ATARC

# cATO Working Group

*CONOPS for Improving the RMF/ATO Process by Unifying the Selection, Implementation, and Continuous Monitoring of STIG/CIS Controls*

10/16/2024

# RMF/ATO – *System-level Control Automation*

Automation holds the promise of dramatically enhancing the RMF/ATO process. Unified automation with unified content simplifies system-level control compliance in pre-production, deployment, and sustainment of app stacks and workloads. It relies on unified content capable of implementing, assessing, and reporting on system-level controls in a singular, unified process.

This white paper examines traditional techniques and offers a new approach to automating these controls. In North America, there are two publishers of system-level policies, the DoD, which publishes the Security Technical Implementation Guides (STIGs), and the Center for Internet Security, which publishes the CIS Benchmarks. This white paper will focus on STIGs since it is the predominant control set used in the federal government.


## Key Automatable STIG Functions to Support an Agile RMF/ATO Process

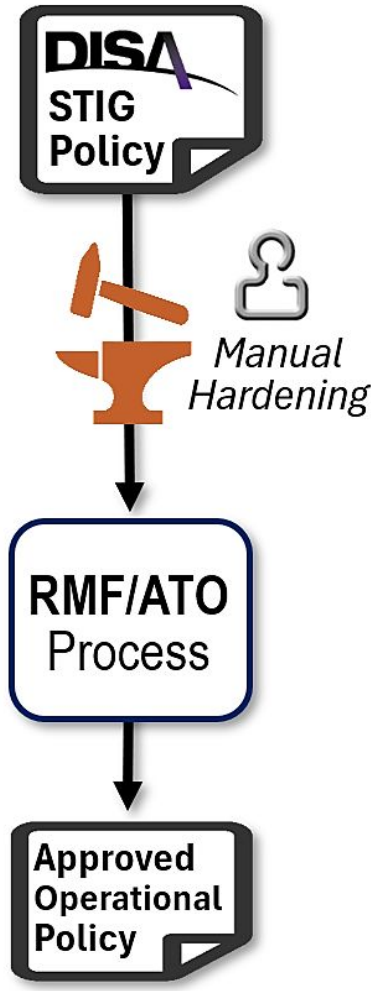
**SELECT** – The process to evaluate, harden, and document STIG controls for a given app stack/workload. Typically, the selection process includes waivers or deviations from standard organizational policy approved for production deployment as part of the RMF/ATO process.

**IMPLEMENT** – The process of executing the approved STIG policy in the production infrastructure. Traditionally, STIG implementation is accomplished by an organization's IT staff with one or more automation tools.

**MONITOR** – The process involves both the assessment (scanning) of STIG controls as well as the maintenance of those controls to bring systems into compliance that have "drifted" out of compliance. The implementation of periodically updated/new STIG policies is also included in the monitoring process.

# SELECT – *STIG Security Controls*

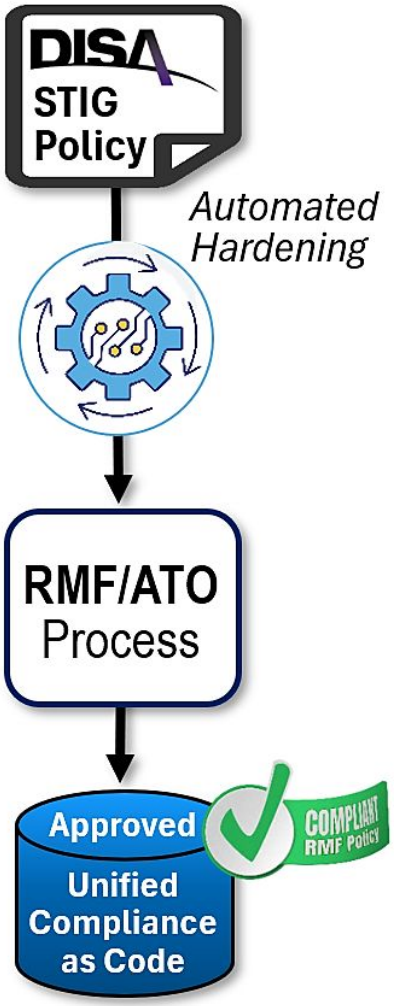
## Traditional



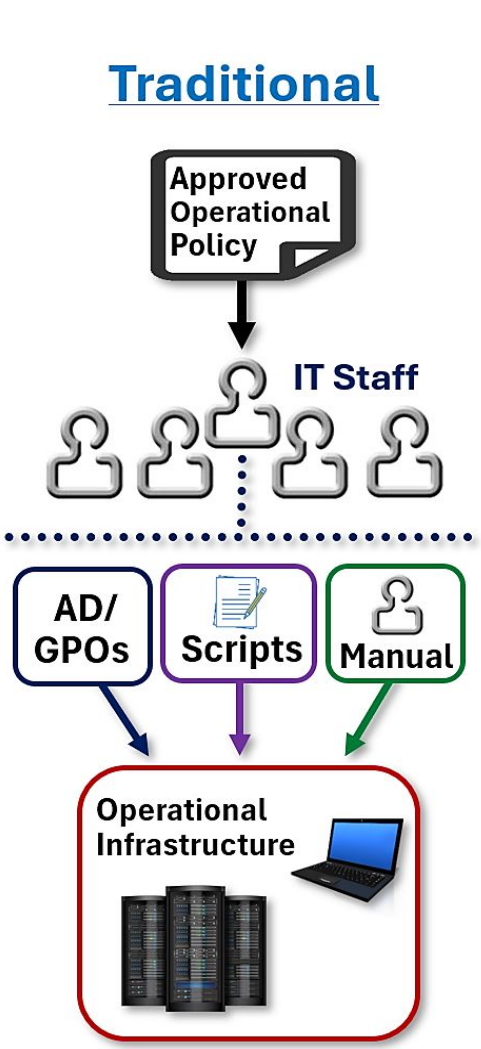

Selecting security controls involved the arduous task of hardening the STIG controls around an app stack/workload. Traditionally, this task takes days/weeks of manual engineering effort. The output of this effort is a document that defines the controls that will be implemented in production, together with details for the POAM/waivered controls. This control selection document is a primary RMF/ATO process input. The timing and resources to complete the control selection activity significantly impact ATO agility.

The "Unified" control selection process employs automation to accelerate the hardening process. An automated hardening capability can be accomplished in an hour, which might take an engineer a week or more to complete. The primary advantage of automating the hardening process is more than just time/resource savings. Automated control hardening creates unified "compliance-as-code" in addition to RMF control compliance documentation. The importance of creating compliance-as-code in this stage will become apparent in the implementation and monitoring activities. Unified STIG compliance-as-code not only accelerates the process but also provides a comprehensive approach with the built-in ability to remediate, assess, and report, instilling confidence in the process's effectiveness.

## Unified

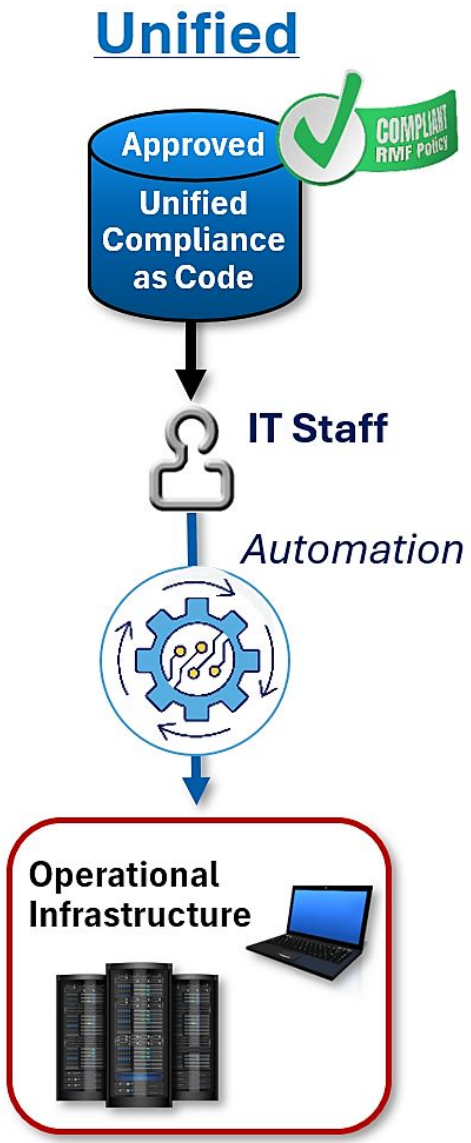


# IMPLEMENT – *STIG Security Controls*



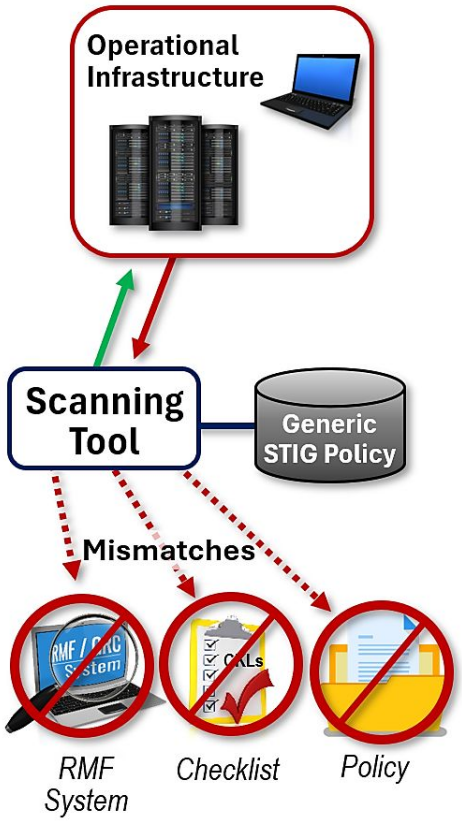

The traditional implementation of STIG controls required the IT organization to interpret the RMF STIG policies from the documentation of the RMF/ATO process. This involved using the tools available in their environments to translate and implement the approved controls into the infrastructure. These tools typically included developing GPOs, writing scripts, and manually updating system resources such as registry keys and configuration files. This translation and implementation process is time-consuming, labor-intensive, and error-prone. The unified approach significantly reduces these human-dependent tasks.

The unified approach significantly reduces the time and effort required for implementation. The heavy lifting is done in the pre-ATO process, and the IT staff can quickly implement the STIGs in production using the same unified automation capability that created the unified policy content. This eliminates the need for translation, as the automation capability uses the exact same content that was approved in the RMF/ATO process. As a result, the time required for implementation is reduced from hours/days to minutes, and the error-prone translation process is eliminated, ensuring a more reliable implementation of the approved STIG policy



# MONITOR – *STIG Security Controls*

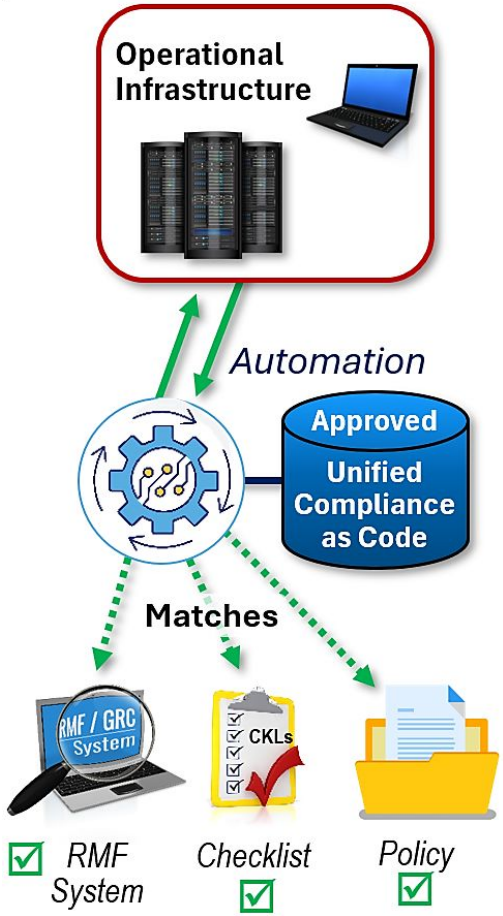
## Traditional



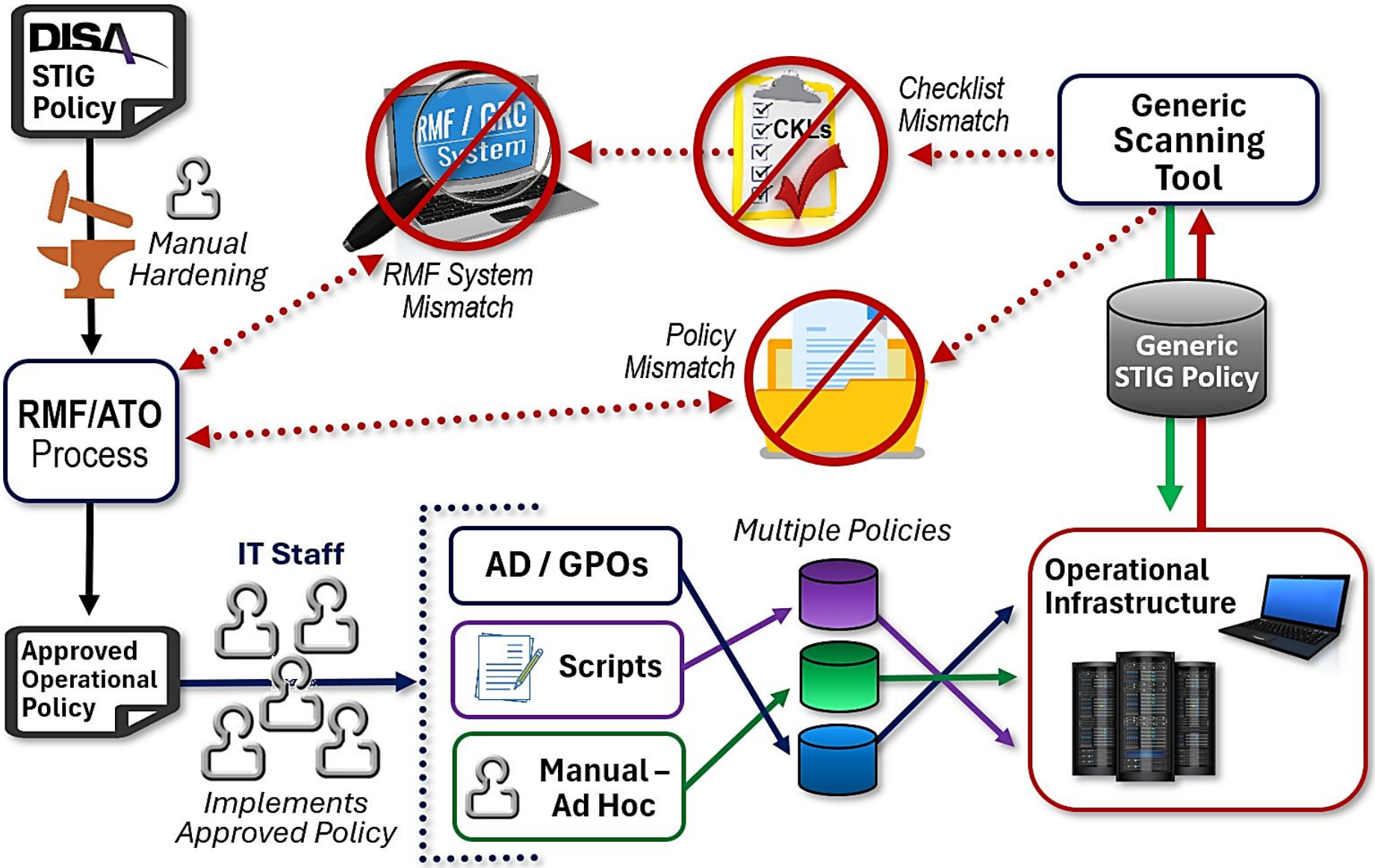

The traditional process for compliance monitoring utilizes scanning tools with generic STIG content. The use of non-tailored generic STIG content ensures that there is no possibility that the monitoring output will match any of the policies used in the RMF/ATO process. These would include the approved policies, the RMF system itself, and the STIG Viewer Checklists that were approved in the RMF/ATO process. Unfortunately, this method cannot be corrected since scanning tool content is practically impossible to tailor, and the scanning systems themselves do not generally allow specifically tailored policies to be directed to specific systems. Scanning content is not coordinated with the implementation content.

The unified approach, in contrast, offers a more promising solution. It leverages the same content approved in the RMF/ATO process to scan production systems. This tailored content, combined with the unified automation, allows for targeting individual/groups of systems and ensures that the results always align with approved policy. This alignment with the approved policy instills confidence in the accuracy of the unified approach. The real advantage is that the infrastructure is continually being remediated with content approved in the ATO process.

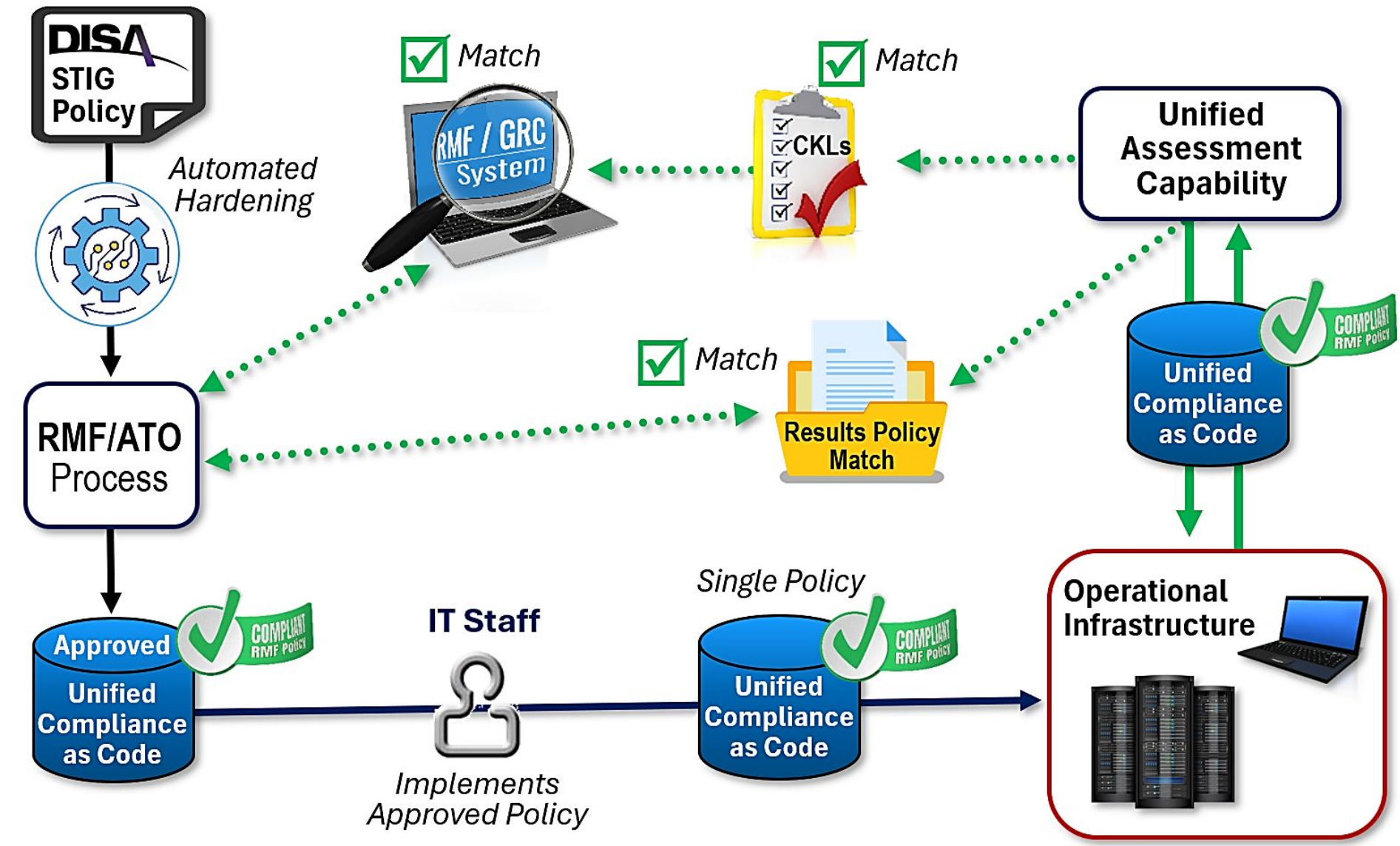
## Unified



# Traditional STIG Compliance Workflow



# Unified STIG Compliance Workflow



# Unified Compliance Automation – *Summary*


As examined in this white paper, new unified automation techniques promise to dramatically decrease the technical requirements necessary to support an initial ATO and the ongoing effort to sustain a continual ATO process. Unified automation with unified content is the natural evolution from the traditional disjointed discrete processes for selecting, implementing, and monitoring STIG compliance. Assessment is no longer the first step in a "find-n-fix" workflow; instead, it is the last step that confirms the integrity of the automation regimen.

## SELECT

Unified automation can reduce hardening time/effort by more than 95%. The unified approach also dramatically reduces the requirement for scarce human technical resources.

## IMPLEMENT

While unified automation significantly reduces the effort to implement approved STIG policy on production workloads, its real advantage is that it significantly cuts timelines, reduces staffing requirements, and reduces policy translation errors.

## MONITOR

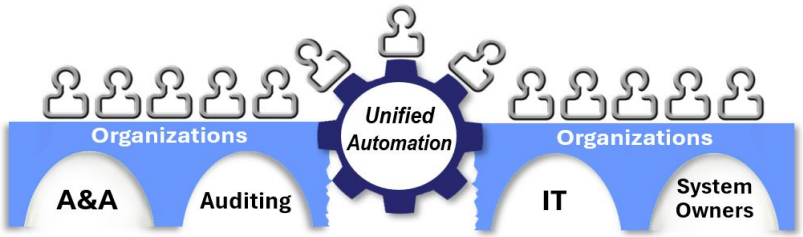
A unified automation approach simplifies compliance staff work by providing output that directly maps to the approved ATO policies. Additionally, the effort of updating new STIGs into the environment can be reduced by up to 90%.

# Unified Compliance Automation – *Future State*

## Organizational Imperatives

Traditionally, Assessment & Authorization (A&A), IT, and auditing organizations have operated with a great deal of autonomy. Their inputs/outputs were typically accomplished with discrete handoffs, and each had its own technologies to accomplish their respective tasks. The successful implementation of unified compliance will be affected more by organizational friction and inertia than cost, level of effort, or technology. Success with this new unified compliance approach will require closer coordination of responsibilities and processes between organizations. This is especially true with the auditing function where there will be a need to "shift left" to better integrate their involvement earlier in the process.

All three organizations will need to "unify" their own compliance responsibilities around a single unified compliance capability. A unified compliance automation system will provide the "bridge" to synchronize all compliance activities toward improving the ATO process.




***Bridging the Gap***

## Additional Use Cases

**CBOM** *(Compliance Bill of Materials)* – CBOM is a key extension to unified STIG automation. CBOM automation includes a super-set of all the machine-automatable controls that were defined and approved in the RMF/ATO process – both STIG and non-STIG. Examples of the additional controls may include specific software/agents, ports/protocols, files/folders/certs, KRIs *(Key Risk Indicators)*, *etc.* CBOM automation gives Risk and Compliance organizations a complete picture of the information necessary to support an agile ATO process. Additionally, since the CBOM is automated with unified content, compliance with these additional RMF controls is ensured and monitored correctly.

**ZTA** - Implementing Zero Trust is a prime objective across the entirety of the federal government. Both CISA and the DoD have emphasized good cyber hygiene as the foundation for Zero Trust. NIST has recommended that "organizations need to implement comprehensive information security and resiliency practices for Zero Trust to be effective." Unified automation is a critical capability that allows organizations to implement an effective cyber hygiene program while supporting an agile ATO process.

# Addendum – *STIG Compliance Technical Workstreams*

| | Workstreams | Tempo |
|---|---|---|
| **Dev / Test Pre-ATO** | Ingest new STIG policies | Quarterly |
| | Update existing baselines/operational policies | Quarterly |
| | Harden & create new/updated operational policies | Variable |
| | Manage manual controls | Variable |
| | Produce RMF output | Variable |
| **Production, Monitoring & Sustainment** | Acquire endpoints into compliance operations | Continuous |
| | Associate new/updated policies/schedules to endpoints | Continuous |
| | Implement new/updated policies in production | Continuous |
| | Monitor & maintain policy compliance in production | Hourly / Daily |
| | Assess compliance and produce reporting | Daily / Weekly |
| | Update compliance results storage | Continuous |
| | Produce specialized output | Daily / Weekly |

# Acknowledgements

*Disclaimer: This document was prepared by the members of the ATARC cATO Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with and shall not be used for advertisement or product endorsement purposes.*

Document Prepared by:
Brian Hajost, Industry Chair, ATARC cATO Working Group