



# KPMG cybersecurity and technology risk solutions for government

KPMG LLP (KPMG) helps government organizations strengthen cybersecurity, streamline risk management, and modernize systems to help reduce complexity, enhance resilience, and align security with business objectives. Through advanced analytics, automation, cloud security, and integrated risk management, we help enhance decision-making, safeguard critical assets, and build stakeholder trust in an evolving threat landscape.

# Zero trust

Zero trust (ZT) helps government agencies achieve their missions in a world where technology simultaneously creates opportunity and risk.

We support an organization's ZT vision and architectures with innovative strategies, methodologies, and transformations that deliver enhanced security with improved technology integration. When thoughtfully deployed, a ZT architecture can simplify the technology stack, lower compliance costs, thwart advanced adversaries, and provide employees with a more secure, seamless user experience.

## ZT integration office

- ZT assessment, gap analysis, and roadmap
- ZT strategy, governance, and data analytics
- ZT metrics and reporting
- ZT organizational change management and strategic communications
- Application discovery and rationalization

## ZT networking and architecture

- Macrosegmentation, microsegmentation, and software-defined perimeters
- ZT network access and secure access service edge
- Secure applications and APIs

## Identity, credential, and access management (ICAM) transformation

- ICAM strategy and governance
- ICAM policies and procedures development
- ICAM implementation and integration
- Attribute identification and lifecycle management

# Security transformation

We help organizations adapt to emerging threats, strengthen security, and maintain trust through robust strategies, risk management capabilities, and governance frameworks aligned with business goals.

## Strategy and governance

- Security program management and governance
- Cybersecurity supply chain risk management development and operations
- Organizational change management
- Security metrics (KPIs, KRIs)
- Asset inventory and data management
- Business continuity and disaster recovery

## Threat management

- Incident management and response planning
- Data-driven anomaly detection
- Vulnerability management and risk scoring
- Threat intelligence
- Resiliency and recovery
- Trusted AI
- Security operations
- Security orchestration, automation, and response



# Security integration

We help agencies build, deploy, and sustain secure cloud platforms, execute system modernization across the software development lifecycle, and integrate advanced cybersecurity measures to protect and monitor systems in real time.

## Platform security

- Securing Microsoft, ServiceNow, Workday, Salesforce, and SAP applications
- Cloud security architecture, integration, and compliance
- DevSecOps
- ZT integration and compliance
- Risk management framework

## Operational technology (OT) security

- OT security assessment, design, and roadmap
- Security for embedded technologies
- Legacy system modernization
- Smart solutions
- ZT architecture and integration

# Risk modernization

With advanced risk assessment tools, analytics, and continuous monitoring approaches, we can help manage operational, financial, and regulatory risks related to technology. We can help with system accreditation and Authority to Operate (ATO), and help improve operational efficiency, compliance, and audit readiness with business process reengineering (BPR).

## Risk management framework (RMF)

- RMF implementations
- Risk assessments
- IT controls assessment and validation
- ATO and continuous ATO
- Continuous monitoring and dynamic risk identification
- Ongoing authorization

## Control monitoring, testing, and remediation

- IT control identification and optimization
- IT control assessments and remediation
- BPR
- Audit readiness, coaching, liaison, and remediation
- Internal compliance and control strategy, coordination, and training

# Why KPMG

KPMG has worked with federal, state, and local governments for more than a century. We have over 1,500 dedicated cybersecurity professionals worldwide, and have been recognized by Forrester, IDC, and ALM Intelligence as a leading global organization of professional services in cybersecurity.<sup>1,2,3</sup>

We're a multidisciplinary organization with business, technology, data and AI, risk, audit, and change management professionals working together using a "one firm" approach. We combine our cybersecurity acumen, government operations experience, and cross-sector and cross-disciplinary experience to deliver robust security solutions that meet the needs of today's government organizations.

We also maintain access to leading technology and expertise through our alliance partners, including:

- ServiceNow
- Microsoft
- Illumio
- Zscaler
- Okta
- SailPoint
- Saviynt
- Ping Identity
- CyberArk
- Google Cloud
- CrowdStrike
- Workday
- Salesforce
- SAP



1. "ALM Intelligence Pacesetter Research: Cybersecurity 2022-2023," ALM Global Properties, April 2022.  
2. Philip D. Harris, "IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment," October 2023.  
3. "The Forrester Wave: Cyber Risk Quantification, Q3 2023," Forrester, 2023.

# Contact us

Talk to our team about how we can help you manage and transform your cybersecurity and risk program.



**Tyler A. Carlin**

Director, Advisory  
KPMG LLP

240-306-5097

[tcarlin@kpmg.com](mailto:tcarlin@kpmg.com)



**Nate Deshong**

Director, Advisory  
KPMG LLP

843-327-6641

[ndeshong@kpmg.com](mailto:ndeshong@kpmg.com)



**Al Yeasin**

Director, Advisory  
KPMG LLP

703-380-3774

[ayeasin@kpmg.com](mailto:ayeasin@kpmg.com)

---

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

Learn about us:



[kpmg.com](https://kpmg.com)

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

