KPMG

Cyber Managed Services

Accelerate and sustain transformational outcomes to help strengthen your cyber defenses

A managed service approach that drives transformational outcomes

KPMG Cyber Managed Services can accelerate your transition to agentic cyber operations and lead to transformed cyber defenses.

KPMG LLP offers a broad suite of cyber managed services—powered by AI, automation, and leading technologies, all backed by our skilled teams. These fully managed offerings provide the security, confidence, insight, and visibility you need to help fortify your enterprise digital defenses.

Managed Identity Services

Privileged access management | Access management | Identity governance and administration

Protecting your business starts with controlling access

Identity touches every aspect of an organization and is the cornerstone of security. Done right, an identity management solution must continuously evolve to improve efficiencies, increase usability, and reduce risk.

Our Managed Identity Services offerings empower your business by enhancing visibility, enabling control over access and entitlement to your digital assets, and enabling efficient, scalable identity governance through our continuous application integration and onboarding processes.

Managed Cyber Risk

Third-party security | Governance, risk, and compliance

Strengthen visibility, security, and trust across your vendor ecosystem

Our Managed Cyber Risk offerings help organizations continuously assess, monitor, and manage vendor security and risk concerns.

Our teams help manage and mitigate the inherent risks of today's enterprise environments to reduce exposure, improve efficiency, and help ensure compliance.

Managed Security Testing

Cyber defense testing

Application security testing

AI security testing

Continuous threat exposure management

Cyber defense confidence through continuous validation

Our Managed Security Testing offerings help to protect your business by identifying unknown security exposures in your applications and infrastructure before being exploited, leveraging offensive testing, attack simulation and informed, risk-based, cyber defense improvement recommendations.

Our solution can help manage and drive informed cyber decision enablement across the enterprise, including your supply chain.

Cyber Threat Management

Managed detection and response | Cyber threat intelligence | Threat hunting

Early detection through extensive, enterprise-wide visibility

Protecting the business from digital compromise requires an approach that targets both reactive and proactive defenses.

Our Cyber Threat Management offerings provide the visibility, instrumentation, and consultation to drive early warning, early risk, and attack detection, coupled with intelligent, enterprise-wide response.

© 2026 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.

Drivers for managed services

Which situation applies to you?

- Need to materially improve in one or more cyber operational areas, quickly and cost effectively.
- Challenges hiring and retaining cyber talent.
- Desire to shift existing cyber talent to more strategic, project-based focus and less on "day-to-day" operational tasks.
- Outgrown or unhappy with current managed services provider.
- Made significant investment in cyber technology but need a partner to optimize my investment.
- Desire to consolidate managed service vendors.
- Need to modernize cyber technology enablement.

How KPMG can help

- Embedding technology uplift and transformation are part of our managed services.
- Our automation led innovation will drive cost efficiency with measurable results.
- Our breadth of cyber managed service offerings will cover most of your cyber operational needs.
- Our accelerators, assets, and alliances will enhance your investment on cyber operations technologies.
- Our delivery model will provide a tailored experience that is different than traditional managed service providers.
- Our emphasis on quality and continuous improvement will help ensure we evolve our service as your business and requirements change.

67% Two out of three organizations report a lack of essential talent and skills to meet their security requirements.

World Economic Forum Global Cybersecurity Outlook 2025

Cost effectively accelerate and sustain transformational improvements.

Shift the responsibility of innovation and continuous improvement to KPMG.

© 2026 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.

Managed Identity Services

Identity and access control for secure, scalable digital operations

KPMG Managed Identity Services helps organizations strengthen security, improve user experience, and reduce operational burden through continuous identity management, backed by AI-powered automation and skilled global resources.

Core offerings

Privileged access management:
Continuous monitoring and management of privileged accounts to prevent misuse or compromise.

Access management:
Continuously monitor and control user access to systems and applications, enforcing authentication and authorization protocols to prevent unauthorized entry and protect sensitive resources.

Identity governance and administration:
Automated provisioning, role management, and compliance enforcement for identity lifecycle operations.

Value-added outcomes

- Reduced risk through automated control and continuous monitoring.
- Improved compliance with evolving regulations and policies.
- Enhanced user experience with frictionless access management.
- Greater efficiency through automation and global delivery.
- Predictable cost and ongoing innovation through a managed subscription model.

KPMG assets and accelerators

- Intelligent orchestration and workflow automation standardize identity processes and accelerate access requests.
- Continuous monitoring and analytics enhance compliance and optimize user experience.
- Access certification and attestation streamline review and validation of user access rights to meet regulatory and audit requirements.
- Integrated delivery and support model provides 24x7 operations backed by skilled global resources.
- Enhanced through platform integrations with: Sailpoint, Saviynt, CyberArk, BeyondTrust, Okta, Microsoft, ServiceNow, Ping, and other custom applications.

© 2026 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.

Managed Cyber Risk

Strengthen visibility, security, and trust across your vendor ecosystem

As reliance on third parties grows, so does exposure. KPMG Third-Party Security combines advanced analytics, automation, and cyber expertise to help organizations continuously assess, monitor, and manage vendor security and risk concerns—reducing exposure, improving efficiency, and ensuring compliance.

Core offerings

Third-party security:
Assess vendors for business impact and inherent risk, evaluating their controls and vulnerabilities, continuously monitoring risk posture with AI and threat intelligence, and supporting decision-making with comprehensive reporting and analytics.

Governance, risk, and compliance:
Modernize traditional, manual GRC processes through integrated workflows, enriched data insights, and AI-enabled automation, thereby enhancing efficiency, consistency, and visibility enterprise-wide while effectively addressing fragmented data and communication.

Value-added outcomes

- Reduced third-party onboarding cycle times and program costs.
- Real-time visibility into third-party security, risk, and performance.
- Continuous compliance confidence across complex vendor networks.
- Stronger, data-driven decision-making through unified reporting.
- Automated, AI-enabled lifecycle management for cost efficiency.

KPMG assets and accelerators

- KPMG KACEY™, a KPMG intelligent automation framework to model risk and streamline vendor workflows.
- AnalyzeNow, a KPMG generative AI tool to validate controls and accelerate document review.
- Automated workflows that connect procurement, GRC, and risk-intelligence platforms.
- Vendor-risk scorecards for real-time insight into posture, trends, and remediation.
- Enhanced through platform integrations with: ServiceNow, OneTrust, Archer, Aravo, CyberGRX, KY3P, and Coupa.

© 2026 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.

Managed Security Testing

AI-enabled testing to continuously uncover and validate security exposures

KPMG Managed Security Testing combines human expertise, automation, and threat-informed analytics to help organizations stay ahead of emerging risks and compliance requirements across their applications, infrastructure, and cloud environments.

Core offerings

Cyber defense testing:
Vulnerability and penetration testing of network and endpoint controls, including segmentation and breach scenarios. Adversarial emulations of red- and purple-team exercises (real world and collaborative) to evaluate detection and response maturity.

AI security testing:
Assessment of AI systems such as large language models and agentic AI to uncover vulnerabilities in authentication, authorization, and configuration.

Application security testing:
Both automated and manual testing to uncover vulnerabilities in web, mobile, and API layers.

Continuous threat exposure management:
Proactive management of cyber risk across your environment is enabled through an AI-driven exposure management approach, powered by our continuous exposure management platforms and guided by our cyber defense advisors.

Value-added outcomes

- Continuous validation of application, infrastructure, and cloud controls.
- Faster remediation through automation and prioritized risk insights.
- Predictable subscription model for ongoing validation without administrative overhead.
- Greater confidence in compliance and audit readiness.
- Lower total cost and operational burden versus ad-hoc or annual testing.

KPMG assets and accelerators

- Security questionnaires and architecture reviews provide expert validation of control design, configuration, and compliance posture.
- Automated scan orchestration streamlines scheduling, execution, and reporting across testing types.
- Centralized analytics and dashboards correlate test data to highlight critical exposures.
- AI-based remediation guidance maps findings to business impact and compliance priorities.
- Continuous threat-intelligence feeds update testing logic and improves detection accuracy.

© 2026 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.

Cyber Threat Management

Early-stage, high-confidence cyber risk exposure detection and response

Core offerings

Managed detection and response:
24x7 monitoring and response for cyber attacks and enterprise risk exposure, including insider threat, insecure configuration changes, and OT/IT/Cloud.

Cyber threat intelligence:
Operational cyber threat monitoring, strategic and tactical intelligence, early warning intelligence that informs your cyber defenses.

Threat hunting:
Hypothesis-driven, intelligence-led threat hunting across your enterprise.

Value-added outcomes

- Assigned cyber advisor to provide proactive defense consultation
- Automated, enterprise-wide attack containment at your control
- Enhanced cyber defenses via our assigned cyber threat intelligence team supported by industry leading cyber threat intelligence sources
- Identify risk exposure events in your environment beyond cyber attack and malware detection
- Boost confidence in supply chain security with our external monitoring solution
- Collaborative threat hunting across your security tooling
- Custom, insightful reporting to drive cyber defense improvements

High confidence

Proactive defense

—

Early warning

—

Early detection

—

Curated experience

KPMG assets and accelerators

- Threat hunting platform (600+ packages) to improve scale
- SOAR platform to enable automated, orchestrated, enterprise-wide cyber attack containment
- Industry leading cyber threat intelligence solutions
- External monitoring platform to detect early-stage compromises that bypassed your internal monitoring tools
- Attack path discovery platform to proactively plug critical exposure gaps
- Cyber defense advisors across cyber functional domains
- Leading incident response capabilities
- Enhanced through platform integrations with: Microsoft, ServiceNow, Google and Crowdstrike.

© 2026 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 value

Each of our services combine advanced technologies, leading practices, well-established processes, and our experienced specialists' deep knowledge of your environment, to provide you with a curated experience that helps optimize your investment and strengthen your cyber defense. The result is reduced risks and confidence that your cybersecurity operations are managed consistently, efficiently, and cost-effectively. Our suite of KPMG Cyber Managed Services offerings focus on delivering outcome-based results that help build resilience and trust in your cyber operations.

- Extensive solution set
- Global scale
- Risk intelligence
- Operational automation
- Pragmatic innovation
- Curated experience
- Predictable costs
- KPMG assets and accelerators

With nine cyber delivery centers and over 6,000 global cyber security professionals, we have the scale, experience, and resources to help deliver on your cyber goals.

Core delivery principles

The KPMG delivery philosophy is centered on six core principles that guide how we provide demonstratable, value-based outcomes.

01 Enhance user experience

"Assigned Core Delivery Team" and "pod" based analysts model with experience in selected service areas that know your preferences so we can intuit your needs, and expectations.

02 Emphasis on quality – by design

Quality controls are built into our processes by design to "get it right the first time" and enhance our outcomes.

03 Tailor and evolve to your needs

The services you need today are not the same as they will be in the outlying years. We will maintain our delivery flexibility to tune our services as your needs evolve.

04 Focus on efficiency

Process simplification and automation for both our operations and your tasks are at the heart of what we do and will be at the center or what we bring to your experience.

05 Facilitate interrelated functional capability uplift

Our managed inter-lock approach will help connect adjacent functions to help drive improvements in your broader cyber defenses.

06 Continuously learning and improving

Observing collectively between our team and yours to identify, prioritize, track and report to help improve current state capabilities.

© 2026 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.

To learn more about how KPMG can help with your cybersecurity goals, get in touch.

Chris Crevits
Principal, Advisory
Cyber Managed Services
KPMG LLP
T: 314-307-0762
E: ccrevits@kpmg.com

Evan Rowell
Managing Director
Cyber Managed Services
KPMG LLP
T: 704-219-8109
E: erowell@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 more about us: **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.

© 2026 KPMG LLP, a Delaware limited liability partnership and its subsidiaries are part 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.