EXECUTIVE GUIDE | CYBERSECURITY GOVERNANCE

Closing Recurring Cybersecurity Findings

A governance and remediation operating model for turning audit findings into durable control assurance.

A finding is not closed when the task is complete. It is closed when evidence proves the control works - and monitoring keeps it working.

Why this matters now

The Department of Veterans Affairs Office of Inspector General's fiscal year 2025 FISMA audit, issued July 27, 2026, reported continuing deficiencies involving access controls, configuration management, security management, and service continuity. The audit made 19 recommendations; some addressed deficiencies repeated over multiple years, while six earlier recommendations were closed due to improvements. The signal is broader than one agency: recurring findings are often an operating-model problem as much as a technical one.

VALLEN CONSULTING GROUP | AUGUST 2026

The Finding-to-Assurance Operating Model

Durable remediation connects accountability, root-cause correction, delivery discipline, independent testing, and continuous monitoring. Each component must operate as part of one evidence chain.

1. Accountable control ownership

Assign one executive risk owner and one operational control owner, with decision rights and escalation defined.

2. Risk-based triage

Prioritize by mission impact, exploitability, exposure, dependency, recurrence, and regulatory consequence.

3. Root-cause and control design

Diagnose why the control failed; redesign policy, process, technology, data, skills, or vendor obligations.

4. Integrated remediation delivery

Manage corrective actions as a governed portfolio with milestones, dependencies, resources, and blockers.

5. Independent validation

Require objective testing, traceable evidence, and explicit residual-risk disposition before closure.

6. Continuous monitoring

Track whether controls remain effective and trigger reassessment when the environment or risk changes.

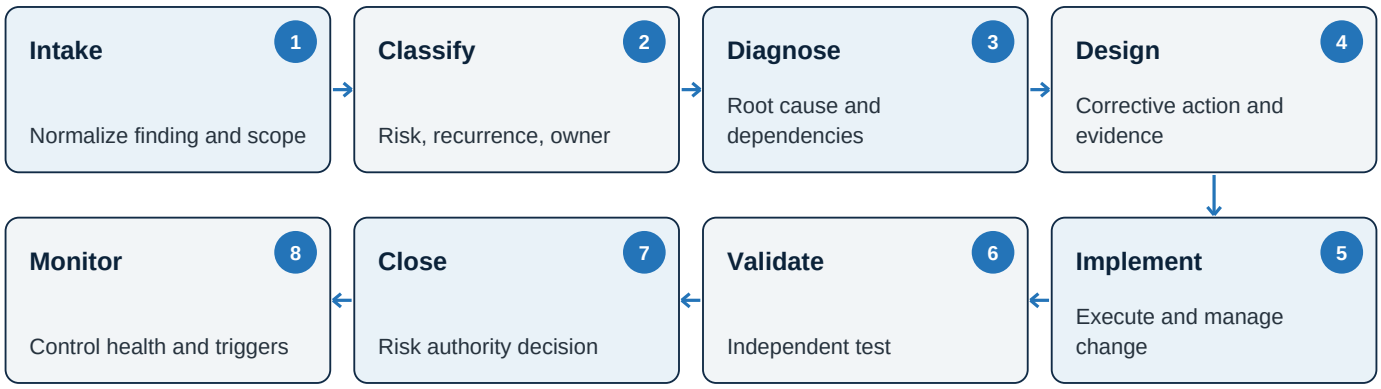
Recurring findings usually persist where ownership is diffuse, actions treat symptoms, evidence is assembled late, or closure is disconnected from monitoring.

Closure standard

+ The control requirement and affected assets are explicitly mapped.
+ Root cause is documented and the corrective action addresses it.
+ Implementation evidence is complete, current, and traceable.
+ Independent testing confirms the control operates as intended.
+ Residual risk is accepted by the appropriate authority.
+ A monitoring trigger detects degradation or recurrence after closure.

A closed-loop remediation process

Move from audit intake to sustained assurance through eight governed stages.



Sequence follows the numbered path. Each stage ends with a decision gate, evidence check, and named owner.

Governance layers

Layer	Primary job	Cadence and evidence
Executive risk committee	Set risk tolerance; resolve high-impact decisions; accept residual risk	Monthly; severity, aging, recurrence, blocked decisions, mission exposure
Remediation office	Integrate the portfolio; enforce standards; manage dependencies and escalation	Weekly; action plan, milestones, owners, blockers, evidence completeness
Control owners	Correct the control and keep it operating	Working cadence; control design, implementation proof, operating metrics
Independent assurance	Test effectiveness and challenge closure evidence	At validation gates; test plan, samples, results, exceptions, retest

Three non-negotiable separations

+ The person implementing a corrective action should not be the sole authority validating it.
+ The team declaring completion should not silently accept residual risk.
+ The register tracking open items should not be the only evidence that a control works.

A 90-day stand-up plan

Period	Focus	Core outputs
Days 0-30	Reconcile and assign	Canonical finding inventory; severity and recurrence taxonomy; accountable owners; governance charter
Days 31-60	Diagnose and plan	Root-cause analyses; corrective-action plans; evidence standards; integrated dependency roadmap
Days 61-90	Test and institutionalize	Priority validations; closure decisions; executive dashboard; monitoring triggers; lessons backlog

Executive remediation dashboard

Exposure

Open findings by severity, mission impact, system, and control family

Aging

Time open, time beyond target, and blocked-decision days

Recurrence

Repeat-finding rate and findings reopened after closure

Delivery

Milestone performance, dependencies, and corrective actions at risk

Evidence quality

Percent complete, first-pass validation rate, and retest volume

Control health

Post-closure performance, monitoring exceptions, and degradation triggers

Move from finding management to durable control assurance.

Vallen Consulting Group supports governance design, PMO and remediation-office stand-up, operating-model design, program recovery, executive reporting, and performance measurement. Visit vallenconsultinggroup.com.

Sources and use note

1. VA Office of Inspector General - Federal Information Security Modernization Act Audit for Fiscal Year 2025, Report 25-01698-70, July 27, 2026.

2. NIST Special Publication 800-37 Revision 2 - Risk Management Framework and the NIST RMF Monitor Step.

This Vallen framework is an advisory governance model. It does not replace agency policy, system-specific authorization requirements, audit standards, legal advice, or applicable cybersecurity obligations.