

The Cost of Manual RMF and FISMA Compliance Across the Federal Government

Market Research Analysis with TECTIX™ Automation Savings Projections

Executive Summary

This paper examines the federal cost of executing the Risk Management Framework (RMF) and Federal Information Security Modernization Act (FISMA) and the National Institute of Standards and Technology (NIST) Special Publication 800-53 compliance process. **Total annual federal spending on RMF compliance falls within a defensible range of \$5 billion to \$12 billion per year.** The largest cost driver is manual labor performed by federal employees and contractors producing security documentation, evidence, and continuous monitoring reports.

This analysis grounds its claimed automation savings in measured production data from the TECTIX™ platform developed by Markon. TECTIX automates the RMF package review process using 178 discrete validation checks. The platform was developed from lessons learned during Markon's support to the U.S. Army Materiel Command (AMC), where TECTIX reduced Authority to Operate (ATO) package review time from approximately two weeks to one day across 580 plus AMC systems (Markon, 2026).



When applied to the federal information system population, **TECTIX achievable savings range from approximately \$300 million per year at the conservative scaling to approximately \$1.5 billion per year** as planned artificial intelligence and machine learning features for artifact generation are deployed (Markon, 2026). These estimates are derived from measured per system savings rather than aspirational competitor claims.

Despite more than a decade of recognized need, federal RMF automation efforts have produced uneven results. The Department of Veterans Affairs became the first agency to submit a machine-readable System Security Plan using the Open Security Controls Assessment Language (OSCAL) in January 2025, nearly eight years after the National Institute of Standards and Technology launched their automation program. In May 2025, the Acting Department of War Chief Information Officer publicly characterized the current RMF and ATO processes as antiquated and announced an initiative to dismantle the existing process.

However, RMF itself cannot truly be dismantled because FISMA is codified in **44 U.S.C. § 3551** and statutorily requires federal agencies to develop, document, and implement information security programs protecting federal information and information systems, meaning any replacement framework must satisfy the same legal mandates. Therefore, the only durable path to materially reducing compliance cost, accelerating authorization timelines, and improving security outcomes is **intelligence process automation** and not process elimination.

1. Methodology and Scope

No single line item in the federal budget captures the cost of FISMA compliance. The Office of Management and Budget publishes an annual FISMA reports to Congress focused on security posture and incident reporting rather than aggregate spending. Agency budget submissions intermix operational defense, compliance activity, and information technology modernization in nontransparent ways. FISMA was enacted in 2002 and modernized in 2014 with the statutory goal of fostering risk-based policy for cost effective security under 44 U.S.C. § 3553. The inability to measure the program with precision is itself a structural limitation on assessing whether that statutory goal has been met.

This analysis estimated federal RMF compliance costs using a triangulated methodology across three independent analytical models.

The first is a top-down approach using published federal cybersecurity budget totals aggregated by the Office of Management and Budget and industry analysts (GovWin IQ, 2025).

The second is a bottom-up approach using per system Authorization to Operate (ATO) cost data multiplied by an estimated count of federal information systems operating under an active authorization.

The third is a historical ratio approach applying compliance to information technology spending benchmarks (Netsurion, 2023) to current federal information technology spending totals (U.S. Government Accountability Office, 2024).

Automation savings projections are grounded in measured production data from the TECTIX platform deployed at the U.S. Army Materiel Command, as reported in the platform technical demonstration (Markon, 2026).

The scope of this analysis is limited to federal information systems operating under direct agency Authorization to Operate decisions made by federal Authorizing Officials.

The **Federal Risk and Authorization Management Program (FedRAMP)** authorization process for commercial cloud service providers is excluded from this analysis because FedRAMP authorization costs are borne primarily by the vendor seeking authorization rather than by the federal government. While federal agencies do incur sponsorship and program office labor associated with FedRAMP

authorizations, those costs are a small fraction of the federal RMF compliance burden and warrant a separate analytical question.

Accordingly, the cost figures and savings projections in this paper apply to federal agency internal RMF processes including Department of War systems authorized through the Enterprise Mission Assurance Support Service (eMASS) and civilian agency systems authorized through agency specific governance, risk, and compliance (GRC) platforms.

2. Federal RMF Compliance Cost Analysis

Federal annual RMF compliance spending is estimated within a defensible range of \$5 billion to \$12 billion annually, based on three progressively broader cost models, summarized below.

The \$5 billion lower-bound estimate is derived using a bottom-up system cost methodology. The federal unclassified information system population is not publicly disclosed in aggregate but can be estimated at **approximately 20,000 to 25,000 ATO holding systems** based on the OMB IT Dashboard count of 6,700 civilian IT investments plus industry estimates of 8,000 to 12,000 Department of War unclassified systems tracked in eMASS.



All figures are annual recurring costs including federal civilian agencies and the Department of War.

Source: Government Accountability Office (GAO) FISMA Reporting (2019–2023); Agency budget justifications; Industry analysis.

Federal agency internal information systems vary in cost by FIPS Publication 199 impact level. High impact systems run \$400,000 to \$1,000,000 in initial ATO development costs. Moderate impact systems run \$100,000 to \$500,000 in initial cost (StackArmor, 2024). Low impact and inherited control systems run \$30,000 to \$100,000. Annual sustainment for continuous monitoring, control reassessment, and Plan of Action and Milestones (POA&M) maintenance runs \$60,000 to \$120,000 per system on average, with high impact systems running \$150,000 to \$300,000 per year (StackArmor, 2024). Blended annual cost per system, amortizing initial ATO over the three-year

reauthorization cycle and adding sustainment, is approximately \$150,000. Applied to 22,500 systems plus system attributable tooling and assessor costs, the figure is approximately \$5 billion per year.

The \$8 billion midpoint estimate adds the Continuous Monitoring and Mitigation program (approximately \$400 million federal appropriation plus \$1 billion to \$1.5 billion in agency side operations), independent assessment labor (\$400 million to \$600 million per year), and federal governance, risk, and compliance platform licensing totaling approximately \$300 million to \$500 million per year across **eMASS, Xacta, Archer, and ServiceNow GRC**.

The \$12 billion upper bound estimate adds embedded contractor compliance overhead on federal information technology services contracts, where system engineers and information system security officers spend an estimated 20 to 40 percent of their time on RMF artifacts (Cybersecurity and Infrastructure Security Agency, 2024). The U.S. Government Accountability Office (2025a) has documented similar findings on contractor compliance burden in federal information technology programs.

3. Cost Composition: Labor, Tooling, and Process Delay

The federal RMF process remains heavily manual. NIST itself observes that security controls and control baselines are represented in proprietary formats requiring data conversion and manual effort to describe their implementation, an explicit motivation for the OSCAL program (National Institute of Standards and Technology, 2023). The cost composition across the \$5 billion to \$12 billion range breaks down into three categories.

3.1 Federal Employee Labor

Federal employees performing RMF related work include system owners, Information System Security Officers (ISSOs), Information System Security Managers (ISSMs), Authorizing Officials, privacy officers, and mission program staff. The

Office of Personnel Management classifies most of these positions under the 2210 IT Management occupational series, which the federal government uses as the primary job series for information technology and cybersecurity professionals (Office of Personnel Management, 2018). DoW Instruction 8510.01 codifies the ISSM and ISSO roles within the federal RMF process. The total

The Cost Of Manual Compliance



18 to 24 months

AVERAGE DOW ATO TIMELINE



Up to 40%

OF CONTRACTOR TIME SPENT ON RMF PAPERWORK



Thousands

OF HAND-CREATED STIG CHECKLIST FILES PER AGENCY



18,500

GOV'T CYBER ROLES CUT IN 2025 RIFS AS COMPLIANCE BURDEN PERSISTS



Compliance labor

INVISIBLE IN CYBER BUDGET CROSSCUT

federal 2210 workforce historically exceeded 83,000 civilian positions (GovLoop, 2017), and as of 2026 the series has lost more than 18,500 employees during the 2025 federal workforce reductions (Friedman, 2026), leaving an estimated 60,000 to 65,000 positions across the 2210 series and related cybersecurity occupational series.

No federal workforce study has quantified the percentage of federal cybersecurity worker time spent specifically on FISMA and RMF compliance activities. Based on the operational responsibilities documented in DoW Instruction 8510.01 and the DHS ISSO Guide (Department of Homeland Security, 2013), this analysis estimates that approximately 20 to 30 percent of federal cybersecurity worker time is allocated to FISMA related compliance activity rather than operational defense, incident response, or engineering work. The General Schedule pay scale establishes federal employee base salaries, with a GS-13 Step 5 earning approximately \$138,000 to \$151,000 in 2026 depending on locality and a GS-14 Step 5 earning approximately \$163,000 in Washington, DC (FedTools, 2026). Applying the Defense Business Board fully burdened cost methodology (Defense Business Board, 2018), which includes salary, benefits, retirement, training, facilities, and overhead, produces an estimated fully loaded cost of approximately \$180,000 to \$220,000 per year for a blended GS-13 to GS-14 federal cybersecurity workforce.

Combining the estimated workforce size, time allocation, and fully loaded cost yields approximately \$2.4 billion to \$3.9 billion per year in federal employee labor on RMF and FISMA compliance activities. Much of this labor is charged to mission accounts rather than to cybersecurity accounts and is therefore invisible in the federal cybersecurity budget crosscut.

3.2 Contractor Labor and Pass Through Cost

Federal contractors perform a substantial portion of the actual RMF artifact production labor, particularly System Security Plan development, security control assessment evidence collection, POA&M maintenance, and continuous monitoring report generation. The federal government obligated approximately \$755 billion on contracts in fiscal year 2024 and \$793 billion in fiscal year 2025 (U.S. Government Accountability Office, 2025b, 2026). Of the broader federal information technology spend, approximately \$95 billion is reported on the OMB IT Dashboard across 26 civilian agencies and 6,700 IT investments, with an additional \$37 billion in Department of War unclassified national security systems, classified IT, and classified cyberspace spending (U.S. Government Accountability Office, 2024). The federal IT services contracting subset of these obligations is estimated at approximately \$60 billion per year, derived as the services portion of the approximately \$132 billion federal IT spend.

System engineers, ISSMs, ISSOs, and compliance specialists on federal IT services contracts perform a wide range of RMF related work. Industry sources describe the compliance documentation and tracking workload as substantial enough to consume the time of dedicated personnel even in small organizations, with mid-sized contractors typically requiring at least one ISSO per major system boundary (Quzara, 2026). No published federal study or industry survey quantifies the percentage of federal IT services contractor time spent specifically on RMF artifacts, but based on the operational

responsibilities documented in published ISSO and ISSM role guides and the eMASS package production workload described in agency documentation (SteelCloud, 2025), this analysis estimates that 20 to 40 percent of compliance specialist labor and 5 to 15 percent of system engineer labor on federal IT services contracts is allocated to RMF documentation, assessment, and continuous monitoring activities.

Applied to the estimated \$60 billion federal IT services contract obligation base, conservatively attributing \$3 billion to \$6 billion of this contractor labor specifically to RMF paperwork yields the largest single cost component of the federal RMF process. This component is invisible in the federal cybersecurity crosscut because it is billed under engineering or operations labor categories.

3.3 Tooling and Independent Assessor Costs

Federal GRC platform licensing and sustainment runs approximately \$300 million to \$500 million per year. The Department of War Enterprise Mission Assurance Support Service (eMASS) traditionally requires personnel to complete a Security Technical Implementation Guide Viewer Checklist for each policy on each endpoint, producing thousands of hand created checklist files (SteelCloud, 2025). The Continuous Diagnostics and Mitigation program represents another \$1.4 billion to \$1.9 billion when federal appropriation and agency side operations are combined. Independent assessor costs, including agency security control assessor labor and agency Inspector General FISMA evaluations across approximately 100 federal entities subject to FISMA, total \$400 million to \$600 million per year.

TECTIX Measured Results @ U.S. Army Materiel Command

**90%**REDUCTION IN ATO PACKAGE REVIEW
TIME**Two weeks to one day**

PER PACKAGE REVIEW

**178+**

AUTOMATED RMF CHECK ITEMS

**\$15,600**MEASURED SAVINGS PER SYSTEM PER
YEAR**580**

AMC SYSTEMS SUPPORTED

3.4 Timeline Cost

Traditional ATO timelines range from 6 months to over 2 years across federal agencies, with the Department of War average at 18 to 24 months (Second Front, 2026). Rise8 (2025) documents similar timeline data across federal agencies. The General Services Administration 18F group documented in 2018 that ATO processes had traditionally taken 6 to 18 months with substantial back and forth between system owners and assessors (Feldman, 2018). These timelines impose opportunity costs in deferred mission capability that the appropriated budget does not capture.

4. The AMC Case Study and TECTIX Measured Performance

This section grounds the automation savings projection in measured production data rather than vendor aspirational claims. Markon developed the TECTIX platform from lessons learned during RMF compliance services delivered to the U.S. Army Materiel Command. The AMC environment supports more than 580 individual information systems requiring active ATOs (Markon, 2026).

4.1 Pre Automation Baseline

Prior to TECTIX deployment, AMC ATO package reviews took approximately **two weeks of analyst labor per package**. The review was conducted as a hand check of multiple aspects of an eMASS package, including categorization records, control implementation statements, control assessments, POA&M entries, artifact attachments, and continuous monitoring data. With this manual process, AMC had difficulty securing ATOs across all 580 plus individual systems within required timelines (Markon, 2026). The pre automation baseline of approximately 80 labor hours per package review is consistent with broader federal observations on eMASS workload (SteelCloud, 2025).

4.2 Post Automation Results

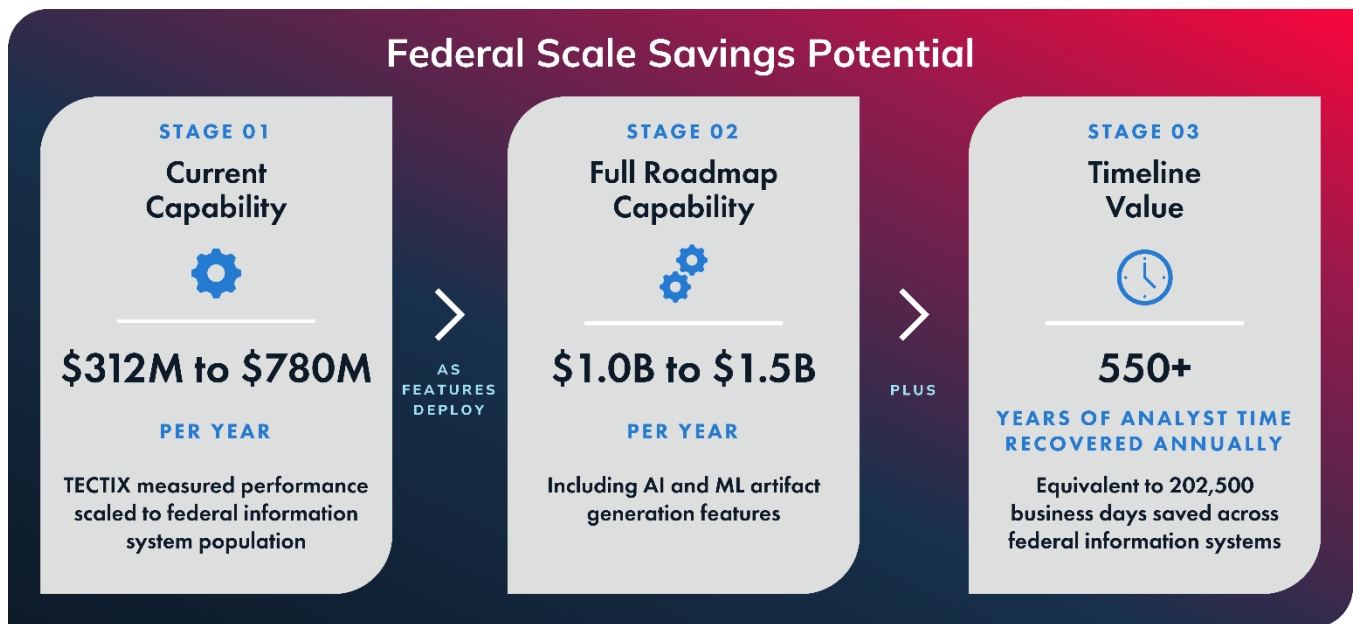
Markon translated the package review requirements into automated check logic. After developing and operationalizing the automated tool in AMC, package review time decreased from two weeks to one day, with strong packages completed in under one hour. This represents an approximate 90 percent reduction in ATO package review time, with 72 hours saved per package per review cycle distributed across ISSMs, authorizing officials, privacy officers, and system owners (Markon, 2026). Additional measured savings include approximately 1 hour saved per system on quarterly Security Technical Implementation Guide checklist updates, approximately 7 hours saved per month per team on POA&M entry tracking, and automated eMASS queries replacing manual continuous monitoring checks (Markon, 2026).

4.3 Measured AMC Annualized Savings

Markon reports a measured per system annualized savings of approximately \$15,600 at a \$100 per hour blended labor rate, yielding total annual savings of approximately \$546,000 at the 35-system test scale referenced in the platform demonstration (Markon, 2026). This figure encompasses ATO review and testing labor reduction, quarterly STIG checklist automation, POA&M entry tracking automation, and continuous monitoring query automation. The platform currently automates 178 plus individual check items spanning thousands of underlying controls, assets, POA&Ms, and artifacts.

5. Federal Scale Savings Projection

Scaling the measured AMC TECTIX performance to the federal information system population produces the savings range presented in this section. The projection uses the measured \$15,600 per system annualized savings figure (Markon, 2026) as the foundation, with adjustments for federal labor rate variation and TECTIX feature scope.



Grounded in measured TECTIX performance at U.S. Army Materiel Command

5.1 Current Capability Projection

At the measured AMC \$100 per hour blended labor rate, applied to the estimated 20,000 to 25,000 federal ATO holding systems, current TECTIX capability yields annual federal savings of approximately 312 million to \$390 million. Federal labor rates for contractor and federal employee compliance work are typically higher than the AMC benchmark used in the TECTIX demonstration. At a fully loaded federal blended rate of approximately \$200 per hour (which reflects realistic contractor billable rates plus federal employee fully loaded cost), the corresponding annual federal savings range increases to approximately \$624 million to \$780 million. These figures represent the addressable savings achievable from current TECTIX measured capabilities applied across the federal enterprise.

5.2 Roadmap Capability Projection

The TECTIX roadmap includes additional artificial intelligence and machine learning capabilities currently in development. Planned features include intelligent evidence mapping, automated POA&M generation, predictive ATO readiness scoring, smart document summarization, and assessor ready package generation (Markon, 2026). These planned features would extend TECTIX from a review

and check automation tool into a broader artifact generation platform. Commercial RMF automation vendors with similar artifact generation scope have demonstrated 80 percent or greater labor cost reductions in their target markets (RegScale, 2025). Applying a conservative expansion factor of approximately 2x to the measured AMC per system savings, reflecting the addition of artifact generation labor to the current review and check labor TECTIX already automates, yields a federal annual savings projection of approximately \$1.0 billion to \$1.5 billion per year when the planned artificial intelligence and machine learning features reach operational maturity across the federal information system population.

5.3 Timeline Value

Beyond direct labor savings, TECTIX delivers timeline reduction value. Applying the measured AMC 9 business day per package review savings to the federal information system population yields approximately 202,500 business days saved annually, equivalent to over 550 cumulative years of analyst review time. The opportunity cost reduction translates directly into faster mission capability delivery, which carries economic value that the appropriated federal budget does not capture but which has been recognized in cost benefit analyses by federal pilot programs including 18F (Feldman, 2018) and U.S. Air Force Platform One (Security Compass, 2025).

5.4 Summary Range

The defensible TECTIX federal savings range, grounded in measured AMC performance and the publicly documented platform roadmap, is approximately \$300 million to \$1.5 billion per year. This range is more conservative than the headline savings figures cited by broader scope commercial RMF automation vendors because it is grounded in measured per system performance rather than aspirational vendor claims. As planned artificial intelligence and machine learning features are deployed, the upper bound of this range becomes the realistic operational target. The TECTIX team has direct AMC measured performance data to substantiate the lower bound and clear development roadmap documentation to substantiate the upper bound.

6. Conclusion and Caveats

Federal annual spending on the manual RMF and NIST 800-53 FISMA compliance process is reasonably bounded at \$5 billion to \$12 billion per year. The largest single cost component is contractor labor on federal information technology services contracts. The second largest is federal employee labor charged primarily to mission accounts. The third largest is tooling and independent assessor costs. Application of the TECTIX automation platform could reduce this cost by \$300 million to \$1.5 billion per year based on measured performance at the U.S. Army Materiel Command and the documented platform roadmap, with corresponding ATO package review timeline reductions of approximately 90 percent.

Several caveats apply. The line between compliance spending and security spending is inherently blurry because tools such as Security Information and Event Management platforms serve both operational defense and continuous monitoring purposes. Department of War cybersecurity figures

are partially hidden from public reporting through the classified cybersecurity scorecard mechanism. Federal information system counts are reported inconsistently across agencies. The trajectory of federal cybersecurity spending is downward in the current budget cycle, with the fiscal year 2027 budget request continuing the contraction begun in fiscal year 2026 (Vijayan, 2026). The fiscal year 2026 budget began this trajectory the previous year (Vijayan, 2025). Federal automation efforts have produced uneven results over the past decade. The OSCAL saw its first agency adoption in 2025 after launching in 2017 (Department of Veterans Affairs, 2025). The Department of War publicly declared in May 2025 that the current RMF process is unfit for purpose and launched an initiative to dismantle it (Miller, 2025).

The substantial cost of the manual FISMA regime, the measured automation savings demonstrated at AMC, and the documented federal recognition that current processes are unsustainable together warrant continued executive attention to RMF automation as a focus area for both cost reduction and mission capability acceleration.

7. Bottom Line and a Call to Action

Compliance activities that slow mission delivery, strain an already depleted cyber workforce, and divert resources away from operational defense. At the same time, the current administration and Department of War leadership have publicly prioritized government efficiency, workforce optimization, artificial intelligence adoption, software modernization, and the reduction of bureaucratic barriers that delay capability delivery to the warfighter. TECTIX directly aligns to these priorities by automating labor intensive compliance processes, reducing ATO timelines by up to 90 percent, accelerating mission deployment, and enabling agencies to redirect scarce cybersecurity talent toward higher value operational outcomes instead of administrative paperwork. The modernization of RMF through intelligent automation is no longer simply a cybersecurity initiative. It is a government efficiency and mission readiness imperative.

7.1 The Strategic Choice

The federal government is approaching an inflection point in cybersecurity compliance. The current RMF and FISMA ecosystem was built for a slower era of technology deployment, yet today's mission environment demands rapid software delivery, continuous modernization, and resilient cyber operations at scale. The data presented in this analysis demonstrates that manual compliance processes are no longer sustainable from either a cost or mission effectiveness perspective.

Federal leaders now face a strategic choice. They can continue funding a labor-intensive compliance model that diverts billions of dollars away from mission capability, or they can aggressively modernize through automation platforms that reduce friction, accelerate ATO timelines, and improve security visibility simultaneously. Automation is no longer a future aspiration. Measured operational results at the U.S. Army Materiel Command demonstrate that meaningful reductions in labor hours,

review timelines, and administrative burden are already achievable today through platforms such as TECTIX.

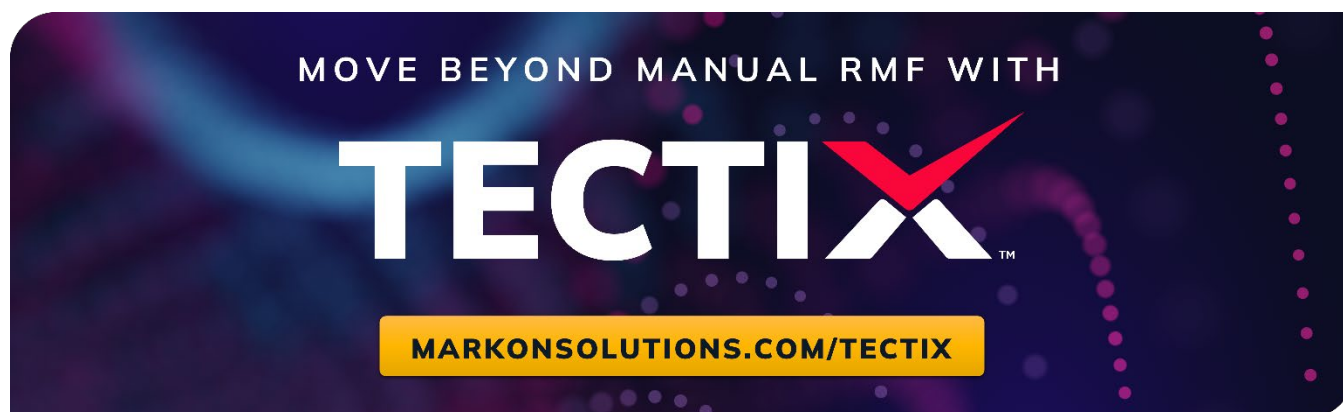
Administration and DoW Priority		TECTIX Capability
	Government Efficiency and Reduction of Bureaucratic Barriers	Automated RMF package review reduces analyst labor by 90%, freeing resources for higher value mission work
	Workforce Optimization Amid Cyber Workforce Reductions	178+ automated check items reduce manual ISSM and ISSO workload while preserving compliance quality
	Artificial Intelligence Adoption Across Federal Operations	AI and machine learning roadmap features deliver intelligent evidence mapping, predictive ATO readiness, and assessor ready package generation
	Software Modernization and Faster Capability Delivery	ATO package review reduced from two weeks to one day enables faster deployment cycles aligned with DevSecOps practices
	Mission Acceleration to the Warfighter	Continuous monitoring automation eliminates compliance bottlenecks slowing capability delivery to operational forces

7.2 Recommendations for Federal Leadership

For agency CIOs, CISOs, Authorizing Officials, and acquisition leaders, the recommendation is clear. Federal organizations should prioritize RMF automation initiatives as a strategic cost reduction and mission acceleration effort rather than solely a compliance exercise. They should shift cybersecurity personnel away from manual artifact production and toward operational defense, threat hunting, and engineering innovation. They should pilot automation capabilities within high volume ATO environments where measurable return on investment can be rapidly demonstrated. They should standardize machine readable compliance data and integrate automation directly into DevSecOps and continuous monitoring pipelines. They should invest in artificial intelligence enabled compliance tooling that reduces analyst workload while improving audit readiness and decision quality.

The federal government cannot eliminate its statutory FISMA obligations under 44 U.S.C. § 3551 et seq., but it can fundamentally transform how those obligations are executed. Agencies that modernize first will gain a significant operational advantage through faster deployment cycles, lower compliance overhead, and more efficient use of scarce cybersecurity talent. Agencies that fail to modernize risk becoming trapped in an increasingly expensive and administratively unsustainable compliance model. The path forward is not the elimination of RMF. The path forward is intelligent

automation, continuous assessment, and scalable compliance modernization that enables mission success at the speed demanded by modern national security operations.



About Markon

Markon is the leader in full-spectrum cyber, digital transformation, and critical intelligence solutions for national security. Our highly cleared workforce, hundreds of battle-tested experts, and industry-leading NSA-certified Red Teams and DoW red team operations strengthen secure, resilient mission readiness. Markon brings a fresh approach and deep dedication to what matters most: supporting our people and advancing our clients' missions. Markon is consistently recognized on USA Today's Top Workplaces USA, the Washington Post's Top Workplaces, as well as ENR's Top 50 Program Management Firms and Top 100 Professional Services Firms lists. Markon is also a five-time HIRE Vets Platinum Medallion Award recipient and a Virginia Values Veterans (V3) certified employer. Markon is a portfolio company of Sterling Investment Partners. Learn more at markonsolutions.com.

References

- Cybersecurity and Infrastructure Security Agency. (2024). *FY 2024 CIO FISMA metrics version 1.0*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-12/FY24_FISMA_CIO_Metrics_v1.0_FINAL_1.pdf
- Defense Business Board. (2018, February). *Fully burdened and lifecycle cost study* (FY18-01). U.S. Department of War. [https://dbb.defense.gov/Portals/35/Documents/Reports/2018/DBB%20FY18-01%20FBLCC%20Study%20Final%20\(Feb%202018\).pdf](https://dbb.defense.gov/Portals/35/Documents/Reports/2018/DBB%20FY18-01%20FBLCC%20Study%20Final%20(Feb%202018).pdf)
- Department of Homeland Security. (2013, September). *Information system security officer (ISSO) guide*. DHS. [https://www.dhs.gov/sites/default/files/publications/Information%20System%20Security%20Officer%20\(ISSO\)%20Guide.pdf](https://www.dhs.gov/sites/default/files/publications/Information%20System%20Security%20Officer%20(ISSO)%20Guide.pdf)
- Department of Veterans Affairs. (2025, January 21). *VA first federal agency to submit OSCAL system security plan ahead of White House deadline*. Digital VA. <https://digital.va.gov/security-excellence/va-first-to-submit-oscal-plan/>
- Feldman, A. (2018, July 19). *Taking the ATO process from 6 months to 30 days*. 18F, General Services Administration. https://web.archive.org/web/2024*/18f.gsa.gov/2018/07/19/taking-the-ato-process-from-6-months-to-30-days/
- FedTools. (2026, March 24). *GS pay scale 2026: Free salary lookup*. FedTools. <https://www.fedtools.com/resources/gs-pay-guide-2026>
- Friedman, D. (2026, April). *OPM adds cybersecurity jobs to Tech Force hiring program*. Federal News Network. <https://federalnewsnetwork.com/hiring-retention/2026/04/opm-adds-cybersecurity-jobs-to-tech-force-hiring-program/>
- GovLoop. (2017, August 18). *The murky numbers behind the federal government's cybersecurity force*. GovLoop. <https://www.govloop.com/the-murky-numbers-behind-the-federal-governments-cybersecurity-force/>
- GovWin IQ. (2025, September 18). *Defense FY 2026 IT and cyberspace activities budget highlights*. Delttek. <https://iq.govwin.com/neo/marketAnalysis/view/Defense-FY-2026-IT-and-Cyberspace-Activities-Budget-Highlights/8615>
- Markon. (2026, May 14). *TECTIX RMF Automation Demo*. Markon, LLC. Internal technical demonstration.
- Miller, J. (2025, May 9). *Arrington kicks off effort to eliminate RMF for DoD software*. Federal News Network. <https://federalnewsnetwork.com/defense-main/2025/05/arrington-kicks-off-effort-to-eliminate-rmf-for-dod-software/>
- National Institute of Standards and Technology. (2023). *More about OSCAL*. NIST. <https://pages.nist.gov/OSCAL/about/>

- Netsurion. (2023). *IT security: How much should you spend?* Netsurion.
<https://www.netsurion.com/articles/it-security-how-much-should-you-spend>
- Office of Personnel Management. (2018). *Interpretive guidance for cybersecurity positions*. OPM.
<https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf>
- Quzara. (2026, April 8). *ISSO vs ISSM: The definitive guide to information system security roles in federal compliance*. Quzara. <https://quzara.com/blog/isso-vs-issm-guide>
- RegScale. (2025, December 9). *Streamline RMF process and accelerate ATO for federal agencies*. RegScale. <https://regscale.com/knowledge-hub/rmf-ato-solutions/>
- Rise8. (2025). *How long does the ATO process take?* Rise8. <https://www.rise8.us/resources/how-long-does-the-ato-process-take>
- Second Front. (2026, March 16). *DoD Authority to Operate (ATO) explained*. Second Front.
<https://www.secondfront.com/resources/blog/dod-ato-explained/>
- Security Compass. (2025, April 3). *ATO vs. continuous ATO: Key differences explained*. Security Compass. <https://www.securitycompass.com/blog/ato-continuous-ato-differences-explained/>
- StackArmor. (2024, May 21). *How much does FedRAMP compliance cost?* StackArmor.
<https://stackarmor.com/how-much-does-fedramp-compliance-cost/>
- SteelCloud. (2025, August 25). *Outpacing the threat: Accelerate RMF and ATO readiness through automation*. SteelCloud. <https://www.steelcloud.com/the-urgency-of-action-rmf-and-ato-readiness-through-automation/>
- U.S. Government Accountability Office. (2024). *Information technology: Federal agencies are making progress in implementing GAO recommendations* (GAO-24-106693).
<https://www.gao.gov/products/gao-24-106693>
- U.S. Government Accountability Office. (2025a). *Cybersecurity: NASA needs to fully implement risk management* (GAO-25-108138). <https://files.gao.gov/reports/GAO-25-108138/index.html>
- U.S. Government Accountability Office. (2025b, June 24). *A snapshot of government-wide contracting for FY 2024*. <https://www.gao.gov/blog/snapshot-government-wide-contracting-fy-2024-interactive-dashboard>
- U.S. Government Accountability Office. (2026). *A snapshot of government-wide contracting for FY 2025*. <https://www.gao.gov/blog/snapshot-government-wide-contracting-fy-2025-interactive-dashboard>
- Vijayan, J. (2025, July 9). *Trump seeks unprecedented \$1.23 billion cut to federal cyber budget*. CSO Online. <https://www.csoonline.com/article/4019109/trump-seeks-unprecedented-1-23-billion-cut-to-federal-cyber-budget.html>
- Vijayan, J. (2026, April 10). *The cyber winners and losers in Trump's 2027 budget*. CSO Online. <https://www.csoonline.com/article/4156978/the-cyber-winners-and-losers-in-trumps-2027-budget.html>