SteelCloud

Synchronizing Cyber Compliance Between IT and A&A Organizations

Cracking the Compliance Code with Unified Content & Automation

March 2024

Organizations place a lot of emphasis on streamlining the RMF process to support continuing ATOs. It's a noble pursuit. However, it impacts an organization's ability to properly implement approved controls into the production environment as they were selected/approved in the RMF process. This challenge is exacerbated by the fact that assessment artifacts provided by scanning tools rarely match the controls approved in the RMF/ATO process. Most notably, checklists created by this process are inaccurate and require a significant amount of manual re-work. The resulting lack of synchronization is caused by an inherent flaw in the traditional way that RMF data is approved, implemented, and assessed.

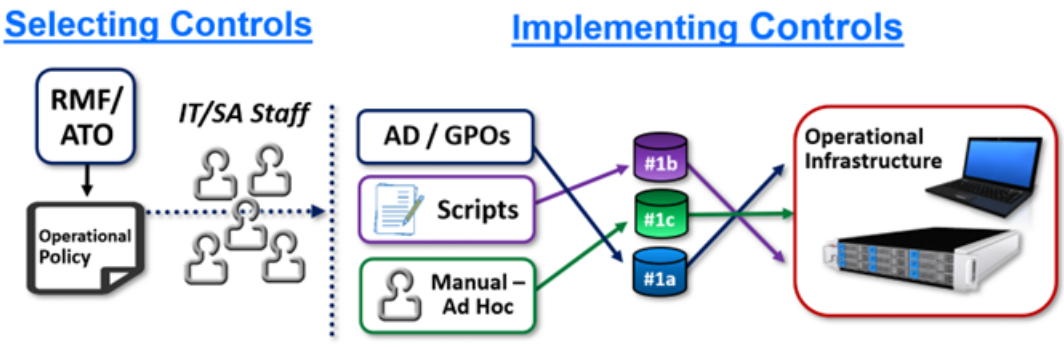
Traditional methods of cyber compliance automation rely on multiple processes and multiple technologies from multiple vendors, which effectively isolate the processes for:

- ✓Selecting controls
- ✓ Implementing controls
- ✓Maintaining controls
- ✓ Assessing controls

It is easy to recognize the ongoing challenge of achieving a singular result when using multiple processes/systems with differing content to achieve that result. The challenge is magnified supersized when you consider the compliance challenges encountered throughout an application's entire development to production lifecycle. Traditional means of assessment and authorization are not compatible with the efficient, accurate and streamlined compliance process organizations want to pursue.

Identifying the Cyber Compliance Operations Flaw

Traditionally, a control specification is created as part of the RMF/ATO process. Selecting controls involves the arduous task of hardening all of the appropriate system-level controls (i.e., STIGs) around an app stack. This task is usually done manually by seasoned IT staff, taking weeks or months. The output of that hardening process is then approved for release into production as part of the RMF/ATO process. An approved operational policy document details all of the approved control values and any deviations required and identified in the hardening process. This document is supplied to the IT/Sys Admin staff to implement the approved controls using GPOs, various scripting tools, and/or manual processes.



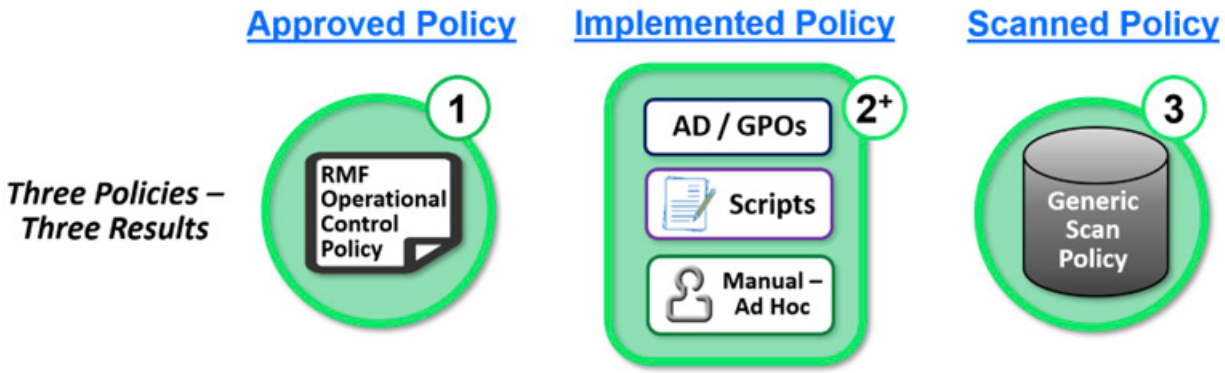
How often is the policy that's defined/approved in the RMF/ATO process implemented correctly in the production environment? Rarely. Therein lies the rub. There are multiple opportunities for human error as the approved policies are translated into various GPOs and/or scripts. Furthermore, assessment tools used to "check" the implementation of policies are generally not tailored to the specifically approved RMF system-level controls. The result is that the production implementation of controls seldom matches the RMF/ATO-approved policy.

Once in production, ongoing maintenance assessments are made using generic scanners with generic policy content. As with implementing controls, the maintenance content is typically not tailored to the control specification defined by the RMF/ATO process. Therefore, the generic scanner produces results that contain real control failures and significant numbers of false positives and negatives.

It is clear that traditional implementations of policy controls utilize three or more policies that are not synchronized:

1. The policy that is approved in the RMF/ATO process
2. The policy that is implemented by the IT organization with the various tools available in the environment
3. The scan results that are produced using generic policies

The result is an overall compliance failure requiring significant human resources to sift through results for actionable data. The burden is high enough that the reconciliation process can take days/weeks, thereby eliminating any possibility of an agile RMF monitoring process.

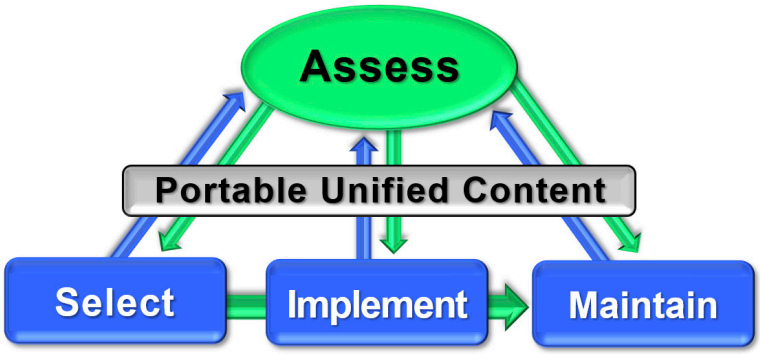


Addressing the Root Cause with Automation

The solution is easy to identify. Organizations must use the same policy and automation solution for all three steps — selecting, implementing/maintaining, and assessing system-level security controls. The simplest visualization of this process is a linear progression ending with the "assess." step.

But in reality, the process is not linear, and assessment is not the final step, rather it is at the center and a key requirement of each of the component steps. So, a proper visualization would look more like a diagram where assessment is integrated into all of the steps. A compliance automation solution must operate seamlessly in both pre-ATO (pre-production) and post-production phases of the application lifecycle. The key requirement is that a single automation tool and a single set of compliance-as-code must be able to assess and remediate systems using content that is transportable from domain to domain. This would include labs, the cloud, unclassified, and classified environments.

Additionally, in each of the assessment steps, content must be tailored to the specific app stack/system to render useful results. Generic scans against non-specific systems simply provide volumes of less-than-useful data that inhibit efficiency.



Anatomy of Solution

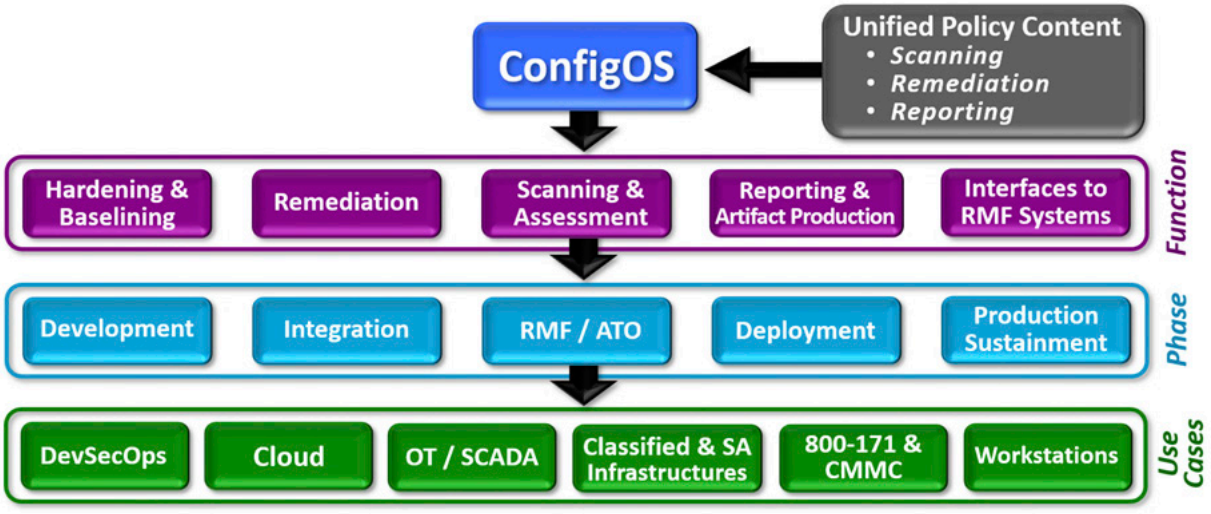
Several imperatives are key to effectively automating the synchronization of the RMF/ATO function within the IT organization:

- ✓ **Unified Operations** - The automation tool must be unified in both its automation capabilities and its ability to utilize unified content to implement, maintain, and assess controls at a granular level.
- ✓ **Hardening Process Simplification** - The hardening process needs to be simplified and automated so thatnon-specialized personnel can easily harden system-level controls around an app stack with minimal effort and experience. Accomplishing this will justify the creation of compliance-as-code early in the production process as possible. Hardening automation should also accelerate both RMF and quarterly policy updates activities, exercise all of the individual system-level controls, and create compliance-as-code with all deviations documented.
- ✓ **Policy Portability**– Once created in the pre-production phase, the compliance-as-code policy should be portable so it can be easily moved from domain to domain, as the app stack moves from phases of development to production.
- ✓ **RMF Artifacts** - A complete solution should also produce the requisite RMF artifacts, such as checklists and RMF system update files.

- ✓ **Capacity and Simplification** – This is a tricky one. The automation solution and requisite policy content must be agile enough to quickly harden policy around an individual app stack/system while having the capacity to remediate and maintain thousands of systems with discrete policies tailored for each system.
- ✓ **Policy Maintenance Automation** – An important task is the maintenance of policy. This requirement is two-fold. First, the solution should be able to eliminate drift by bringing production systems into compliance while they are in production. And second, the solution should automate the quarterly process of ingesting, testing, and creating new production policy baselines. Finally, the solution should reliably automate the deployment of the undated policies in production by bringing the infrastructure into compliance with the new policies.

SteelCloud's ConfigOS – Checking All the Boxes

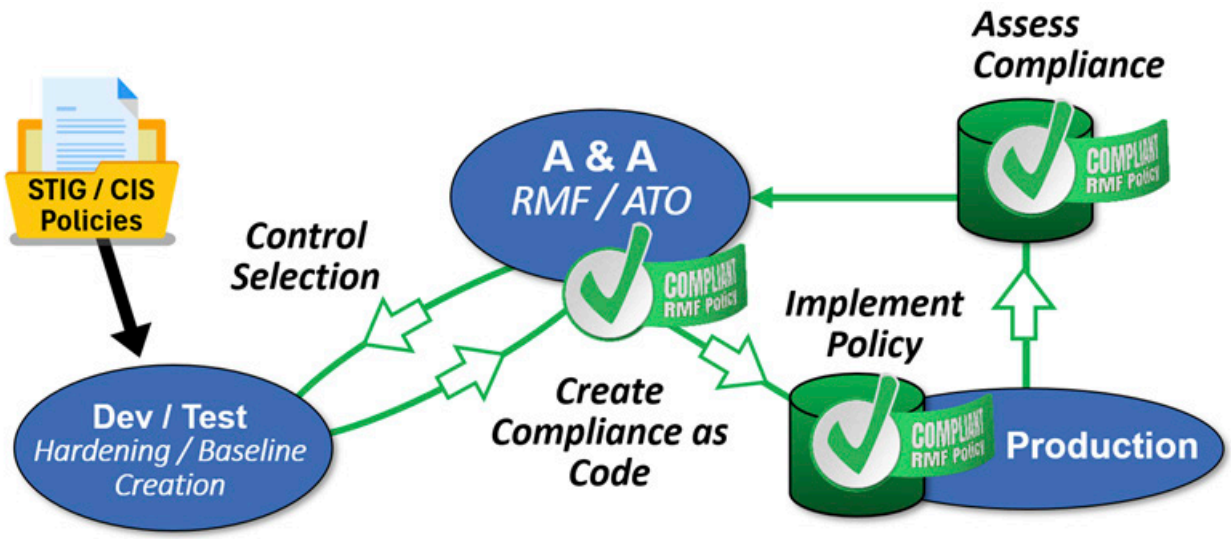
The ConfigOS cyber automation solution is elegantly designed software that easily allows organizations of any size to meet their compliance objectives. It is easy to implement and operate by any systems administrator with basic operating system skills. The key to its effectiveness is twofold—ConfigOS has unified automation for both assessment and remediation. It performs its tasks with unified content built for selection, implementation/maintenance, and assessment of controls based on STIG and CIS standards. And it also provides a comprehensive set of reporting, file creation, and checklist production tools.



ConfigOS has been proven to accelerate and automate compliance in virtually any type of environment, from the commercial cloud to classified air-gapped labs.

Accelerating the RMF/ATO Process with Hardening Automation & Unified Content

Historically, creating compliance-as-code in the pre-ATO phases of an app stack's lifecycle has been challenging to accomplish and hard to justify. ConfigOS dramatically simplifies the process of hardening and creates compliance-as-code as an automatic by-product of the hardening process. Utilizing unified content and advanced automation, ConfigOS routinely allows a user to harden all baseline controls around an app stack in about 60 minutes versus weeks or months.



The real advantage of the ConfigOS hardening process is that it automatically produces unified compliance-as-code policy baselines that can be used to scan, remediate, and report. This policy baseline will include descriptions of waivers/deviations of policy and the identification of controls that are to be remediated versus those that are scan-only. Once created and approved, the ConfigOS compliance-as-code policies can be moved directly into the production environment to implement and maintain the approved policies for specific systems or groups of systems.

In summary, ConfigOS delivers the following advantages:

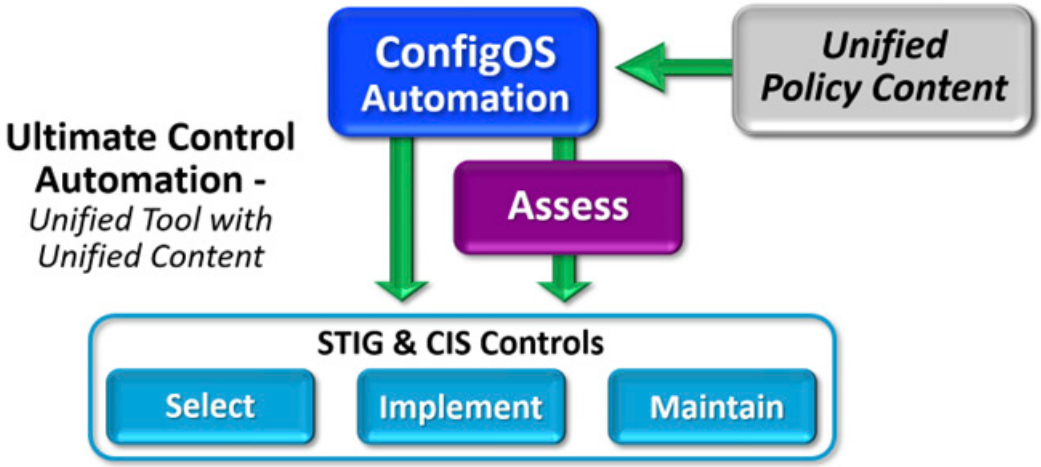
- ✓ Provides unified policies that are used to select, implement/maintain, and assess controls.
- ✓ Accelerates the RMF process by automating the technical tasks to harden app stacks and produce RMF artifacts.
- ✓ Produces approved compliance-as-code as an automatic by-product of the hardening process.
- ✓ Approved policies can be deployed directly into production to implement and maintain compliance with RMF-approved controls for specific systems or groups of systems.

Closing the Loop – The Synchronization of RMF and Production Compliance

Using a single system-level control automation together with unified content ensures that all infrastructures and compliance activities are wholly coordinated and synchronized. Production infrastructures' compliance always matches RMF-approved policies, and the results reported back to the A&A organization match what was approved in both form and detail.

Conclusion – Unified Automation with Unified Content

The key to bringing about this fundamental improvement is creating compliance-as-code policy as an output of the RMF process. Traditional approaches, including those using single-purpose tools to simplify steps along the way, cannot efficiently or effectively achieve that goal. A comprehensive automation solution that unifies policy content, however, ensures that the selection, implementation, and assessment of controls are automatically and continually in synch.



About SteelCloud

SteelCloud's patented ConfigOS software is the industry leader for automating STIG, CIS and CMMC compliance, detecting vulnerabilities, and remediating issues. With ConfigOS, weeks of manual work is completed in about an hour. Better yet, maintaining secure baselines is effortless, providing a strong foundation for Zero Trust and other emerging cybersecurity initiatives in the government and DIB. SteelCloud makes hard things—and hardening things—simple. For more information call (703) 674-5500, email info@steelcloud.com or visit www.steelcloud.com.

SteelCloud
20110 Ashbrook Place, Suite 200
Ashburn, VA 20147
1.703.674.5500
info@steelcloud.com | **steelcloud.com**