

# AUTOMATED COMPLIANCE CHECK: GUIDE TO THE ANSIBLE PROJECT



Graham Tech  
White Paper



**GRAHAM**  
TECHNOLOGIES

# TABLE OF CONTENTS

**1.0 EXECUTIVE SUMMARY ..... 2**

**2.0 INTRODUCTION: FROM MANUAL AUDITS TO AUTOMATED ASSURANCE ..... 3**

THE AUTOMATED COMPLIANCE JOURNEY WITH ANSIBLE ..... 4

**3.0 STARTING POINT: A SECURITY RULE BECOMES A TASK ..... 5**

**4.0 EXECUTION: HOW THE CHECK TRAVELS THROUGH THE SYSTEM..... 6**

**5.0 DESTINATION: TURNING RAW DATA INTO ACTIONABLE INSIGHT..... 7**

**6.0 SO WHAT?: KEY BENEFITS OF AUTOMATION..... 8**

**7.0 CONCLUSION: THE FUTURE OF AUTOMATED COMPLIANCE ..... 9**

# 1.0 EXECUTIVE SUMMARY

This white paper describes how the Ansible Project enables continuous compliance by translating security requirements into 'policy as code,' executing automated validation checks across systems, and generating standardized evidence artifacts for audits and operational monitoring. Using Red Hat Ansible Automation Platform, compliance checks (such as validating disk encryption mandated by STIGs) run on a schedule or trigger, capture results in formats like JSON/CSV/SAR reports, and deliver outputs to dashboards and a centralized compliance database. This automated approach reduces manual audit effort, improves consistency at scale, provides near real-time visibility into compliance posture, and strengthens transparency and auditability through repeatable, version-controlled evidence aligned to federal standards such as NIST 800-53.

# 2.0 INTRODUCTION: FROM MANUAL AUDITS TO AUTOMATED ASSURANCE

In the world of IT security, proving that systems are configured correctly has traditionally been a painstaking, manual process. Auditors would spend weeks or months combing through systems, generating static reports that were obsolete the moment they were printed. This is where the modern approach of continuous compliance comes in, transforming a periodic, static event into a dynamic, ongoing process.

This document explains how the Ansible Project serves as a core engine in this modern ecosystem, automating compliance to make it faster, more reliable, and more transparent.

The project's primary goals are to achieve:

- **Compliance Enforcement:** Automatically check systems against established security standards, such as the National Institute of Standards and Technology (NIST) 800-53 framework and Security Technical Implementation Guides (STIGs).
- **Operational Efficiency:** Drastically reduce the time and manual effort required for audits and system checks, freeing up experts to focus on more complex challenges.
- **Platform Integration:** Seamlessly feed the results of these automated checks into monitoring tools and dashboards, providing a real-time view of the organization's compliance posture.

To make this process concrete, we will follow a single, common security requirement throughout this guide: **validating disk encryption**. This check, mandated by STIGs, ensures that sensitive data stored on a server is protected. Let's trace the journey of this single check from a written rule to an actionable insight on a dashboard.

# The Automated Compliance Journey with Ansible

## 1. Define: Policy as Code



Security rules from standards like NIST and STIGs are translated into Ansible playbooks.



**ANSIBLE PLAYBOOKS**

## 2. Execute & Generate Evidence



The playbook runs automatically, validates systems, and captures the results as evidence artifacts.



**EVIDENCE ARTIFACTS**

## 3. Deliver Actionable Insights



### DASHBOARDS & TOOLS

Enables real-time detection of issues like configuration drift for immediate remediation.



### COMPLIANCE DATABASE

Creates a permanent, auditable record for assessment teams to verify compliance.

## KEY BENEFITS OF AUTOMATION



### Continuous ATO Alignment

Shifts compliance from a once-a-year event to an ongoing, near real-time process.



### Scalability and Consistency

The same check runs across thousands of systems, eliminating human error and inconsistency.



### Transparent and Auditable

Creates repeatable, version-controlled evidence that simplifies and speeds up audits.

# 3.0 STARTING POINT: A SECURITY RULE BECOMES A TASK

Every automated task begins with a human-defined requirement. In this system, security rules are not just items on a checklist; they are translated into code. The Ansible Project maps its work to specific NIST 800-53 Rev. 5 controls, such as AC-2 (Account Management) or CM-6 (Configuration Settings), ensuring every action has a clear purpose.

This translation from rule to code is done using an **Ansible playbook**. A playbook is a file containing a set of instructions that tells the automation platform exactly what to do. Think of it as a repeatable recipe for a specific task. This practice of managing policy in version-controlled files is a fundamental industry shift known as "**Policy as Code.**" It treats compliance rules with the same rigor and repeatability as application code, eliminating ambiguity and configuration drift at the source.

"For our example, a playbook is written to validate that STIG-required disk encryption is active. This playbook is the automated instruction that directly maps to the federal security requirement." With the playbook created, the abstract security rule now exists as a tangible, executable set of instructions, ready to be deployed.

# 4.0 EXECUTION: HOW THE CHECK TRAVELS THROUGH THE SYSTEM

Ansible/AAP is responsible for running the compliance checks and generating the evidence artifacts, while downstream dashboards and the compliance database handle storage, visualization, and long-term audit tracking of the results.

Once the playbook is defined, the next step is to run it and gather the results. The magic of this system lies in its repeatable, automated data flow. Let's break down the journey of our disk encryption check into four distinct stages:

- **Orchestration and Execution:** The process begins when the Red Hat Ansible Automation Platform (AAP) is instructed to run the disk encryption playbook. This is typically done through automated pipelines, ensuring the check runs on a schedule or in response to a specific event without any manual intervention.
- **System Validation:** The playbook connects to the target system (e.g., a server). It then executes its predefined instructions to verify the compliance status. For our example, it checks the server's configuration to confirm that disk encryption is enabled and functioning correctly.
- **Evidence Generation:** The result of the check—whether the disk is encrypted or not—is captured. This raw output is then converted into standardized **evidence artifacts**. These artifacts are structured data files that serve as proof of the check and its outcome, created in several formats for different uses:
  - JSON, CSV, SAR reports (System Assessment Reports)
- **Data Transmission:** Finally, these newly created evidence artifacts are pushed out from the automation platform to centralized locations for storage and analysis.

This entire workflow is supported by a robust ecosystem of technologies that ensure security and reliability:

- **Source Control:** Stores the versioned playbooks, so there is always a clear record of the "recipe" used for the check.
- **Cloud Services:** Provide encrypted storage for the evidence artifacts, ensuring the results are kept safe and secure.
- **Identity and Access Management:** Enforces user account controls throughout the process, making sure only authorized systems and personnel can initiate or modify checks.
- The technical execution is now complete. The check has run, and the results have been securely collected and stored.

# 5.0 DESTINATION: TURNING RAW DATA INTO ACTIONABLE INSIGHT

The evidence artifacts generated in the previous step don't just sit in storage; they are sent to two primary destinations where they are transformed from raw data into valuable, actionable information.

Destination	Purpose
<b>Dashboards &amp; Tools</b>	Artifacts are pushed to security and operations monitoring tools. This allows teams to detect and remediate critical issues like <b>configuration drift</b> —unauthorized changes that violate the security baseline—in near real-time.
<b>Compliance Database</b>	Results are stored in a centralized compliance database. This creates a permanent, auditable record that assessment teams can use to verify compliance over time.

Let's bring our disk encryption example to its conclusion. After the playbook runs, a security operator might see a red flag appear on a dashboard, indicating that a specific server is now "non-compliant" because its disk encryption was disabled. At the same time, an auditor preparing for a review could pull the generated SAR report from the compliance database as official evidence. If a gap were found, the system could also point to compensating control documentation that explains the exception.

This closes the loop, turning an automated check into a clear signal for both daily operations and long-term governance.

# 6.0 SO WHAT?: KEY BENEFITS OF AUTOMATION

Adopting this automated workflow provides significant advantages over traditional, manual methods. The value goes beyond simply saving time; it fundamentally changes how compliance is managed.

- **Continuous ATO Alignment:** This system shifts compliance from a static, once-a-year event to a continuous, ongoing process, aligning with modern federal guidelines like NIST SP 800-137. Instead of wondering about the state of their systems, teams have a constant, near real-time view.
- **Scalability and Consistency:** The exact same playbook can be run across one server, a hundred servers, or thousands. This ensures that every system is evaluated against the identical standard, eliminating the human error and inconsistency that can plague manual audits.
- **Transparency and Auditability:** Because the entire process is automated and version-controlled, it creates repeatable, auditable evidence. This evidence is directly mapped to specific federal requirements, making audits simpler, faster, and more accurate.
- **Future Readiness:** This approach aligns the organization with the broader industry shift toward Policy as Code, building a foundation for more advanced, automated governance and scoring in the future.

# 7.0 CONCLUSION: THE FUTURE OF AUTOMATED COMPLIANCE

We have followed the complete journey of a single compliance check: from a security rule being translated into an Ansible playbook, to the playbook's execution across the infrastructure, and finally, to the transformation of its results into actionable reports and real-time dashboards. This automated loop provides a powerful mechanism for maintaining security and proving compliance at scale.

The evolution of this system doesn't stop here. Planned enhancements aim to make the process even smarter and more integrated, including:

- Standardizing reports with an open-source format called **OSCAL** for broader federal and inter-organizational use.
- Using **Artificial Intelligence and Machine Learning (AI/ML)** to develop more intelligent compliance scoring, leveraging techniques like reinforcement learning and anomaly detection.
- **Expanding coverage** to include more systems and third-party tools.



**Headquarters**

1401 Mercantile Lane  
Suite 301  
Largo, MD 20774

Phone: (240) 764-7899  
Fax: (301) 560-6579  
info@graham-tech.net

**graham-tech.net**

