




Improving security compliance in the Intelligence Community with automation

“Organizations should maximize the use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF). Automation is particularly useful in the assessment and continuous monitoring of controls, the preparation of authorization packages for timely decision-making, and the implementation of ongoing authorization approaches—together facilitating a real-time or near real-time risk-based decision-making process for senior leaders.”

NIST SP 800-37

Risk Management Framework for Information Systems and Organizations²

 facebook.com/redhatinc
 @RedHat
 linkedin.com/company/red-hat

Executive summary

Achieving and maintaining security compliance for information technology systems in the U.S. Intelligence Community (IC) takes time and effort that would be better served advancing the mission. By adopting an enterprise automation strategy based on Red Hat® Ansible® Automation Platform, security compliance can be applied to multiple systems using a configuration-as-code approach. This saves time and effort during the authority to operate (ATO) process and subsequent operations, while improving consistency and accuracy at scale.

Risk management and authority to operate

IC information technology systems must go through the ATO process, which is aimed at minimizing and managing security risk. For an information technology (IT) system to gain ATO, a system security plan must be created which, among other things, defines a set of policy controls from 1 or more compliance profiles that must be applied to the components of the system. The common security controls used within the IC are primarily defined in [NIST Special Publication 800-53¹](#), *Security and Privacy Controls for Information Systems and Organizations*, and implementing these controls is typically done by following DISA Security Technical Implementation Guides (STIGs). STIGs are available for many IT system components, including operating systems, network devices, virtualization and cloud environments, container platforms, and numerous applications such as databases, web servers, application servers, and the like. From a risk management perspective, STIGs are valuable tools that provide expert advice from product manufacturers as well as consistent baselines for compliance efforts across the IC. Beyond the STIGs, many agencies and organizations have additional internal security policies which also must be applied to IT systems, ranging from policies managing supply chain risk management to those aimed at mitigating insider threats. Taken together, this varied set of security controls must be applied for an IT system within the IC to gain ATO and go into production.

Compliance challenges

Once the necessary controls are identified, they must then be applied to the relevant system components. Depending on the individual implementers, this might be done by manually configuring each system component, or using various checklists, scripts, or domain-specific or vendor-specific tooling. If a system security plan covers components that are managed by separate teams—for example, network administrators and operating system administrators—different teams often take different approaches depending on the tools they are most familiar with. These disparate approaches can present certain challenges to meeting the necessary security controls:

- ▶ The manual configuration approach is labor-intensive and prone to human error, and does not scale well with large IT systems.

¹ *“NIST Special Publication 800-53, Rev. 5 Security and Privacy Controls for Information Systems and Organizations.” accessed 25 April 2024.*
² *“NIST Special Publication 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.” accessed 23 April 2024.*

Authority to Operate

Ansible Automation Platform has achieved Authority to Operate in more than 1 intelligence agency and the Department of Defense.

Broad Interoperability

With over 55 certified technology partners, Red Hat Ansible Automation Platform can automate security controls across a wide IT environment, including network, cloud, security, infrastructure, and edge systems.

- ▶ Scripts can scale better than manual configuration, but are usually limited to applying controls to operating systems or applications, and may not be portable across these IT system components. They also require expertise in each scripting language used, and can also be fragile if not written correctly, applying unintended configurations. Maintenance over time can be challenging.
- ▶ Vendor-specific tooling typically only works with a single vendor's products, and also requires specific expertise that may not extend to different vendor products. This can fragment efforts to achieve compliance, and may require additional personnel who have the needed expertise.

Added to these is the challenge of maintaining compliance over time. While compliance is verified during the ATO process, reverification often does not take place until years later when the system ATO is renewed. During the intervening period, mission requirements may dictate configuration changes with unintended consequences to compliance, or controls may be disabled during troubleshooting and never restored. Loss of institutional knowledge through personnel turnover or contract changes means that the reasons for any configuration deltas may be lost.

Overcome compliance challenges with automation

Like their civilian and industry counterparts, many IC organizations are discovering the benefits of [building a robust IT automation strategy](#)³ as a means of increasing staff productivity and efficiency, as well as improving the accuracy of IT system configuration at scale. A strategic automation initiative will enable existing personnel to focus less on day-to-day system maintenance and more on solving mission-critical problems. When applied to compliance requirements, a holistic automation strategy based on [Red Hat® Ansible® Automation Platform](#) provides a way to overcome the challenges discussed previously:

- ▶ Automating the implementation of a compliance control ensures that it is applied consistently at any scale, reducing or eliminating any errors that could be introduced using a repetitive manual configuration process.
- ▶ Scripts can be considered a type of automation, but they are often tactical in nature, written by an individual or team for a specific need on a specific system. Writing automation content using a cross-platform tool introduces the opportunity to treat an automated task as a strategic asset, an opportunity that can be employed for consistent results by teams managing multiple IT systems. Using a single automation platform reduces the need for multiple scripting languages and the expertise that may entail.
- ▶ A cross-platform automation capability such as Ansible Automation Platform also reduces reliance on multiple vendor-specific tools for managing configuration or compliance. This opens up opportunities for more teams—including those with no expertise using vendor-specific tools—to create useful automation content that can be used strategically across different IT systems with the same compliance requirements.

Automation also empowers system owners to take a proactive approach to compliance over the lifecycle of an IT system. Automation is specifically called out in [NIST Special Publication 800-37](#)¹, *Risk Management Framework for Information Systems and Organizations*, as a key capability when applying and monitoring system security controls in a continuous manner. Any control which is automated can not only be checked, but reapplied on a regular cadence to minimize configuration

³ *The Enterprisers Project. "CIOs and automation: How to build a robust automation strategy." 7 March 2023.*

Red Hat is an Automation Leader

Red Hat has been named a leader by Forrester Research in The Forrester Wave: Infrastructure Automation, Q1 2023.⁴

drift. In other words, compliance automation with Ansible Automation Platform can provide the underpinnings of a continuous compliance framework used to ensure a system remains compliant throughout its life cycle.

Automation and configuration-as-code

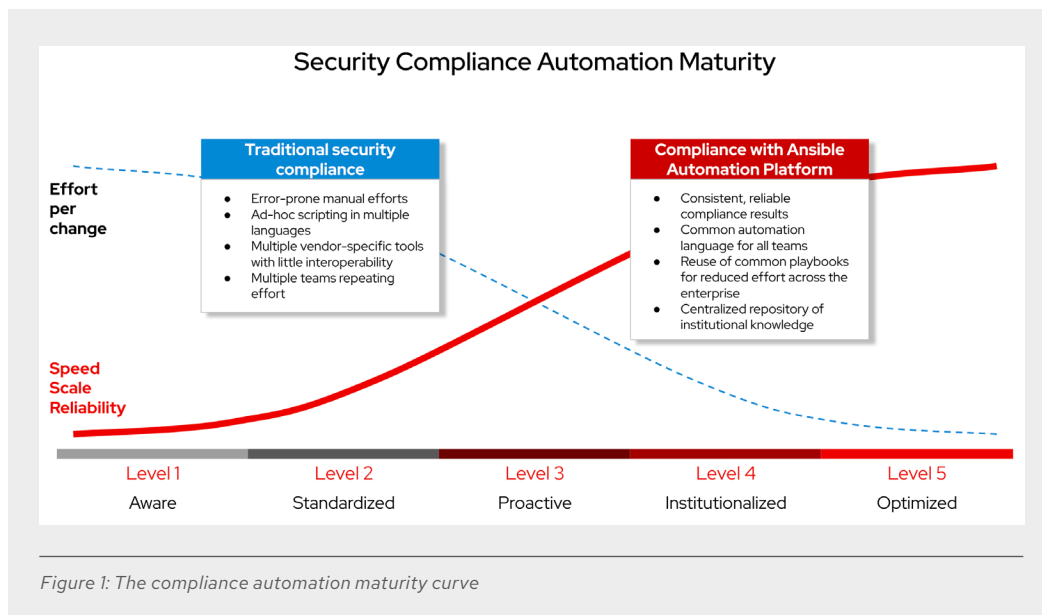
An advantage to using Ansible Automation Platform is that all automation tasks are captured in simple, human-readable artifacts called [Ansible Playbooks](#). These playbooks can be treated as code and kept under source code control, meaning that the compliance state of an IT system that is captured in playbooks can be managed using a common code development pattern: intended configuration changes can be added to a new or existing playbook, tested for accuracy, reviewed by approving authorities, committed to a production repository, and automatically applied to systems once committed. Under this configuration-as-code paradigm, ad-hoc changes to security settings are reduced if not eliminated, there is transparency as to who committed security-relevant configuration changes to the playbook repository, and configurations may be rolled back to previous states if desired.

The configuration-as-code approach has additional benefits. IC agencies have many IT systems in production, all of which require a system security plan that defines the security controls which must be applied. While the IT systems may be numerous, the infrastructure components that comprise those systems are finite—physical or virtual servers, operating systems, network devices, storage devices, and the like. The controls applied to these components are largely sourced from the same policies, meaning that different system owners end up applying a common set of controls to their systems. In other words, there is significant overlap between IT systems when implementing security controls. A second-order effect of a configuration-as-code approach to compliance automation is that these configurations can be reused by multiple system owners.

Institutionalized compliance through automation

Reuse of compliance automation at scale with Ansible Automation Platform results in an institutionalized capability for making the ATO process easier and quicker. A repository of common playbooks can be preapproved by security auditors and made available to the enterprise, and using the role-based access capabilities of Ansible Automation Platform, system owners can run 1 or more playbooks to apply well-known security controls across their individual systems. Institutional knowledge surrounding the compliance process and the security controls involved only increases as more teams use centralized, vetted security control configuration, reducing the risk of knowledge loss as individuals leave or change projects. This is particularly important when addressing agency or organization-specific security requirements beyond those controls defined in the STIGs.

⁴ Red Hat press release. “Red Hat Named a Leader in Infrastructure Automation by Industry Research Firm.” 21 March 2023.



Additionally, automation is not limited to the realm of security compliance. Many security-related IT operations can be automated, including security patching, updating system component software, managing firewall rules, or orchestrating complex sets of tasks related to investigation enrichment, threat hunting, or incident response.

With Ansible Automation Platform, the benefits of compliance automation to the IC are clear: consistency and accuracy in implementing security controls, reduced effort when bringing multiple IT systems of any scale into compliance, and reduced time to achieve ATO for mission-critical systems.

Get started

Red Hat can help you with more information on security compliance automation with Ansible Automation Platform. When you are ready, email: info-IC@redhat.com.

Learn more

Fast-track your mission with Red Hat. Learn more about how [Red Hat helps the U.S. Intelligence Community](#).



About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with [award-winning](#) support, training, and consulting services.

[f facebook.com/redhatinc](https://facebook.com/redhatinc)
[@RedHat](https://twitter.com/RedHat)
[in linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)

North America
 1888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
 00800 7334 2835
europa@redhat.com

Asia Pacific
 +65 6490 4200
apac@redhat.com

Latin America
 +54 11 4329 7300
info-latam@redhat.com