



KPMG Cyber

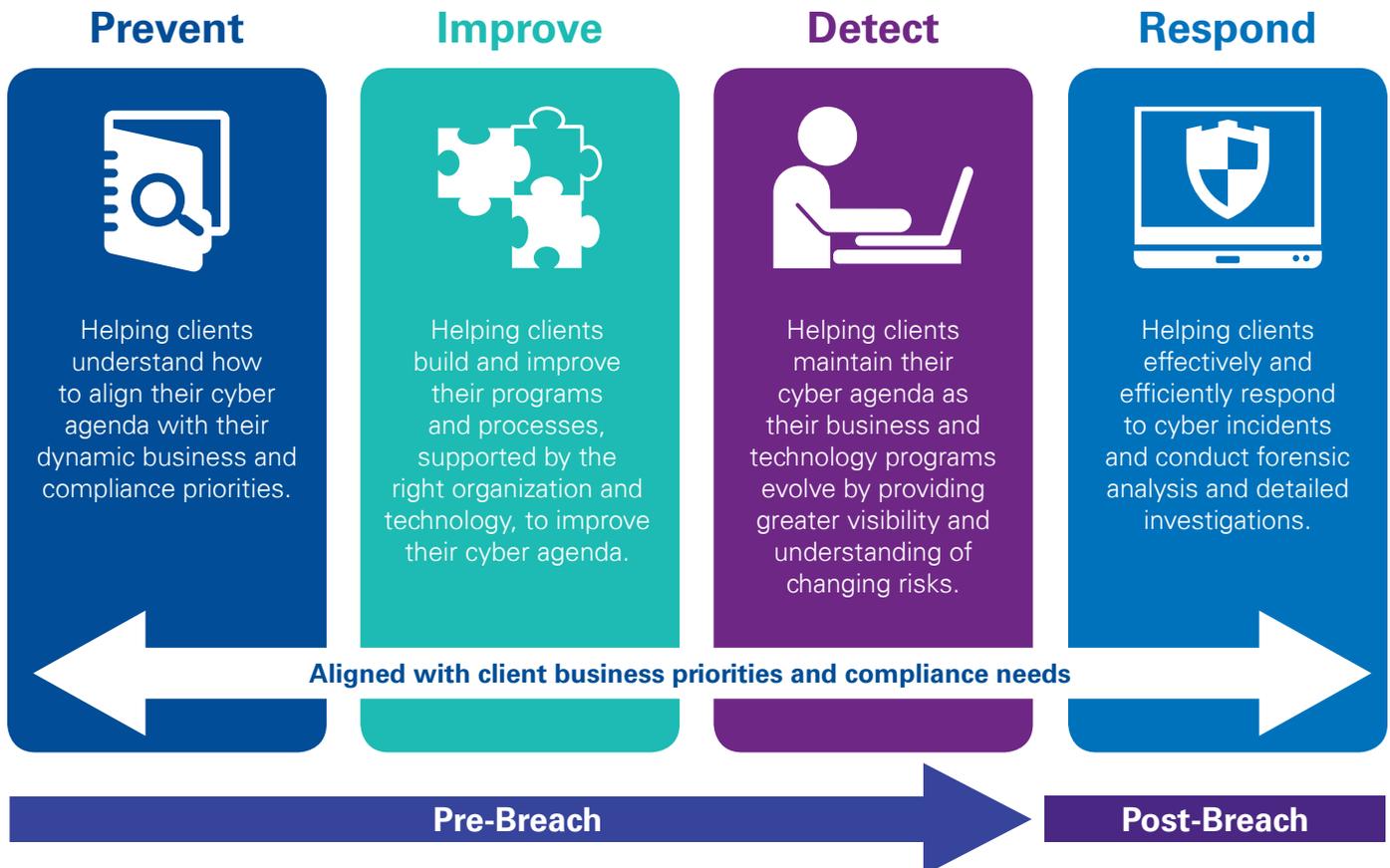
Federal Government

KPMG LLP (KPMG) 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:

- Our **razor-sharp focus** on delivering **value**—aiming to come in on time, on budget, and in scope
- Our ability to navigate technically and organizationally **complex** environments to help you achieve success
- Our **accelerated robust tools**—designed to provide faster time to value, support lower risk, and leverage appropriate technology
- Our ability to handle **scale**—our largest client’s budget is more than \$1.2 billion, and our largest engagement is more than \$100 million
- Our **multidisciplinary** approach—leveraging KPMG’s breadth and depth in areas ranging from risk management to organizational change, and from forensic investigation to economics.

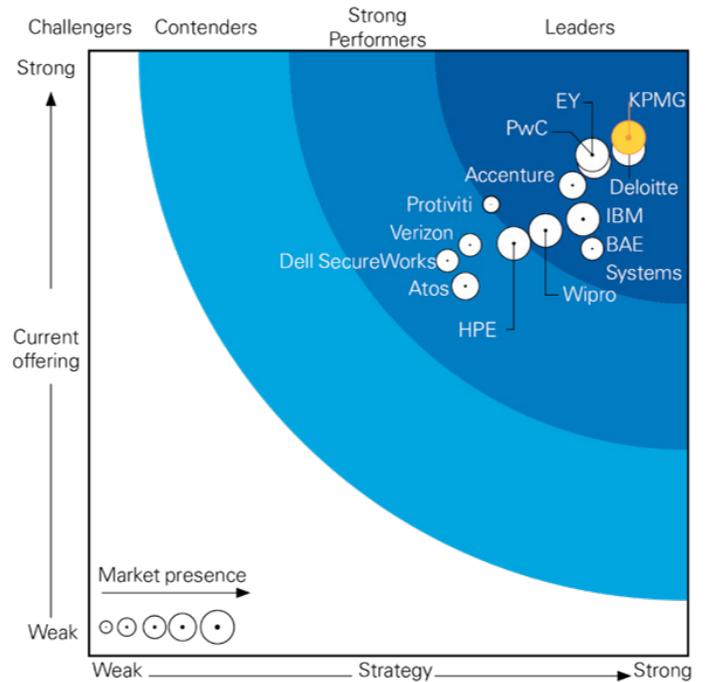
Keep it simple – accessible, protected information

KPMG’s approach to cybersecurity is designed to be simple and effective—it also aligns to the needs of our clients in resolving their security services and follows a “Prevent/Improve/Detect/Respond” model.



Forrester Wave Q1 2016

“ KPMG is recognized as a Global Leader for its Identity and Access Management Services. KPMG has moved cybersecurity to the heart of its business. KPMG recently listed cybersecurity as one of its six strategic growth initiatives as well as a key to all other initiatives. To bolster this commitment, the company has increased and deepened its range of services, investing heavily in R&D and acquisitions. KPMG has a clear view of the relevant security issues for business executives and technicians. Clients applaud KPMG for being “doers” and easy to work with. They also identify strategic advice, subject matter expertise, flexibility and adaptability, and delivery of commitments as being strengths for KPMG. ”



The Leader on The Forrester Wave™:
Information Security Consulting Services, Q1 2016

A representative sample of KPMG's Cyber capabilities

Strategy and governance

- CyberSecurity/Maturity Assessment
- Risk Management Framework
- Security Strategy Alignment w/ Business Goals/Objectives
- Metrics/Reporting/Dashboards
- Security Organization & Governance
- Security Architecture
- Policy & Procedure Improvement
- Privacy Strategy & Assessment
- Social Media Strategy, Policy Development, and Monitoring
- Data Governance Strategy Development
- Enterprise Risk Management
- Vendor Security/Privacy Programs
- Compliance/Framework Gap Assessment
- Business Impact Assessments
- Business Continuity and Disaster Recovery
- Planning and Coordination
- High-Availability Design and Implementation
- Crisis Management and Contingency Planning
- Information Security Metrics

Transformation and implementation

- Identity and Access Management (IAM)
- IAM Current-State Assessment
- IAM Strategy and Road Map
- Privileged User Management
- Cloud IAM
- IAM Project Governance
- Role Management/Engineering
- Access Certification and Compliance
- Identity Federation
- Access Management and User Provisioning
- Archer and IT Governance, Risk, and Compliance (GRC) Integration and Implementation
- Vulnerability Management/ Incident Response Program Integration with GRC Solution
- Logging Monitoring and Analytics
- Asset Protection
- Security Program Delivery
- Industrial Control Systems Security
- Information Security Metrics

Cyber risk

- Global Vulnerability and Penetration Security Assessment
- Malware Assessment
- Application/Host/Database Virtualization Security Assessment
- Mobile Application Code Security Review and Integration
- Forensic Analysis and Support
- Cloud-based Security Assessment
- Security Operations Center Strategy, Design and Implementation
- Vulnerability and Incident Management Strategy, Design, and Implementation
- Security Analytics
- Log Management, Security Monitoring, and Analysis
- Incident Response Program
- Technical Remediation Activities

Cyber response and investigations

- Investigation Services:
- Cyber Investigation & Digital Evidence Recovery
- Cyber Investigation Assessment Response
- Merger and Acquisition (M&A) cyber due diligence
- Preventive Services:
- Cyber Threat Risk Assessment
- Third-Party Threat Intelligence Model Development
- Cyber Attack Detection Program Development
- Cyber Awareness Training
- Malware Analysis
- Cyber Threat Intelligence “Red Team” Service
- Corporate Intelligence Services

Contact us

Tony Hubbard
Principal

T: 703-286-8320

C: 202-486-4945

thubbard@kpmg.com

Ken Adams
Director

T: 703-286-8102

C: 202-285-2750

kennethadams@kpmg.com

kpmg.com/socialmedia



For more information and insights, visit kpmg.com/us/federalcyber.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A. NDPPS 627393

The KPMG name and logo are registered trademarks or trademarks of KPMG International.