performs a gap analysis and provides recommendations to improve the overall maturity of the Security Architecture program.

- ***Architecture Organization & Operations Design:*** The objective is to define Security Architecture organizational capabilities. During this phase KPMG will review current Security Architecture organization capabilities and review current processes and procedures followed by the Security Architecture organization. KPMG assists the client with establishing a Security Architecture Governance model and creates/ updates processes for the Security Architecture organization. KPMG has the ability to provide assistance with implementation of an Enterprise Security Architecture artifacts tracking tool.
- ***Architecture Design and Roadmap:*** The objective is to develop an in-depth future state architecture design based on cyber strategy and target operating model. KPMG will gather comprehensive business, IT and security requirements to assist in the development of a security reference architecture, a future state enterprise security and/or individual solution security architectures. KPMG will develop a security roadmap to implement the future state security architecture.

Client challenges

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

1. **Lack of personnel trained in cyber security disciplines**
2. **Limited alignment with organizational goals and objectives**
3. **Minimal or unstructured long-term security strategy**
4. **Inconsistent security architecture and security solutions with limited or no standardization**
5. **Solutions providing a band-aide fix to mitigate findings due to an incident, leading to a vast list of security solutions to fund and manage**
6. **Organizational reluctance to embrace new technologies (cloud, AI, IoT, others) due to security concerns**
7. **Existence of "shadow IT" stemming from organizational reluctance**
8. **Inability to standardize or leverage knowledge from previous security projects**

Security architecture drivers

Some of the drivers to develop a standardized security architecture for any organization include:

Changing Threat Landscape drives Security Architecture to improve Security based on new threats and information provided by threat feeds.

Evolving Technologies drives architects to always look to improve agency security posture due to ever-changing technologies and capabilities.

Legal and Regulatory Requirements demand a structured security architecture to address the security needs based on Federal regulatory changes.

Business Requirements motivate Security Architecture in meeting business technical security needs.

Risk Management and Compliance promotes the need for a structured Security Architecture in place ensuring IT security risks are mitigated with security solutions.

Benefits and outcomes

Potential client benefits by adopting a standardized/structured security architecture framework:

01	Security architecture strategically aligned with business goals
02	Value-added spend on Cyber security focused on improving overall capabilities
03	Security architecture fully integrated with enterprise architecture
04	Effectively protect critical business assets from cyber attacks
05	Architecture facilitates continuous monitoring of security posture
06	Architecture manifests a business risk-focused security strategy
07	Architecture promotes auditable compliance
08	Architecture facilitates move to continuous authorization

Conclusion

Based upon several Federal and industry architecture frameworks, the KPMG Security Architecture Service provides the foundation for Agencies to plan, develop and deploy a threat-based cybersecurity architecture that aligns with business and mission needs, and facilitates informed, threat-based risk management decisions.

Contacts

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

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

Shane Cashdollar
Director, Advisory
T: 703-286-8236
E: scashdollar@kpmg.com

Sallie Sweeney
Director, Advisory
T: 703-286-8000
E: salliesweeney@kpmg.com

Joe Faraone
Director, Advisory
T: 703-286-8000
E: jfaraone@kpmg.com

kpmg.com/socialmedia