WHITEPAPER

AI-Powered Cybersecurity 3-Part Series

Part 2: GRC Compliance Challenges, Best Practices, & Innovations

July 2026

Evolver

As cyberattacks against the U.S. federal government become more frequent and sophisticated, senior leaders increasingly expect cybersecurity programs to use automation and AI to demonstrate measurable risk reduction, operational resilience, and audit-ready evidence, rather than simple policy compliance. U.S. Federal guidance continues to emphasize performance-based cybersecurity, encourage the application of AI-powered defensive cyber operations (DCO) tools, and the need to accelerate the software cybersecurity testing authorization to operate (ATO) process, while independent oversight continues to report that many federal agency programs remain only partially effective on achieving their respective information security compliance.[1]

Governance, Risk, and Compliance (GRC) is the cybersecurity discipline that translates laws, policies, standards, and mission requirements into accountable decisions, repeatable processes, and defensible evidence. This whitepaper analyzes the most common cybersecurity Governance Risk & Compliance (GRC) implementation challenges in the U.S. Federal government agencies information system environments, outlines best practices, and offers technology innovations that scale, including Evolver's Integrated Technology Solution (EITS), "GUARDIAN," an automated and AI-powered risk-based vulnerability management tool.

What Is Cybersecurity Governance, Risk, & Compliance (GRC)?

Cybersecurity GRC is best understood as an operating model rather than a documentation exercise:

- *Governance* establishes leadership direction via strategy and policy documents, ensures accountability via processes, and defines decision rights for cybersecurity risk.
- *Risk management* identifies, qualifies, quantifies, and prioritizes cybersecurity risks while documenting risk acceptance decisions and continuously monitoring program effectiveness.
- *Compliance* implements and demonstrates adherence to required cybersecurity risk management frameworks (RMF) including ISO 27001, Department of War (DoW) CMMC 2.0, National Institute of Standards & Technology (NIST) - NIST SP 800-53, NIST SP 800-171, etc. and related information security controls and cybersecurity processes.

The NIST Cybersecurity Framework (CSF) 2.0 underscores that governance is a first-order cybersecurity function through its dedicated *Govern* function.[2] NISTIR 8286 similarly emphasizes integrating cybersecurity risk into enterprise risk management (ERM) so senior leaders can govern cybersecurity alongside other mission risks.[3]

In U.S. Federal cybersecurity, compliance is commonly operationalized through the NIST Risk Management Framework (RMF) and the NIST SP 800-53 control catalog. RMF embeds security and privacy across the system life cycle, while SP 800-53 provides the control language agencies implement and assess.[4]

Senior Leader Note: Effective cybersecurity GRC treats compliance evidence as the output of operational processes. If evidence is produced manually and periodically, it will be late and often inaccurate.

The U.S. Federal Cybersecurity GRC Operating Model: RMF, Continuous Monitoring, & Evidence

The RMF provides a structured process (Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor) for making consistent, repeatable authorization decisions. The Monitor step ultimately determines whether GRC scales or becomes a perpetual backlog.[5] The "Monitor" step is where GRC either scales or becomes a perpetual backlog.

NIST defines information security continuous monitoring (ISCM) as maintaining ongoing awareness of security posture, vulnerabilities, and threats to support risk

decisions.[6] In practical terms, continuous monitoring requires (1) reliable telemetry from security tooling, (2) normalization/correlation so results are decision-quality, and (3) governance workflows that convert findings into verified remediation and updated evidence.

U.S. Federal compliance is also moving toward machine-readable evidence. OSCAL provides standardized, machine-readable representations of System Security Plans (SSPs), cyber vulnerability scans, Security Assessment Report (SAR) results, and Plan of Action & Milestones (POA&Ms) reports, reducing manual friction and enabling automation.[7] FedRAMP modernization reinforces this direction, emphasizing scale and reuse while moving toward machine-readable packages and deterministic telemetry.[8]

U.S. Federal Government Cybersecurity GRC Implementation Challenges

1) Fragmented telemetry and inconsistent IT asset inventories undermine executive visibility into cybersecurity risks

Distributed federal environments often maintain multiple, conflicting sources of truth for IT assets and vulnerabilities. The result is duplicate findings, inconsistent severity ratings, and incomplete visibility into system boundaries.

2) Manual Cybersecurity evidence cannot keep pace with hybrid multi-cloud change velocity

When SSPs, SARs, and POA&Ms are maintained manually, compliance evidence quickly falls behind operational reality. As FedRAMP and government agencies move toward automation and machine-readable packages, document-centric compliance becomes increasingly mismatched to cloud delivery and continuous authorization expectations.[9]

3) Cyber vulnerability overload and severity-only triage misallocate remediation effort

Traditional cyber risk severity scoring alone does not reflect cyber exploitation likelihood or mission impact. U.S. Federal cybersecurity policy increasingly requires exploitation-aware prioritization: BOD 22-01 mandates remediation of vulnerabilities in the Known Exploited Vulnerabilities (KEV) catalog by due dates, and EPSS provides an additional predictive signal for exploitation likelihood.[10]

4) POA&Ms become backlogs when they are not tied to accountable cybersecurity remediation workflows

POA&Ms are intended to be corrective action plans that track weaknesses, milestones, and completion dates.[11] Without integration to trouble ticketing, change management, and verification of closure, POA&Ms will contribute to persistent negative findings and ineffective cybersecurity programs noted by U.S. government oversight bodies.[12]

5) Shared responsibility and cybersecurity supply chain risk expand the governance surface area

Cloud adoption and contractor-heavy delivery models distribute control ownership across agencies, providers, and integrators. At the same time, software supply chain dependencies require explicit cybersecurity supply chain risk management (C-SCRM) that is integrated into enterprise risk governance, not treated as a one-time vendor assessment.[13]

6) AI and quantum change the evidence and control-validation problem

AI adoption and post-quantum cryptography (PQC) migration will introduce new control requirements, new inventories, and new forms of evidence. OMB's PQC memo directs agencies to inventory quantum-vulnerable cryptography and plan migration, while NIST's PQC standards provide concrete implementation targets.[14] NIST's AI RMF provides a framework for managing AI risks that agencies can adapt for both mission AI and AI-enabled cybersecurity operations.[15]

Best Practices for U.S. Federal Government Cybersecurity GRC Programs

1) Govern cybersecurity risk as enterprise risk with decision-grade reporting

Use Enterprise Risk Management (ERM)-aligned constructs (e.g., risk registers, risk owners, and time-bound

decisions) so senior leaders can govern cybersecurity alongside other mission risks. [16]

2) Establish authoritative IT asset inventories and system boundaries as prerequisites for cybersecurity continuous monitoring

Cybersecurity continuous monitoring depends on knowing what is in scope. Mature programs enforce authoritative inventories, consistent identifiers across tools, and validated system boundaries to reduce blind spots and duplicate work.[17]

3) Engineer cybersecurity compliance evidence as a pipeline (OSCAL where feasible)

Treat cybersecurity risk management framework artifacts as outputs of operational telemetry and workflow. Adopt OSCAL-aligned artifacts where feasible to enable automation, versioning, and reuse.[18]

4) Prioritize cybersecurity risk remediation using exploitation signals plus mission context

Implement cybersecurity risk mitigation prioritization policies that fuse KEV deadlines, EPSS likelihood, asset criticality, and control impact to create a defensible remediation backlog aligned to real threat behavior.[19]

5) Make Cybersecurity POA&M governance closed loop with accountable owners and verified closure

Integrate cybersecurity POA&M items with operational tickets, change control, and closure validation so POA&Ms function as corrective action controls rather than static backlogs.[20]

6) Build crypto-agility and AI governance now (inventory, policy, and evidence)

Begin PQC inventory and migration planning per OMB direction and align AI adoption with trustworthy AI principles, so governance mechanisms can absorb rapid changes in cryptography and AI-enabled operations. [21]

Common Tooling for U.S. Federal Government Cybersecurity GRC

U.S. Federal GRC programs typically rely on an ecosystem of tools that includes GRC platforms, asset management systems, vulnerability scanners, threat intelligence feeds, and ITSM workflows. The challenge is rarely a lack of tools, but a matter of integrating them into a unified governance process

As agencies move toward machine-readable evidence and continuous authorization to operate (C-ATO), toolchains must support (a) risk-based prioritization that fuses threat intelligence and mission context and (b) evidence export aligned to RMF artifacts, ideally in machine-readable formats such as OSCAL.[22]

Evolver GUARDIAN: From Findings to Fixes at the Speed of Federal Compliance

Evolver GUARDIAN addresses one of the most common GRC challenges in federal environments: fragmented vulnerability management that leads to inconsistent risk scoring, unclear ownership, slow remediation, and growing POA&M backlogs.[23]

GUARDIAN integrates Evolver Federal's GRC/RMF services with Nucleus Security's FedRAMP Moderate authorized vulnerability and exposure management platform.[24] The integrated capability is designed to deliver closed-loop, risk-based vulnerability governance that directly supports RMF evidence obligations:

- *Unify:* Ingest and normalize cyber vulnerability exposure (CVE) data from 160+ scanners and tools to create a single exposure source of record.[25]
- *Prioritize:* Fuse exploitation intelligence (KEV), predictive signals (EPSS), asset criticality, and control impact to rank what matters first.[26]
- *Execute:* Automate cybersecurity remediation workflows via ownership assignment, SLA dashboards, and ticketing/Information Technology Service Management (ITSM) integration.

- *Prove:* Export cybersecurity remediation status and evidence into RMF artifacts (POA&Ms and OSCAL-aligned documentation), accelerating ATO sustainment and audit readiness.[27]

Because U.S. federal government information system environments are distributed, GUARDIAN also supports multi-tenancy and role-based access controls (RBAC) to segment data by program or enclave while maintaining enterprise rollups—an essential feature for governing mission portfolios.[28]

Customer Benefits: GUARDIAN operationalizes a measurable control system for cybersecurity vulnerability risk, connecting cybersecurity exploitation-aware prioritization to accountable cybersecurity remediation and continuously updated RMF evidence.

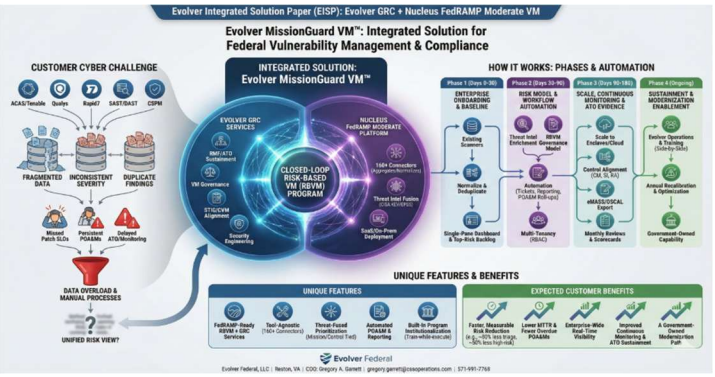

Figure 1. Evolver GUARDIAN™ integrated solution model supporting closed-loop, risk-based vulnerability governance and RMF evidence export.

A Practical Evolver GUARDIAN Adoption Roadmap

A typical Evolver GUARDIAN adoption approach phases capability delivery to produce measurable outcomes quickly while scaling to enterprise sustainment.[29]

Phase	Primary Outcomes
Phase 1 (0–30 days)	Connect key data sources, normalize and de-duplicate findings, establish ownership, and baseline risk posture.
Phase 2 (30–90 days)	Operationalize threat-informed prioritization (KEV/EPSS) and automate workflow integration (ticketing/SLAs/POA&M rollups).
Phase 3 (90–180 days)	Scale across enclaves and systems; mature evidence export aligned to RMF artifacts and continuous monitoring reporting.
Phase 4 (180+ days)	Institutionalized sustainment: training, quality control, metric governance, and continuous improvement.

The Future of U.S. Federal Government Cybersecurity GRC: AI, Quantum, and Continuous Compliance Engineering

Over the next several years, we expect the U.S. Federal government cybersecurity GRC will continue shifting toward continuous assurance: machine-readable evidence, automated control validation, and risk reporting derived from operational telemetry. FedRAMP modernization and requests for comment on machine-readable packages reinforce that authorization artifacts and supporting telemetry will increasingly be delivered in formats suitable for automation.[30]

AI and quantum will accelerate this shift. AI can augment triage, evidence extraction, and control cybersecurity monitoring, but it introduces governance requirements captured in NIST's AI RMF. [31] Quantum-driven cryptographic modernization will require automated inventories, migration planning, and new evidence artifacts as agencies implement PQC standards.[32]

GUARDIAN is positioned for this evolution because it is built around normalized telemetry, policy-driven prioritization, workflow automation, and evidence export. These are the same primitives required for both compliance engineering (OSCAL and machine-readable packages) and trustworthy AI-enabled automation without turning GRC into an unsustainable manual process.

Conclusion

U.S. federal agencies need cybersecurity GRC programs that produce decision-quality risk visibility and audit-ready evidence at the speed of modern operations. GUARDIAN delivers that capability by unifying exposure data, prioritizing remediation based on real-world risk, enforcing accountable workflows, and continuously generating RMF evidence.

About the Authors

Gregory A. Garrett is the Chief Operating Officer and Chief Innovation Officer for Evolver. He leads all of Evolver's technology thought leadership and technology business units, which provide advanced IT, AI, cybersecurity, electronic security, and eDiscovery services to federal agencies and Fortune 500 companies.

With over 25 years of executive experience and a background as a CIO, CTO, CISO, and COO, he has managed more than $40 billion in global tech contracts and served in key roles across both large and mid-sized firms. A retired U.S. Air Force Colonel and accomplished author, Garrett has also contributed extensively to industry thought leadership through 24 books, more than 150 articles, expert testimony, and over 250 speaking engagements.

Nidhi Panchasara specializes in AI strategy, human-centered design, and cybersecurity integration. She advises government and commercial clients on deploying responsible AI in operational environments. She brings over 25 years of experience in IT leadership, cybersecurity operations, and program management, with prior senior roles at NTT DATA, Huntington Ingalls Industries, TurningPoint Global Solutions, and Computer Sciences Corporation.

Dr. Brian McElyea is an accomplished cybersecurity executive recognized for leading large-scale digital transformation initiatives and building high-performing Cyber Centers of Excellence that drive mission-aligned security outcomes. With over two decades of leadership across healthcare, defense, and federal sectors, he has guided global organizations through the complexities of risk management, compliance, and modernization with measurable results.

Works Cited

Office of Management and Budget. *M-25-04: Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*. 15 Jan. 2025, https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf. Accessed 8 Mar. 2026.[1]

GAO. *CYBERSECURITY: Federal Agencies' Implementation of FISMA Continued to Be Mostly Ineffective*. GAO-24-106291, Jan. 2024, https://www.gao.gov/assets/gao-24-106291.pdf. Accessed 8 Mar. 2026. [1, 12]

National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. Feb. 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Accessed 8 Mar. 2026. [2]

National Institute of Standards and Technology. *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. NISTIR 8286, Oct. 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf. Accessed 8 Mar. 2026. [3, 16]

National Institute of Standards and Technology. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST SP 800-37 Rev. 2, Dec. 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. Accessed 8 Mar. 2026. [4, 5]

National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53 Rev. 5, Sept. 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Accessed 8 Mar. 2026. [4]

National Institute of Standards and Technology. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST SP 800-137, Sept. 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf. Accessed 8 Mar. 2026. [6, 17]

National Institute of Standards and Technology. *OSCAL (Open Security Controls Assessment Language)*. NIST, n.d., https://pages.nist.gov/OSCAL/. Accessed 8 Mar. 2026. [7, 9, 18, 22, 27]

Office of Management and Budget. *M-24-15: Modernizing the Federal Risk and Authorization Management Program*. 25 July 2024, https://www.whitehouse.gov/wp-content/uploads/2024/07/M-24-15.pdf. Accessed 8 Mar. 2026. [8, 13, 30]

FedRAMP. *RFC-0024: FedRAMP Rev 5 Machine-Readable Packages*. 13 Jan. 2026, https://www.fedramp.gov/2026-01-13-rfc-0024/. Accessed 8 Mar. 2026. [8, 9, 30]

CISA. *BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities*. 3 Nov. 2021, https://www.cisa.gov/news events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities. Accessed 8 Mar. 2026. [10]

CISA. *Known Exploited Vulnerabilities Catalog*. Cybersecurity and Infrastructure Security Agency, n.d., https://www.cisa.gov/known-exploited-vulnerabilities-catalog. Accessed 8 Mar. 2026. [10, 19, 26]

FIRST. *Exploit Prediction Scoring System (EPSS)*. Forum of Incident Response and Security Teams, n.d., https://www.first.org/epss/. Accessed 8 Mar. 2026. [10, 19, 26]

FedRAMP. *Plan of Action and Milestones (POA&M)*. FedRAMP.gov, n.d., https://fedramp.gov/docs/rev5/playbook/csp/authorization/poam/. Accessed 8 Mar. 2026. [11, 20]

National Institute of Standards and Technology. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST SP 800-161 Rev. 1, May 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf. Accessed 8 Mar. 2026. [13]

Office of Management and Budget. *M-23-02: Migrating to Post-Quantum Cryptography*. 18 Nov. 2022, https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-Migrating-to-Post-Quantum-Cryptography.pdf. Accessed 8 Mar. 2026. [14, 21, 32]

National Institute of Standards and Technology. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*. 13 Aug. 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf. Accessed 8 Mar. 2026. [14, 32]

National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1, Jan. 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. Accessed 8 Mar. 2026. [15, 21, 31]

Evolver. *Evolver Integrated Solution Paper (EISP): Evolver GRC + Nucleus FedRAMP Moderate Vulnerability Management (Evolver GUARDIAN)*, https://evolverinc.com/wp-content/uploads/2026/03/030326_Evolver_EITS_Guardian-1.pdf. Internal solution paper, n.d. [23, 24, 26, 27, 28, 29]

AWS Marketplace. *Nucleus for Government Enterprise Vulnerability Management Platform*. Amazon Web Services, n.d., https://aws.amazon.com/marketplace/pp/prodview-he2m4vylpu24a. Accessed 8 Mar. 2026. [24, 25]

CISA. *Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools*. 26 Sept. 2024, https://www.cisa.gov/sites/default/files/2024-09/Strategy%20for%20Migrating%20to%20Automated%20Post-Quantum%20Cryptography%20Discovery%20and%20Inventory%20Tools.pdf. Accessed 8 Mar. 2026. [32]