Advancing Governance Innovation and Risk Management for Cybersecurity Priorities

Services to assess agency management's alignment with cross-agency cybersecurity investment priorities

The Challenge

Office of Management and Budget (OMB) Memorandum 24-14 (M-24-14), *Administration Cybersecurity Priorities for the FY 2026 Budget*, issued on July 10, 2024, requires Executive Agencies to consider and respond to the Administration's cross-agency cybersecurity investment priorities within their FY 2026 Budget submissions.

M-24-14 emphasizes the importance of sustained investments across five pillars to enhance the nation's cybersecurity posture: (1) defending critical infrastructure through zero trust architectures, technology modernization, and leveraging government-managed cybersecurity shared services; (2) disrupting and dismantling threat actors by prioritizing resources to investigate and combat cybercrimes; (3) shaping market forces to drive security and resilience and accountability; (4) investing in a resilient future by supporting the National Cyber Workforce and Education Strategy (NCWES); and (5) preparing for the post-quantum future, and forging international partnerships to pursue shared goals by expanding global cyber capability building efforts.

Performance Audits, Council of the Inspectors General on Integrity and Efficiency (CIGIE) Blue Book Evaluations, or an Agreed-Upon Procedures (AUP) approach, using National Institute of Standards and Technology (NIST) criteria, and applicable American Institute of Certified Public Accountants (AICPA) Audit or Attestation standards, aligned with cybersecurity requirements, can provide agencies with trustworthy results that promote compliance and deliver insights to the agency.

Chief Information Security Officers (CISO) and Agency Inspectors General (IG) should consider these questions when defining their agency's risk management posture:

01	How will the agency modernize its defenses by transitioning to zero trust architectures and prioritizing technology modernization?
02	How will the agency prioritize resources to investigate cybercrimes, disrupt threat actors, and dismantle ransomware infrastructure?
03	How will the agency leverage federal procurement to improve accountability with Government-specified minimum secure software development practices?
04	How will the agency support the NCWES to address challenges in hiring and retaining cyber professionals?
05	How will the agency expand global cyber capacity efforts and improve collaboration with international law enforcement partners?

How KPMG LLP (KPMG) can help

We bring an experienced team that understands what agencies need to achieve the requirements of OMB M-24-14. Our team has direct experience conducting performance audits, evaluations and AUPs over the areas described in OMB M-24-14 and our team's experience means less upskilling and reduced audit risk.

KPMG understands the importance of maintaining a strong cybersecurity posture and investing in enhancements to meet and align with federal and regulatory mandates. We leverage our experience and knowledge of cybersecurity, information technology controls, and federal operations to execute performance audits, CIGIE Blue Book Evaluations, and AUPs for our clients. We work together with our clients to target the most pressing issues facing them and devise the right performance audit, CIGIE Blue Book evaluation, or AUP to meet their risk management or compliance needs.

Performance audits are an independent and objective examination of the efficiency and effectiveness of government programs or operations. CIGIE Blue Book Evaluations are designed to ensure that federal inspection and evaluation work adheres to high standards of quality, integrity, and accountability. Agreed-upon procedures report on a subject matter or an assertion about a subject matter under the responsibility of another party.

Prior to submitting a response to the administration's cybersecurity priorities in the FY 2026 Budget submission to OMB and the Office of the National Cyber Director (ONCD), KPMG can assist agencies by conducting performance audits, CIGIE Blue Book Evaluations, and AUPs to evaluate performance measurement strategies associated with budget requests, assess current and target maturity levels for high-value assets and high-impact systems, and analyze the feasibility of government-managed cybersecurity shared services.

Additionally, KPMG can support Sector Risk Management Agencies by conducting performance audits, CIGIE Blue Book Evaluations, and AUPs to evaluate cybersecurity risk initiatives.

Our professionals help federal agencies identify and evaluate the risks and results associated with cybersecurity to enhance their security posture and operational effectiveness. At KPMG, we have supported federal agencies through the execution of performance audits in the areas noted above, as well as in the areas of cybersecurity, zero-trust, technology modernization, insider threat, the evaluation of shared services and third-party providers, and regularly perform vulnerability and penetration testing performance audits and AUPs for our clients.

KPMG is a leading provider of financial statement and IT assurance engagements to the federal government. We have the team, expertise, and experience to help you achieve your agency's objectives related to OMB M-24-14.

Contact us

Jason A. Gould
Managing Director
T: 703-286-6896
E: jagould@kpmg.com

Alvamerry Schaefer
Director
T: 703-286-6956
E:aoschaefer@kpmg.com

Learn about us: **kpmg.com**