CYBERSECURITY

TYTO Athene

MODERNIZING FEDERAL CYBERSECURITY RISK MANAGEMENT

Executive Summary

While Government agencies have been facing escalating cybersecurity demands in terms of rapidly evolving threats, an increasing number of mandates, and growing oversight burdens, agencies are now also dealing with abrupt cuts to budgets and the workforce. In this context, an agency's ability to meet FISMA requirements, while effectively managing enterprise cyber risk, requires a pivot to well-integrated, automation-based solutions. stackArmor delivers a proven solution for cloud security, compliance automation, and risk management that accelerates compliance timelines, improves audit readiness, and strengthens governance.

Introduction

Through the first half of Fiscal Year 2025 (FY25), there have been substantial cuts to federal spending. The impacts vary from agency to agency, but on average federal workforce cuts are estimated to be in the range of 10-15%. Congress is still considering the passage of a new budget, but there appears to be a complementary impact on federal budgets. Furthermore, such reductions, which have been detailed in budget proposals, suggest a focus on trimming overhead and internal operational structures, likely because these functions are easily reorganized or automated compared to the frontline roles that maintain direct service delivery to citizens.

Challenges

The prioritization of spending on front-line, citizen-facing services reflects a mandate for agencies to achieve cost savings by streamlining internal support functions while attempting to sustain essential services for the public. Agencies face an exceedingly difficult challenge accomplishing such a pivot without eroding internal technical and security expertise, which could undermine long-term operational resilience. Agency CIOs and CISOs must address some long-standing, underlying challenges related to cybersecurity governance, risk, and compliance to succeed as they navigate this:

Compliance & Audit Complexity: FISMA requirements demand extensive documentation, coordination, and continuous tracking, and are subject to a slate of audits, which require proof these requirements are met.

Limited Risk Visibility: Siloed data and inconsistency in documentation hinders comprehensive and timely understanding of cybersecurity risk.

Proposed Solution

stackArmor has developed an integrated suite of tools with the express purpose of automating the business processes throughout the RMF lifecycle. It delivers the solution in the form of secure landing zones for all three of the major cloud service providers (CSPs). This forms the backbone of a hybrid cloud hosting environment that has the ability to integrate with and support on-premise IT infrastructure. Agencies benefit from the fact that the processes and procedures required to implement security requirements, such as regular vulnerability scanning and management, periodic log reviews, user account recertification procedures, and more, are automated through industry-leading IT tools. They've been designed and implemented to remove the non-value-added labor that is associated with conducting these activities and automatically captures the evidence needed to prove the activities are occurring. Demonstrable benefits agencies can gain from this approach include:

Faster Compliance

Reduce timelines as well as labor required for attaining ATOs.

Audit Readiness

Automatically generated compliance artifacts that streamline audit response.

Improved Risk Posture

Real-time insight enable informed decisions and faster remediation.

Scalability

Flexible for both enterprise-wide and project-specific initiatives.

Path Forward

Agencies must modernize their approach to meeting cybersecurity governance and risk management demands in order to accomplish the mandate to "do more with less." In doing so, agencies can achieve a long-lasting rebalancing of spending, thereby improving support for citizen-facing services without risking the long-term viability of those services. stackArmor's integrated solution automates the activities necessary to implement the NIST RMF and provides agencies with the tools and expertise needed to successfully achieve this outcome. Further, it's not a solution that has been developed in a rushed response to the budgetary climate that has emerged over the last few months. It has been developed over the course of nearly a decade and is positioned as a mature solution that's ready when agencies need it most.

ThreatAlert®

Case Study Snapshot

A federal agency accelerated its FedRAMP Moderate ATO by 50% using stackArmor's ThreatAlert® solution, gaining real-time compliance tracking and strengthening executive risk visibility.

FR 50%

Call to Action

stackArmor provides secure cloud, risk, and compliance solutions tailored to public sector needs. Trusted by federal agencies and cloud providers, stackArmor's team of automation, cloud, and security experts delivers proven success in cybersecurity governance, risk, and compliance automation for agencies at a time when it is needed most.

For more information about our cybersecurity services, please email bd@gotyto.com

https://gotyto.com

Tyto GSI is registered in System for Award Management (SAM) as a Large Business under NAICS Code 541519.

TYTO Athene

DATA TO DOMINANCE