From burden to battlefield: Accelerating ATOs with the new cybersecurity risk management construct

Cumbersome and slow is not a requirement of compliance. Adaptable, dynamic, and flexible compliance can be a reality.

Over the last dozen or so years, executing the risk management framework (RMF) and obtaining an authority to operate (ATO) has increasingly become a burdensome and time-consuming effort, robbing the Department of Defense (herein referred to as Department of War or DoW) of agility and impeding its ability to empower the warfighter with leading-edge technology.

And so, the newly released **cybersecurity risk management construct** (CSRMC) comes as welcome relief. The RMF's manual evidence collection and paper-based accreditation packages had been introducing multimonth delays at a time when cyber threats are evolving by the hour, leaving systems exposed to adversary innovation and undermining the very purpose of the RMF as a safeguard against dynamic risk.

The CSRMC marks a pivotal shift in how cyber risk is managed, transitioning from the RMF's reliance on static, manual, checklist-driven assessments to a more dynamic, automated, and continuous approach. This article highlights the shift through use cases that demonstrate CSRMC principles in action, from proactive risk monitoring to automated control validation.

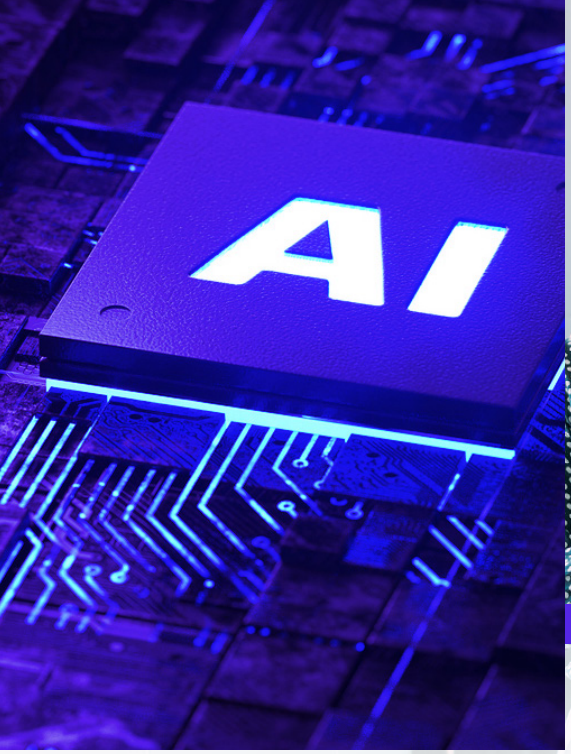
Mission before metrics

Few would argue that the goals of the RMF had become obsolete. The problem isn't with its standards but with its implementation. Traditional RMF execution had become so checklist-driven that it often devolved into a compliance exercise versus a security evaluation. But compliant does not necessarily equate to security or operational sustainability.

Why modern government is important

Government agencies in the US must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

The CSRMC doesn't eliminate compliance but instead re-focuses the RMF first and foremost on security and mission effectiveness. The CSRMC is as much a cultural change as it is a process or technology one. Many security officers and assessors had become conditioned to execute RMF steps as a procedural exercise, often without considering the actual security value those steps provide. Each control may appear equal on paper, but the impact on threat mitigation and mission resilience varies widely. While RMF remains valid, the CSRMC formalizes the transition from static compliance to dynamic, risk-informed decision-making.



Continuous, AI-powered cyber risk management

As laid out in its Fulcrum Strategy,[1] the DoW is aggressively pursuing advanced analytics, artificial intelligence (AI), and machine learning (ML) technologies for their potential to enhance systems that directly aid the warfighter. These same technologies form the backbone of CSRMC, enabling the DoW to deliver cyber-compliant, mission-ready systems in weeks rather than years. They help significantly shrink the gap between innovation and battlefield deployment without compromising security or operational reliability.

A key CSRMC component is to leverage AI throughout the system development lifecycle (SDLC) and not simply as part of a separate postdevelopment review.

In addition to RMF/CSRMC requirements, system security plans (SSPs), and plans of action and milestones (POA&Ms), AI agents can ingest leading knowledge bases from MITRE, the Open Worldwide Application Security Project (OWASP), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology (NIST) to quickly become expert at understanding a broad range of security standards and requirements, identifying cyber threats, and understanding attack tactics and techniques, as well as strategies for mitigating such risks.

Trained in existing RMF and security assessment bodies of knowledge, AI-powered solutions can help proactively identify and manage risks right from the start of development. The solutions can monitor data streams from continuous integration/continuous delivery (CI/CD) pipelines to examine and validate each software commit against known vulnerabilities, security controls, and other security standards and requirements. An AI-enabled assessment can examine vulnerability scan results and telemetry data to continuously correlate and score risks and examine software bills of materials (SBOMs) to immediately identify outdated libraries with known vulnerabilities. Through intelligent documentation and workflow automation, critical RMF artifacts such as SSPs and POA&Ms are kept accurate and current, reducing the administrative overhead associated with manual updates.

While traditional static code analysis tools excel at identifying known patterns and flagging potential vulnerabilities, AI elevates these capabilities by contextualizing and correlating findings in real time to deliver clear, customized remediation advice to developers. Additionally, as the AI continuously learns, it rapidly filters out false positives and prioritizes issues by severity so that the most critical concerns are addressed first during code reviews.

The CSRMC isn't just a framework; it's a mandate for transformation. Organizations that smartly embrace AI-powered cybersecurity and align with CSRMC principles will be best positioned to deliver resilient, secure capabilities at the speed of relevance.

[1] "Fulcrum: The Department of Defense Information Technology Advancement Strategy," June 20, 2024.

Illustrating the power of AI-powered RMF

The following use cases demonstrate how AI-powered risk management can be embedded across the system lifecycle to deliver measurable impact. Each use case highlights a distinct capability: anticipate threats before they reach production, quantify risk to guide investment, and continuously validate controls in production environments. Together, the use cases show how CSRMC principles can be realized at scale.

Use case 1: Cognitive risk management

Cognitive risk management is an approach that anticipates threats, adaptively scores risk, and analyzes changes before they hit production. It applies AI-driven simulation and orchestration to enhance situational awareness, automate risk assessments, and support continuous authorization across the CSRMC lifecycle. It improves human decision-making through explainable automation and integrates adversary simulations into governance workflows so that evolving threats are continuously evaluated and addressed.

When design or infrastructure changes occur, cognitive orchestration spans the full CSRMC lifecycle, from design through operations, by weaving adversary simulations into a broader governance framework. Automated agents detect code commits, SBOM updates, and configuration baseline shifts, then draft preliminary risk assessments mapped to NIST SP 800-53 controls. Rather than ending with red-team playbooks, each simulation becomes a risk input for artifacts including SSPs and POA&Ms. Human analysts remain central, reviewing AI-generated scenarios through an explainable, confidence-scored console that transparently conveys underlying assumptions and uncertainty.

Technically, the system parses infrastructure-as-code (IaC) definitions, asset inventories, and data flow diagrams to generate tailored test scenarios ranging from configuration checks to multistage attack chains, each accompanied by confidence scores and rationales. Human analysts vet and adjust these scenarios in a console before executing them against a digital twin kept in sync with production via continuous IaC reconciliation and telemetry-driven calibration tests. Simulation outcomes automatically update the SSP by adjusting control implementations and residual risk scores, while updating POA&Ms with prioritized remediation tasks based on mission impact. Every proposed change is subject to confidence thresholds and human approval.

The result: Attack chains are converted into actionable artifacts, with human oversight keeping automation fair, bounded, and mission-aligned.

CSRMC core principles: *Continuous monitoring and ATO, cybersecurity assessments, cyber survivability, automation, DevSecOps, and operationalization.*

Use case 2: Economic risk modeling

Economic risk modeling helps leaders invest in the most cost-effective risk reductions. It transforms cybersecurity from a compliance cost center into a strategic investment portfolio, enabling leaders to quantify and optimize risk reduction per dollar spent. By modeling breach probabilities and calculating return on security investment (ROSI), it empowers program managers to prioritize controls that deliver the greatest mission impact.

At its core is an integrated risk economics engine that ingests threat intelligence feeds, vulnerability scan results, asset inventories, business impact analyses, and mission essential functions. The engine employs modeling techniques to forecast breach probability distributions under different control portfolios. Each proposed control is evaluated for expected ROSI, supporting cost-benefit analyses tailored to DoW Fulcrum's resource-informed, risk-based agility. A live dashboard enables decision-makers to compare trade-offs such as tighter key rotation intervals versus deploying inline data loss prevention, and use dynamic sliders to optimize budgets, target risk levels, and generate prioritized control bundles for scaled agile framework (SAFe) planning interval (PI) planning; CSRMC onboarding and ATO decisions; and security orchestration, automation, and response (SOAR) workflows.

The result: Leadership gains real-time clarity on which security measures deliver the greatest risk reduction per dollar, aligning mitigation efforts directly with mission value and budget constraints.

CSRMC core principles: *Critical controls, automation, operationalization, and reciprocity.*

Use case 3: Continuous control monitoring

Continuous control monitoring evaluates what's already deployed and helps keep it compliant. It uses AI and policy-as-code to automate compliance, detect control drift, and maintain audit-ready documentation in real time. It ingests telemetry from across the enterprise, normalizes it into actionable insights, and orchestrates remediation workflows that replace static RMF processes with dynamic governance. Data is streamed from security information and event management (SIEM) systems, cloud security posture management (CSPM) technologies, endpoint detection and response (EDR) systems, identity and access management (IAM) solutions, and vulnerability scanners. These data streams are normalized and mapped to NIST SP 800-53 controls using policy-as-code, enabling automated detection of control drift such as expired certificates, disabled logging, or misconfigurations.

AI models analyze this telemetry to distinguish low-severity issues from high-risk failures. Minor deviations trigger automated remediation playbooks; critical findings generate change tickets prefilled with draft SSP updates and POA&M entries. These flow through existing approval workflows, preserving human oversight while accelerating response. Audit outcomes and remediation data feed back into the system to continuously improve detection and response.

The result: Outdated, static, manual RMF processes are replaced with a continuously governed control environment that automates compliance workflows, and keeps SSPs and POA&Ms audit-ready with minimal manual effort.

CSRMC core principles: *Continuous monitoring and ATO, automation, cybersecurity assessments, cyber survivability, operationalization, and enterprise services and inheritance.*

Making CSRMC a reality

While FISMA, OMB A-130, and NIST standards remain foundational to federal cybersecurity, the CSRMC signals a new era. NIST long emphasized automating controls "to the maximum extent feasible," but that guidance predated automation technologies such as AI and machine learning capable of ingesting threat intelligence, correlating telemetry, and generating risk artifacts in real time. The use cases explored earlier are not theoretical. They demonstrate how these technologies can reshape the way we assess, authorize, and secure systems. However, realizing CSRMC at scale will require more than technology. It demands a shift in mindset, policy, and practice. To make CSRMC a reality, we must confront a series of urgent and complex questions:

- **How do we retrofit legacy systems to support real-time monitoring and policy-as-code?** Can we modernize without rebuilding, or must we make hard choices about what to retire?
- **What telemetry is essential for continuous authorization, and how do we standardize it across platforms?** Without consistent, actionable data, continuous risk decisions are just theory.
- **What metrics will demonstrate CSRMC success, and who owns them?** If we can't measure resilience, how will we know we've improved it?
- **How do we scale pilots into enterprise-wide adoption without losing agility or fidelity?** Can we preserve innovation while building toward standardization?

The answers won't come from one office or one directive. They'll emerge from experimentation, collaboration, and a shared commitment to building systems that don't just comply but endure. Together, we can make CSRMC a transformative force rather than just another acronym.

How KPMG can help

As a leader and innovator in cyber risk management, AI, and advanced cybersecurity analytics, KPMG LLP is well positioned to help the DoW design and implement CSRMC initiatives. We can demonstrate how automation and AI can revolutionize traditional risk management practices, and help deliver a modern, re-envisioned approach that can overcome the limitations imposed by today's static, manual assessments.

While the potential benefits are immense, we also recognize the associated risks. Our approaches are designed to strike the right balance between pioneering innovation and pragmatic risk management. Working together, we can design and deploy AI capabilities to operationalize the CSRMC across its lifecycle phases, empowering our warfighters and maintaining advantage over our adversaries.

Why KPMG

KPMG is the number-one-ranked firm in the US for quality AI advice and implementation[2] and has been recognized by Forrester, IDC, and ALM Intelligence as a leading global organization of professional services for cybersecurity and cyber risk quantification (CRQ).[3, 4, 5, 6]

KPMG is the only major professional services firm to offer its own full-featured CRQ solution. It has been praised by industry analysts for its intuitive design and built-in guidance that supports both technical and nontechnical users, and for its model transparency, scenario scoping, comparative analysis and prioritization, and control performance monitoring capabilities.[7] Extensive benchmarks from our global services insights further accelerate its CRQ analyses.

Our proprietary portfolio of advanced, industry-tested AI solutions and accelerators, including KPMG Signals Repository, KPMG Modern Data Platform, KPMG Ignite, KPMG AI in Control, and KPMG AI Security, enables us to hit the ground running. And our strategic alliances with leading partners in data analytics, AI, and cybersecurity, including Microsoft, Databricks, Informatica, ServiceNow, Cranium, Panaseer, and Rhino.ai, give us access to resources and knowledge that can advance efforts to enable continuous risk scoring, support the implementation of continuous ATO, and accelerate the modernization of legacy systems.

We're a multidisciplinary organization working together as one team, with more than 15,000 technology and risk professionals worldwide, including AI specialists, data scientists, and business process analysts, and over 3,000 dedicated cybersecurity professionals. Our teams have the required clearances to get the job done securely and reliably.

KPMG has worked with the federal government for more than a century, including extensive experience working with military departments and other organizations at the DoW. We have provided ATO support to nearly every major DoW organization. We have a deep appreciation for the mission and a clear understanding that directing every resource as quickly as possible to the warfighter is paramount.

This deep understanding of DoW and federal operations, combined with our commercial experience and strategic technology vendor alliances, distinctly position us to help the DoW achieve its RMF reform and CSRMC objectives, and accelerate authorizations for today's advanced systems.

[2] "Perceptions of Consulting in the US in 2024," Source Global Research, March 2024.
[3] "The Cyber Risk Quantification Landscape, Q4 2022," Forrester Research.
[4] ALM Intelligence Pacesetter Research, April 2022.
[5] IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment (doc #US50463423), January 2024.
[6] "The Forrester Wave, Cyber Risk Quantification," Q2, 2025, Forrester Research.
[7] Ibid.

About KPMG

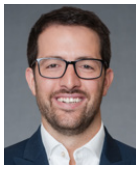
Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.

Contact us

Tyler A. Carlin
Federal Cyber & Tech Risk Offering Lead
KPMG LLP
240-306-5097
tcarlin@kpmg.com

Nate Deshong
Director, Advisory
KPMG LLP
720-219-5317
ndeshong@kpmg.com



Nick Larsen
Manager, Advisory
KPMG LLP
571-201-1174
nicholaslarsen@kpmg.com

read.kpmg.us/modgov