WHITEPAPER

Speeding Secure Software Development and Attaining Authority to Operate Faster and at Scale in the U.S. Government Agencies

Security Compass

How to Expedite Authority to Operate & Secure Development at Scale in the US Government

By Jay Ryan, U.S. Federal Government Program Manager, Security Compass

Connecting secure software development and ATO

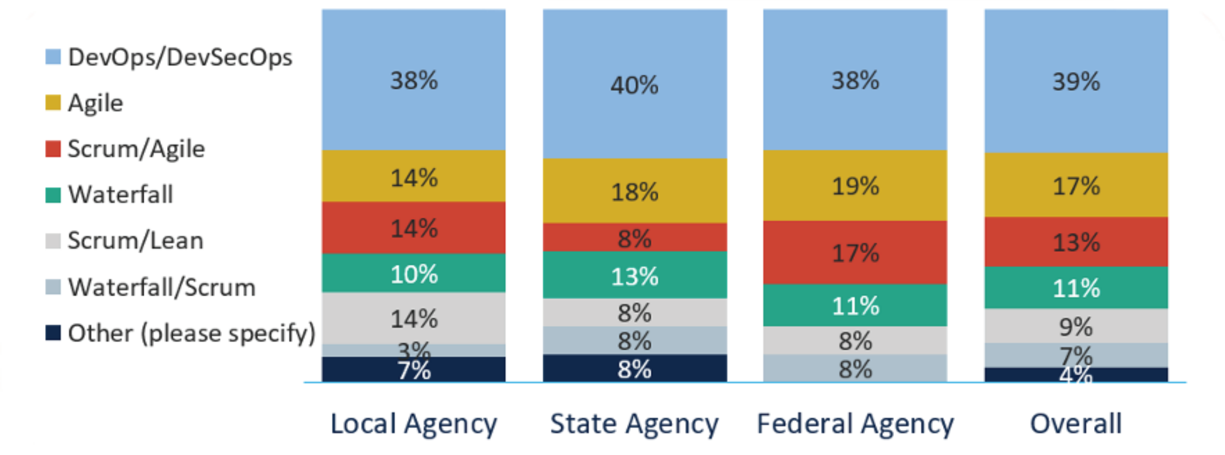
U.S. government agencies are undergoing tremendous change in the area of secure software development maturity. A key benefit of the change is the reduction in time to achieve Authority to Operate (ATO) for software applications. Ensuring software is constructed with security in mind from the very beginning of the software development process reduces the risk of a breach and streamlines ATO attainment. Secure software development does not negate the need for risk assessment and management. Instead, it clarifies threats and mitigation options much earlier in the software development process.

There are a few relevant pieces of evidence that support the notion that secure software development is a U.S. federal government priority.

From Waterfall to Agile and DevSecOps

First, we are witnessing a shift toward Agile and DevSecOps methodologies (see Figure 1) which focus on considering security much earlier in the software release process.

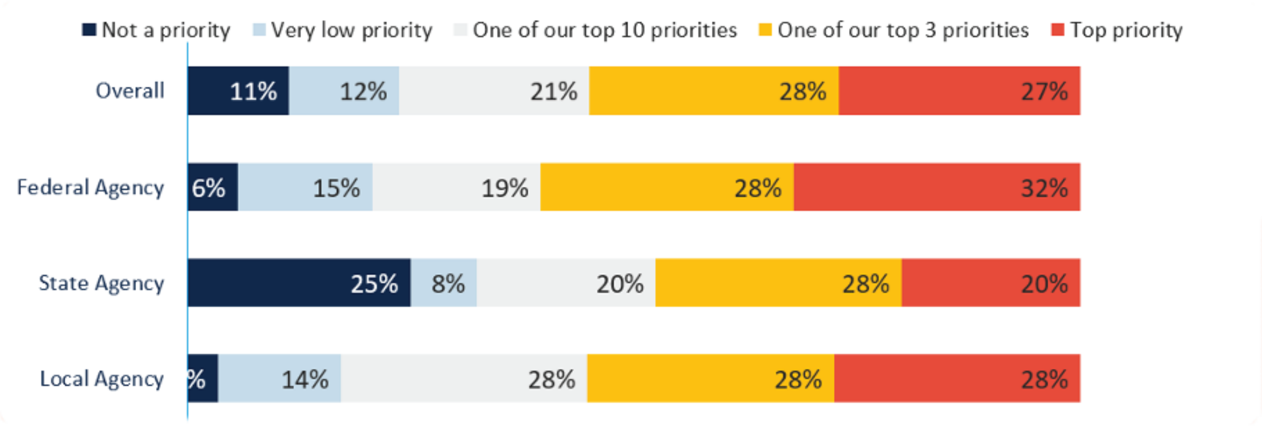
Figure 1:"How would you describe the software development methodology within your organization?"



Source: "The 2021 State of Secure Development & ATO in U.S. Government Agencies" survey (commissioned by Security Compass and conducted by Golfdale Consulting)

We commonly refer to this as a "shift left," (see Figure 2) which implies security and compliance concerns are addressed through the early stagesof design and requirements.

Figure 2: *"To what degree is 'shifting security left' in the software development process a priority within your organization?"*

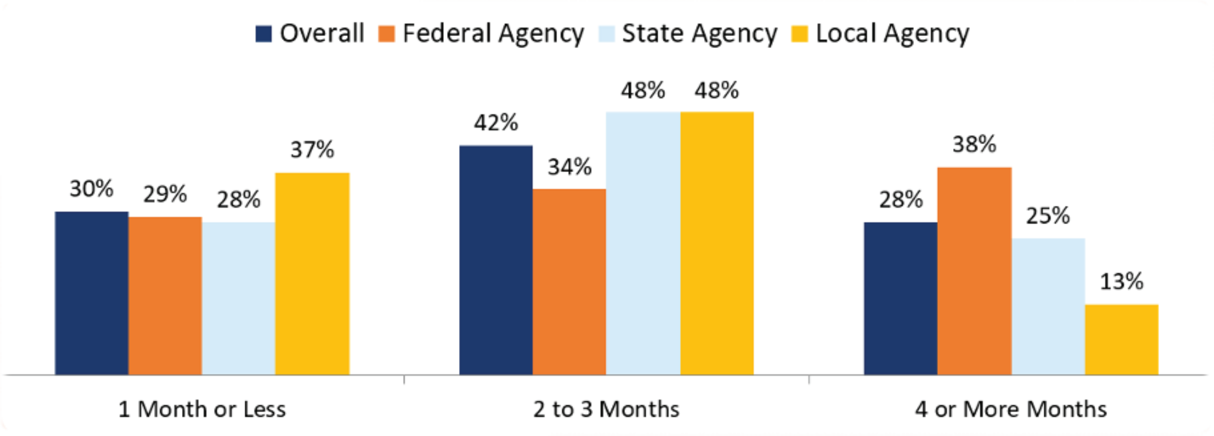


Source: Security Compass and Golfdale survey, "The 2021 State of Secure Development & ATO in U.S. Government Agencies" survey (commissioned by Security Compass and conducted by Golfdale Consulting)

From months to weeks or days

Next is the emphasis on scaling ATO, or the push to shorten the approval process (see Figure 3), ideally driving toward continuous ATO where much lower risk incremental decisions are made, rather than infrequent high-risk decisions.

Figure 3: "What is the average time to achieve Authority to Operate within your organization?"

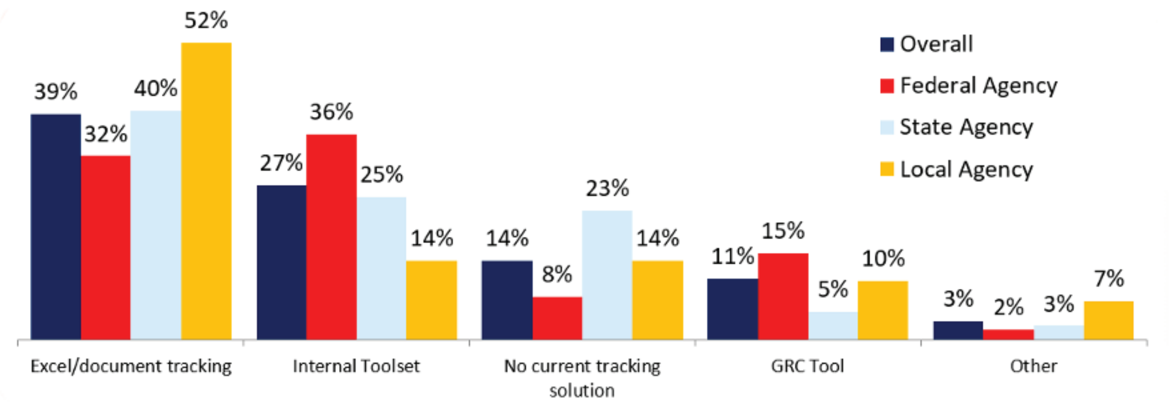


Source: Security Compass and Golfdale survey on US Government, 2021

Security inheritance and scalability

The third piece of evidence is the speed of innovation to support continuous improvement. This includes layered compliance for scalability and security inheritance (see Figure 4), microservices architectures for reusability, cross-functional membership for empathy, external resources for diversity, and factories for better consistency.

Figure 4: "How do you primarily track inherited security from supporting systems/infrastructure in your compliance process?"



Source: Security Compass and Golfdale survey on US Government, 2021.

Current challenges

While much positive change is occuring within the U.S. federal government, it is hardly a smooth transition across the board. Current challenges include:

- **Design enforceability:** There are lingering questions about design enforceability in a still maturing DevSecOps culture. In addition, challenges are presented when designers attempt to proactively influence the early stages of development and are not permitted.

- **Siloed communication:** Existing organizational layers can also impede the need for cross-functional collaboration between development and operations teams and the authorizing official (AO) members.

- **Understanding how to operationalize DevSecOps:** Often there are questions about how to systematically operationalize DevSecOps. In the U.S. government agencies, the need for standards and frameworks at scale is critical so the DevSecOps program follows best practices and remains auditable. In this area alone, there are many standards and frameworks to choose from, including NIST RMF, NIST 800-53, the NIST Cyber Security Framework, FedRAMP, CMMC, CNSSI, and HIPAA, the Department of Defense (DoD) DevSecOps Playbook, the DoD DevSecOps Reference Design, the Air Force Continuous ATO Playbook, the IEEE Standard for DevOps (IEEE 2675-2021), and others. Operationalizing is often achieved through some combination of these documents.

Rising to the challenge

Despite existing challenges, recent innovations in U.S. government agencies continue to catalyze the move toward Continuous ATO. Layered Compliance, for example, is an architectural construct that allows new applications to be built from pre-approved components. This process helps accelerate delivery time for custom applications. Additionally, novel solutions are being built on top of current tools to bring more insight and clarity to decision makers. These new tools take advantage of existing ATO software in order to offer new capabilities and services.

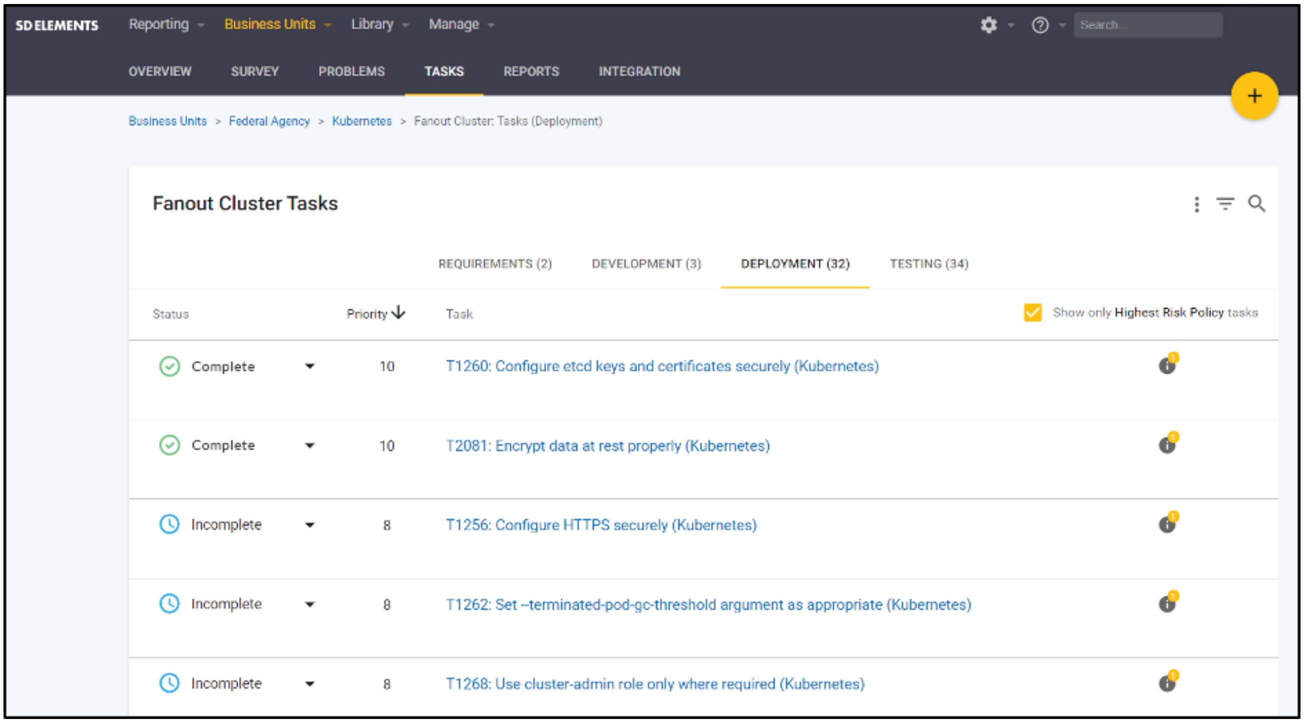
SD Elements provides a scalable solution in the early, mid, and AO reporting stages of an application.

Context sensitive

SD Elements helps streamline the software development process in the early stages by generating context-sensitive security requirements. The platform does this by using an adaptive and customizable survey that enables automated mapping of the current software application architecture to existing standards and frameworks. This mapping ensures that only applicable security requirements for the project are assigned to developers and non-applicable controls are removed. It also reduces the number of controls that need to be addressed by the engineering team for the application by using the inheritance tracking model for controls that are implemented in a higher layer.

Once context-sensitive security requirements are defined within SD Elements, integrations with issue tracking tools like Jira ensure consistent, program-level oversight across software development teams.

Figure 6: Contextual requirements in SD Elements



Business Units > Federal Agency > Kubernetes > Fanout Cluster: Tasks (Deployment)

Fanout Cluster Tasks

REQUIREMENTS (2) DEVELOPMENT (3) DEPLOYMENT (32) TESTING (34)

☑ Show only Highest Risk Policy tasks

Status	Priority ↓	Task
Complete	10	T1260: Configure etcd keys and certificates securely (Kubernetes)
Complete	10	T2081: Encrypt data at rest properly (Kubernetes)
Incomplete	8	T1256: Configure HTTPS securely (Kubernetes)
Incomplete	8	T1262: Set –terminated-pod-gc-threshold argument as appropriate (Kubernetes)
Incomplete	8	T1268: Use cluster-admin role only where required (Kubernetes)

RSA ARCHER® SUITE

servicenow

digital.ai

Azure

ca technologies A Broadcom Company

IBM

GitHub

GitLab

PivotalTracker by Pivotal

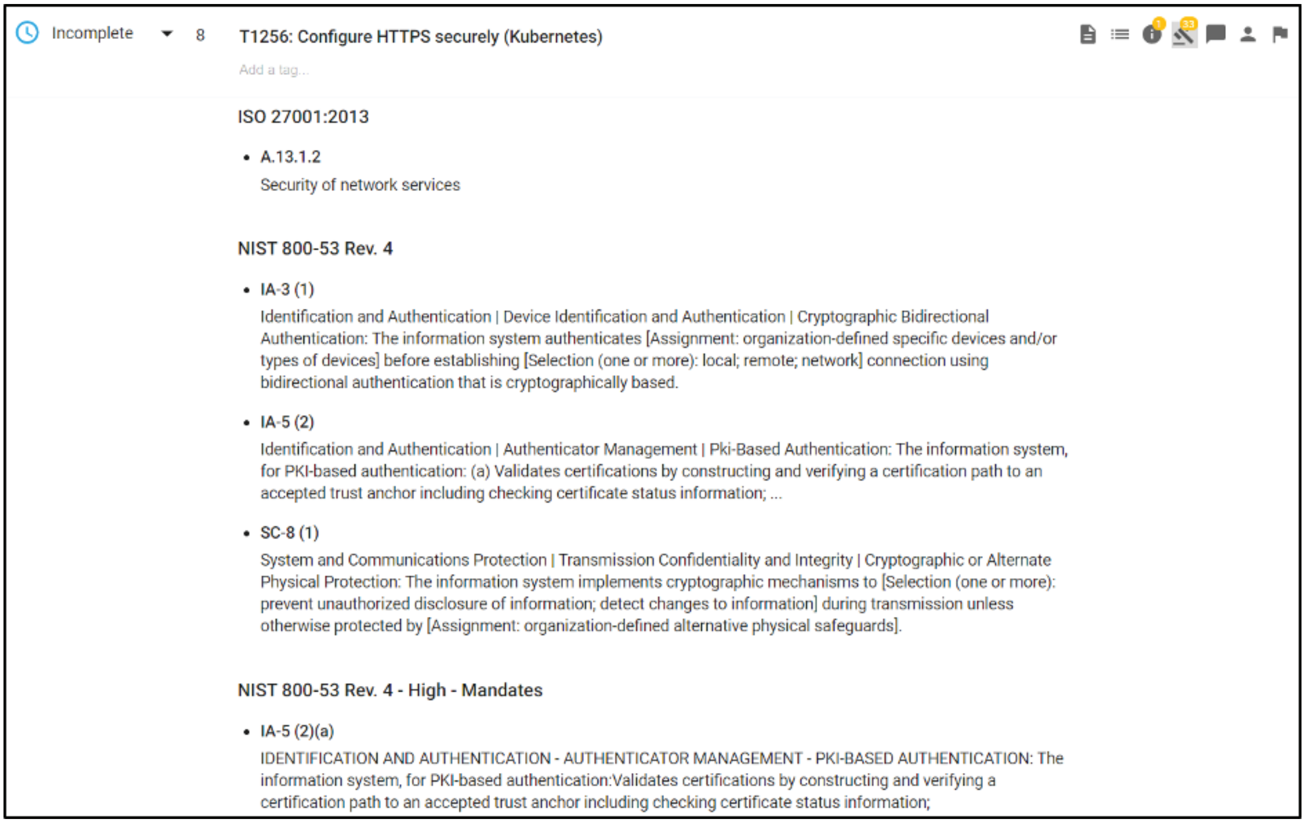
Jira Software

MICRO FOCUS®

Consistent, observable, traceable

In the past, it was common for software development teams to create security requirements tasks based on personal experience. This approach, however, lacks objectivity and consistency required for ongoing system resilience and trust. Measuring against an objective standard provides a baseline of consistent requirements. SD Elements provides the critical traceability of completed tasks against objective standards (developed by NIST, ISO, IEEE, and others) without reliance on subjective experience.

Figure 7: Traceability against objective standards



Incomplete 8 T1256: Configure HTTPS securely (Kubernetes)

ISO 27001:2013

- A.13.1.2
  Security of network services

NIST 800-53 Rev. 4

- IA-3 (1)
  Identification and Authentication | Device Identification and Authentication | Cryptographic Bidirectional Authentication: The information system authenticates [Assignment: organization-defined specific devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.
- IA-5 (2)
  Identification and Authentication | Authenticator Management | Pki-Based Authentication: The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; ...
- SC-8 (1)
  System and Communications Protection | Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection: The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].

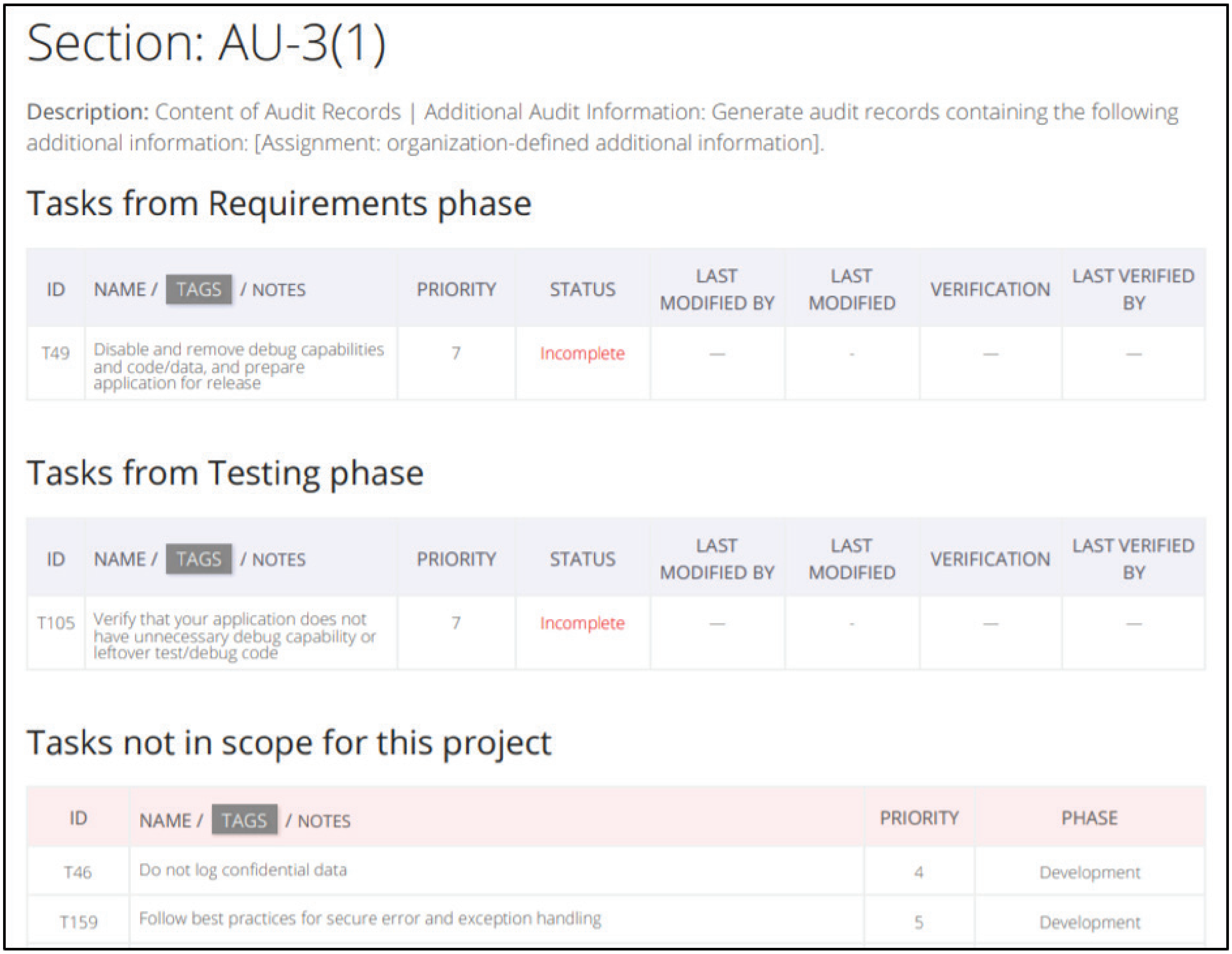
NIST 800-53 Rev. 4 - High - Mandates

- IA-5 (2)(a)
  IDENTIFICATION AND AUTHENTICATION - AUTHENTICATOR MANAGEMENT - PKI-BASED AUTHENTICATION: The information system, for PKI-based authentication:Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

Auditable

As requirements are implemented, reports can be generated to show the status of the security requirements and implemented controls against a standard. These reports can then be used to help demonstrate control compliance to the authorizing official. Compliance information is readily available at any time, with full traceability down into the individual project tasks related to the implementation of specific security controls.

Figure 8: Auditing and Reporting with SD Elementsw



Section: AU-3(1)

Description: Content of Audit Records | Additional Audit Information: Generate audit records containing the following additional information: [Assignment: organization-defined additional information].

Tasks from Requirements phase

ID	NAME / TAGS / NOTES	PRIORITY	STATUS	LAST MODIFIED BY	LAST MODIFIED	VERIFICATION	LAST VERIFIED BY
T49	Disable and remove debug capabilities and code/data, and prepare application for release	7	Incomplete	—	-	—	—

Tasks from Testing phase

ID	NAME / TAGS / NOTES	PRIORITY	STATUS	LAST MODIFIED BY	LAST MODIFIED	VERIFICATION	LAST VERIFIED BY
T105	Verify that your application does not have unnecessary debug capability or leftover test/debug code	7	Incomplete	—	-	—	—

Tasks not in scope for this project

ID	NAME / TAGS / NOTES	PRIORITY	PHASE
T46	Do not log confidential data	4	Development
T159	Follow best practices for secure error and exception handling	5	Development

Achieving ATO faster with SD Elements

SD Elements helps enable rapid or continuous ATO in U.S. government agencies by automating the identification, tracking, dissemination, and management of controls that map to U.S. federal government security and privacy controls. The capabilities required to manage a cross-functional security program at scale are built into the product, which allows U.S. government agencies to focus on rapid software development and innovation in support of mission objectives.

Looking ahead, there are two key challenges to consider. First, much of the current work around DevSecOps is based on cloud adoption and enablement strategies. As we enter into hybrid infrastructures that include IoT devices, the integration of these environments will pose a formidable challenge. Second, the cultural change required will be a significant effort. Moving from an annual routine to a daily routine will require a change in process and tools; reports with timely information need to be produced.

Despite these challenges, we remain optimistic that DevSecOps will continue to help the US Federal Government achieve its goal of reducing ATO timelines while balancing appropriate security earlier in the development lifecycle.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to build more secure software faster. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001