RegScale

E-BOOK

The Compliance as Code Blueprint

A Practical Guide to GRC Automation

Table of Contents

RegScale

> **With compliance as code, organizations can achieve continuous audit readiness with minimal overhead and continuously demonstrate compliance across their development lifecycle.”**

From the Desk of Our Co-Founder:

Why Compliance as Code is the Future

Anyone who’s managed enterprise compliance knows the drill: endless spreadsheets, manual audits, and last-minute scrambling to gather evidence before the deadline. Organizations are still spending countless hours on reactive processes instead of building better, more secure systems.

Compliance as code — i.e. automating compliance policies, controls, and audits by embedding them directly into your infrastructure and application code — offers a fundamentally different approach. With compliance as code, organizations can achieve continuous audit readiness with minimal overhead and continuously demonstrate compliance across their development lifecycle.

The benefits are significant: improved developer productivity, faster release velocity, real time compliance verification, and elimination of tedious manual processes. Compliance as code allows teams to shift-left both security and compliance, catching issues early in the development cycle when they’re cheapest and easiest to fix. Most importantly, by treating compliance as an engineering problem rather than a documentation exercise, businesses can finally break free from the burden of manual GRC.

In this eBook, we explain exactly how to shift your DevSecOps left, with practical steps for operationalizing compliance as code and enabling real-time insights into risk and compliance. We also demystify NIST OSCAL, share real-world success stories, and provide a roadmap for building continuously compliant systems.

The future of compliance isn’t more paperwork — it’s better code. Let’s build it together.

Travis Howerton
Co-Founder and CEO, RegScale

From Paperwork to Pipeline:

Compliance as Code Explained

What is compliance as code?

Instead of treating compliance as a pile of paperwork, compliance as code embeds your policies, controls, and audits directly into your infrastructure and application code.

- **The old way:** Manual spreadsheets, reactive audits, and scrambling for evidence around deadlines.
- **The new way:** Automated compliance checks in your CI/CD pipeline that catch issues before they become problems.
- **The result:** Build better applications, reduce security risks, spot vulnerabilities quickly, and resolve issues early, when they're cheapest to fix.

Reality check:
Our 2025 State of Continuous Controls Monitoring Report found that **only 46% of CISOs** have begun implementing compliance as code.

RegScale

How RegScale powers DevSecOps automation

Instead of treating compliance as a pile of paperwork, compliance as code embeds your policies, controls, and audits directly into your infrastructure and application code.

- **CI/CD integration:** RegScale acts as the policy holder and uses OSCAL and the SBOM to determine your compliance with your organizational requirements in real-time and flag issues.
- **Vulnerability management:** Through OCSF, SARIF, and direct integrations with Wiz, Tenable, Qualys, Snyk, and other leading security tools, we automatically capture asset and vulnerability information across your entire stack.
- **Intelligent automation:** Our automated workflows and integrations ingest relevant compliance data automatically, reducing manual errors.

Learn more about Continuous Compliance Automation in our Guide to DevSecOps Excellence.

What's OSCAL Got To Do With It?

The NIST Open Security Controls Assessment Language (OSCAL) standardizes the language of compliance into a machine-readable format.

- OSCAL makes it possible to automatically process the language used to document, implement, and assess security controls.
- With OSCAL, controls are expressed in machine-readable formats (XML, JSON, and YAML) so you can track changes in Git and feed them directly into your automation pipeline.
- OSCAL improves efficiency and consistency and enables continuous assessment.

As a scalable, standards-based way of conducting real-time, automated, full-lifecycle security assessments, OSCAL is positioned to be the compliance language of the future. Its ability to dramatically reduce manual paperwork and expedite continuous monitoring processes makes it a major benefit to GRC programs.

That's why we're founding members of the nonprofit OSCAL Foundation — and why our OSCAL-native platform supports the full OSCAL schema, including catalogs, profiles, security plans, components, SAP/SAR, and POA&Ms. The result is operationalized compliance as code for customers across industries.

How OCSF simplifies data exchange

Instead of relying on custom integrations for every tool, the Open Cybersecurity Schema Framework (OCSF) creates a common language for assets, vulnerabilities, threats, configurations, tickets, and much more — simplifying integrations and data sharing in continuous monitoring.

RegScale uses our integration platform and our industry-first OCSF-to-OSCAL translator to convert raw telemetry from ticketing systems, vulnerability scanners, SIEMs, and more into structured compliance outputs.

Shifting Left with Compliance as Code

Industry leadership in DevSecOps automation

- Founding members of the NIST OSCAL Foundation
- Fully OSCAL-native platform that enables compliance as code
- Named a Sample Vendor in the Gartner® Hype Cycles™ for I&O Automation, Site Reliability Engineering, and Cyber-Risk Management, three years in a row
- Named a Representative Vendor in the Gartner® Market Guide for DevOps Continuous Compliance Automation Tools, three years in a row

RegScale

Establish Baselines & Attest to Controls

Establish baselines

Bring in the relevant regulations, policies, and controls in machine-readable format (OSCAL).

Use OSCAL profiles to establish control baselines and associate mappings for operational efficiency.

Control attestations

Leverage RegScale's RegML AI to document your control implementations, and leverage OSCAL to publish machine-readable versions of your compliance policies to your existing DevOps tools to monitor and enforce.

40 hours saved per project
with automated SBOM integration

200 hours saved per quarter
by integrating compliance into the CI/CD pipeline

RegScale

Connect to Continuous Monitoring & Normalize

Continuous Monitoring

Leverage OCSF and APIs to pull run-time, operational data in near real-time. See how the systems and applications are executing and how they are secured into RegScale throughout the development life cycle.

Normalization

Leverage RegScale's data processing engine with native support for OSCAL, OCSF, and SBOM (Software Bill of Materials) to create a baseline of your compliance and risk posture. Use RegScale to understand trends in your risk and compliance over time and make business decisions based on the most up-to-date information.

RegScale

Assess & Shift Left

Assessment

Validate completeness and quality in minutes, then publish assessment and issue artifacts in OSCAL to assess against your organization's business rules and organizational risk tolerances. Respond to regulatory requests faster and more consistently and stay always audit ready.

Shift Compliance and Security Left

Leverage the SBOM to monitor every software build as it progresses through your CI/CD pipelines with full visibility of your risk and compliance posture from start to finish, code to cloud. Achieve faster fixes, minimize your risk and threat exposure windows, accelerate development velocity, and improve the quality of code.

$100k/month saved for a client
by implementing compliance as code
within a federal software factory

RegScale

Spotlight

How Our Telecom Customer Leveraged Compliance as Code

- **The Challenge:**
  A global telecommunications company was struggling with scattered tools and compliance blind spots. They needed to streamline their response to audits and implement a scalable standardized process across their DevOps tools.

- **The Solution:**
  By using RegScale to integrate policy/compliance as code into their CI/CD pipeline, the company was able to introduce increased consistency and visibility across DevOps programs and throughout the software development life cycle.

- **The Results**
  The company can now find and remediate compliance and vulnerability issues sooner in the software development process, minimizing delays and increasing both the quality and velocity of software delivered to customers.

$1.8M and 2,000 person hours saved in the first year

Read the Full Details Here

RegScale

Shifting Left with RegScale

RegScale's platform integrates compliance as code into DevSecOps processes to demonstrate compliance requirements across the product development and delivery lifecycle stages with:

- An OSCAL-native platform to enhance security and ensure compliance throughout the product development lifecycle
- An AI-driven platform that ingests data via OCSF or APIs and maps to controls, identifies issues, and tracks through resolution
- Intelligent automation and workflows that offer unmatched visibility and accountability across the entire organization
- Continuously updated documentation to eliminate friction and error-prone manual changes and keep you always audit-ready

RegScale

Ready for the compliance as code advantage that you've been missing?

Let's get started.

Visit RegScale.com to learn more.

Sales@RegScale.com

RegScale.com