Markon

EXECUTIVE BRIEF

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

Market Research Analysis with TECTIX™ Automation Savings Projections

Executive Summary

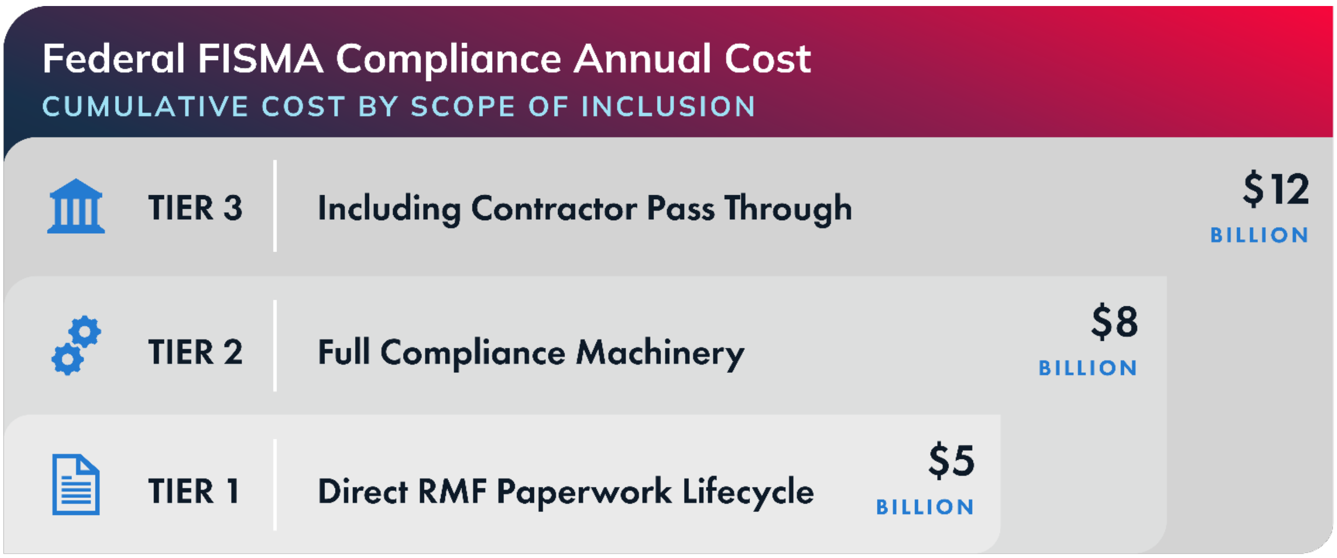
This paper examines the federal cost of executing the Risk Management Framework (RMF) and Federal Information Security Modernization Act (FISMA) and the National Institute of Standards and Technology (NIST) Special Publication 800-53 compliance process. **Total annual federal spending on RMF compliance 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 automation savings in measured production data from the TECTIX platform developed by Markon, a part of Markon LLC. TECTIX automates the RMF package review process using 178 discrete validation checks 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. **TECTIX achievable savings range from approximately $300 million per year at conservative scaling to approximately $1.5 billion per year** as planned artificial intelligence and machine learning features for artifact generation are deployed. 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 only became the first agency to submit a machine-readable System Security Plan using OSCAL in January 2025, nearly eight years after NIST launched the 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 them. 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, meaning any replacement framework must satisfy the same legal mandates. The only durable path to materially reducing compliance cost is **intelligent process automation** and not process elimination.

Federal Compliance Cost Landscape

No single line item in the federal budget captures the cost of FISMA compliance. This analysis estimated federal RMF compliance costs using a triangulated methodology across three independent models: a top-down budget approach (GovWin IQ, 2025); a bottom up per system ATO cost model; and a historical compliance to IT spending ratio approach (Netsurion, 2023; U.S. Government Accountability Office, 2024). The scope is limited to federal agency internal RMF processes, excluding FedRAMP, and includes Department of War systems authorized through eMASS and civilian agency systems authorized through agency specific GRC platforms.



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.

The **$5 billion lower bound** is derived from a bottom up system cost methodology applied to an estimated 20,000 to 25,000 federal ATO holding systems at a blended annual cost of approximately $150,000 per system, amortizing initial ATO development over the three year reauthorization cycle and adding continuous monitoring sustainment (StackArmor, 2024). The **$8 billion midpoint** adds the Continuous Diagnostics and Mitigation program, independent assessment labor, and federal GRC platform licensing across eMASS, Xacta, Archer, and ServiceNow GRC. The **$12 billion upper bound** adds embedded contractor compliance overhead on federal IT services contracts, where system engineers and ISSOs spend an estimated 20 to 40 percent of their time on RMF artifacts (CISA, 2024).

Federal employee labor accounts for approximately $2.4 billion to $3.9 billion per year, driven by an estimated 60,000 to 65,000 cybersecurity positions spending 20 to 30 percent of their time on FISMA compliance activity. **Contractor labor** is the largest single cost component at $3 billion to $6 billion per year, largely invisible in the cybersecurity crosscut because it is billed under engineering or operations labor categories. **Tooling and assessor costs** total approximately $2 billion to $3 billion per year. Traditional ATO timelines range from 6 months to over 2 years, with the DoW average at 18 to 24 months (Second Front, 2026), imposing opportunity costs in deferred mission capability.

The AMC Case Study and TECTIX Measured Performance

Markon developed the TECTIX platform from lessons learned during RMF compliance services delivered to the U.S. Army Materiel Command, which supports more than 580 individual information systems requiring active ATOs. Prior to TECTIX deployment, ATO package reviews took approximately **two weeks of analyst labor per package**, conducted as a hand check of categorization records, control implementation statements, assessments, POA&M entries, artifacts, and continuous monitoring data (SteelCloud, 2025).

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

Markon translated the package review requirements into automated check logic. Package review time decreased from two weeks to one day, with strong packages completed in under one hour, representing an approximate **90 percent reduction in ATO package review time.** Measured per system annualized savings are approximately **$15,600** at a $100 per hour blended labor rate, encompassing ATO review, quarterly STIG checklist automation, POA&M tracking automation, and continuous monitoring query automation.

Federal Scale Savings Projection

At the measured AMC $100 per hour blended labor rate applied to 20,000 to 25,000 federal ATO holding systems, current TECTIX capability yields annual savings of approximately $312 million to $390 million. At a fully loaded federal blended rate of approximately $200 per hour, savings increase to approximately $624 million to $780 million. The TECTIX roadmap includes AI/ML capabilities for intelligent evidence mapping, automated POA&M generation, predictive ATO readiness scoring, and assessor ready package generation. At operational maturity, projected annual savings increase to approximately $1.0 billion to 1.5 billion per year. Beyond labor savings, applying the measured AMC 9 business day per package savings federally yields approximately 202,500 business days saved annually, equivalent to over 550 cumulative years of analyst review time returned to mission execution.

Federal Scale Savings Potential

STAGE 01		STAGE 02		STAGE 03
Current Capability		**Full Roadmap Capability**		**Timeline Value**
$312M to $780M	AS FEATURES DEPLOY	**$1.0B to $1.5B**	PLUS	**550+**
PER YEAR		PER YEAR		YEARS OF ANALYST TIME RECOVERED ANNUALLY
TECTIX measured performance scaled to federal information system population		Including AI and ML artifact generation features		Equivalent to 202,500 business days saved across federal information systems

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

Strategic Alignment and Call to Action

The federal government is spending an estimated $5 billion to $12 billion annually on largely manual RMF and FISMA compliance activities that slow mission delivery, strain an already depleted cyber workforce, and divert resources away from operational defense. 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.

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

Federal leaders now face a strategic choice. They can continue funding a labor-intensive compliance model that diverts billions from mission capability, or they can modernize through automation platforms that reduce friction, accelerate ATO timelines, and improve security visibility simultaneously. 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. 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.