THE COST OF WAITING:
How Delays in STIG Compliance Multiply Risk

Adversaries never stop trying to access your system. Every moment of delay means your systems move further from approved configurations; your audit documentation becomes outdated, and your ATO grows harder to maintain.

Compliance can't wait. Automation keeps it moving.

The Ripple Effect of Delayed STIG Compliance

0–2 Weeks | CONFIGURATION DRIFT BEGINS

- Baselines begin to stray from DISA standard with the day-to-day operations.
- Manual teams scramble to identify which controls have changed and what to apply to which systems.

3-6 Weeks | REMEDIATION BACKLOG GROWS

- Unapplied STIGs create open findings in SCAP scans.
- POA&Ms lengthen as exceptions stack up.
- ATO extensions face rejection due to stale evidence.

6+ Weeks | Mission Impact

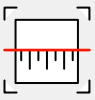
- Systems fall out of alignment with current DISA requirements.
- Time and cost to regain compliance double, often delaying deployment or sustainment schedules.

With over 10,000 STIG controls across DoD environments, failing to apply STIGs with automation compounds effort exponentially.

Manual STIG Process	Automated STIG Process (SteelCloud ConfigOS)
Requires hand-editing XML checklists and running separate SCAP scans	Scans, remediates, and validates controls automatically across environments
Hours spent verifying hundreds of settings per system	90 % reduction in effort per STIG application cycle
Results vary by technician and environment	Standardized, repeatable baselines
Delays trigger recurring POA&M items	Continuous evidence collection keeps POA&Ms short
Audit prep measured in weeks	Audit readiness maintained daily

The Real Cost of Falling Behind

Missed quarterly updates: Every 90-day cycle skipped adds hundreds of controls to the next workload.



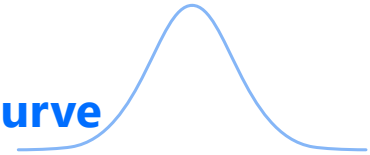
Failed validation scans: Out-of-date benchmarks produce false negatives and extra remediation hours.

Stalled accreditation: Delays in applying STIGs directly impact RMF Step 6 (Authorize System Operation).

Staff burnout: Manual review of DISA XML files and checklists consumes valuable IA resources.

Teams that automate STIG remediation recover faster, maintain stronger audit trails, and avoid compounding backlog.

Automation Reverses the Curve



Automation turns the quarterly scramble into a sustainable cycle.

SteelCloud's ConfigOS continuously applies, verifies, and documents STIG controls, keeping systems compliant with each new DISA release.

- ✓ Updates implemented in hours, not weeks
- ✓ Continuous ATO readiness through automated evidence generation
- ✓ Proven success across classified and unclassified DoD environments

Automation keeps your systems aligned, your documentation current, and your mission moving.

Compliance doesn't pause. Neither do we.