RegScale

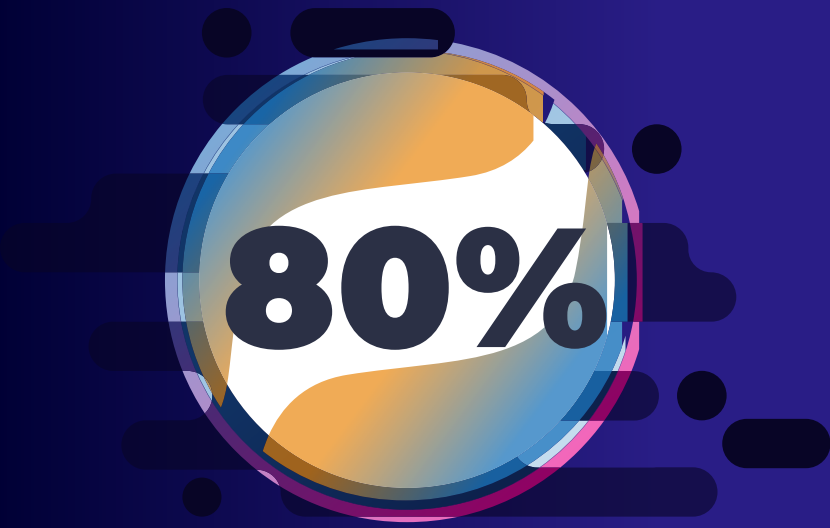
E-BOOK

Demystifying Continuous Compliance Automation

Your Guide to DevSecOps Excellence

TABLE OF CONTENTS

RegScale



of CISOs see automation as key to reducing the burden of manual processing in their compliance and risk management programs

FROM THE DESK OF OUR CO-FOUNDER

THE COMPLIANCE CRISIS

Over the last few years, I've watched the regulatory landscape become increasingly complex — and the costs of manual compliance skyrocket. Companies are stuck in spreadsheet hell and drowning in documentation demands that grow more burdensome and costly each year. It's unsustainable.

These regulatory challenges are compounded by siloed processes that create dangerous blind spots. When IT, development, security, and compliance teams operate in isolation, we see the risks rise for failed audits, costly breaches, regulatory fines, and reputational damage.

Traditional compliance methods — the ones that rely on point-in-time assessments and manual documentation — just can't keep pace anymore. Reactive approaches are leaving companies perpetually behind the compliance curve.

The good news? There's a better way forward. In our industry-first 2025 State of CCM Report, we found that **80% of CISOs** see automation as key to reducing the burden of manual processing in their compliance and risk management programs.

This e-book dives into the topic of GRC automation, exploring how forward-thinking businesses are implementing Continuous Compliance Automation to slash costs, reduce risk, and transform compliance from a burden into a competitive advantage. We hope you'll find it a useful guide for your automation journey.

Travis Howerton
Co-Founder and CEO, RegScale

WHAT IS CONTINUOUS COMPLIANCE AUTOMATION?

Continuous Compliance Automation (CCA) is the practice of embedding automated compliance processes directly into your CI/CD pipelines and DevSecOps workflows. Rather than scrambling to prepare for audits or rushing to meet regulatory requirements at the last minute, CCA ensures that your systems, applications, and processes remain compliant in real time.

THE TECH SPECS

CCA leverages standards like the NIST Open Security Controls Assessment Language (OSCAL) and the Open Cybersecurity Schema Framework (OCSF) to streamline automation and enable compliance as code. As a founding member of the OSCAL Foundation, RegScale is committed to advancing compliance as code across industries.

RegScale

Top Benefits of CCA

- ✓ Reduce costs
- ✓ Lower risk and improve accuracy
- ✓ Remove compliance bottlenecks
- ✓ Maintain an always audit-ready posture
- ✓ Accelerate go-to-market plans with faster delivery of products and services
- ✓ Get real-time visibility into compliance status across frameworks
- ✓ Operate at the speed of innovation

The Intersection of CCA and DevSecOps

- Brings together development teams, security professionals, and GRC professionals.
- Use automated tools and processes to verify compliance requirements throughout the entire software development lifecycle.
- Move teams toward proactivity and away from manual, reactive compliance tasks.

This is also known as a “shift left” strategy:

addressing compliance requirements from the start of the development process rather than treating them as an afterthought.

RegScale

Shifting Left:
How To Add Compliance to Your DevSecOps Pipeline

INDUSTRY-LEADING CCA CAPABILITIES

RegScale has been named a Representative Vendor in the Gartner® Market Guide for DevOps Continuous Compliance Automation Tools three years in a row: 2023, 2024, and 2025.*

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

We wrote the code on compliance. **Literally.**

Leverage RegScale's deep expertise in compliance as code, built on years of hands-on practice and our founding membership in the OSCAL Foundation.

RegScale

Step 1:

Integrate Compliance Checks into Your CI/CD Pipeline

- ✓ Implement automated compliance scanning in your build process to identify and address compliance issues before they reach production.
- ✓ Leverage compliance as code to set up gates at key deployment stages and keep code from moving forward in your pipeline.
- ✓ Create automated feedback loops to immediately notify developers about compliance issues, enabling rapid remediation without disrupting workflows.

RegScale

Step 2:

Automate Evidence Collection and Documentation

- ✓ Leverage compliance as code to enable continuous monitoring of security controls and automatically collect compliance evidence.
- ✓ Set up automated artifact generation to transform collected data into audit-ready documentation without manual effort.
- ✓ Establish real-time compliance dashboards to gain visibility into compliance status across the organization.
- ✓ Integrate existing security and compliance tools through APIs to create a unified GRC ecosystem.

Automation in Action: **FedRAMP High**

We used our own platform to automate critical parts of our FedRAMP High journey. *The result?*

- ✓ **410+ control implementation statements** in **2 weeks** instead of the standard **12-16 weeks**
- ✓ **3-4x faster timeline** for authorization
- ✓ **50% less cost** than average

RegScale

10X your operations with AI

Our RegML AI model boosts automation and eliminates manual work with:

- ✓ **AI Explainer,** offering detailed explanations of complex controls in context
- ✓ **AI Author,** drafting control implementation statements and automatically deriving compliance documentation from updates
- ✓ **AI Auditor,** boosting control documentation **accuracy by 80%**

Step 3:

Transform and Scale

- ✓ Assess once and apply across many standards and 70+ frameworks through cross-mapping.
- ✓ Establish automated cross-framework reporting that satisfies multiple regulatory requirements with a single set of evidence.
- ✓ Maintain always audit-ready status through real-time dashboards and reporting.
- ✓ Ensure consistent monitoring of compliance policies throughout the software development lifecycle by embedding compliance as code into CI/CD pipelines.

RegScale

SUCCESS STORY

GLOBAL TELECOMS COMPANY

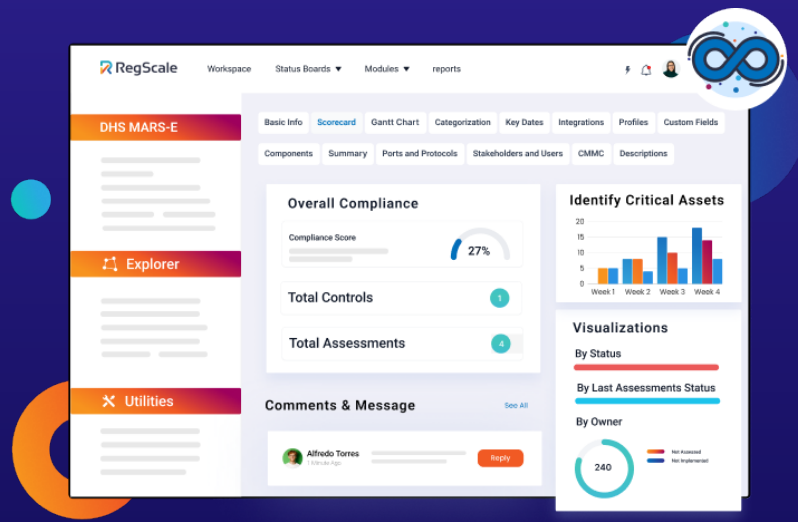
A global telecommunications organization wanted to gain increased visibility and accountability throughout their software development life cycle. The company implemented RegScale's DevSecOps CCA platform to enable consistent application of metrics, KPIs, and runbooks and to improve the overall quality and velocity of code produced.

- ✓ **Policy/compliance as code within CI/CD tooling —** To identify compliance and vulnerability issues sooner in the company's software development process and fix the issues faster, with less impact on the delivery of software.
- ✓ **Embedding compliance into the DevSecOps pipeline —** Enabling the company to apply consistent metrics, KPIs, and runbooks across regulatory frameworks and compliance programs.
- ✓ **Executive and operational dashboards and reports —** For a single, real-time view of security and compliance.
- ✓ **Integrating CCA into the heart of development and compliance processes —** To increase the velocity and improve the quality of software delivered and to provide faster, more secure applications for their customers.

RegScale

A Proven Approach to **Continuous Compliance Automation**

RegScale's CCA platform transforms DevSecOps, helping you maintain velocity while shifting left.



- ✓ Uses OSCAL-native architecture to seamlessly embed compliance as code in your CI/CD pipeline.
- ✓ Ensures code is compliant from initial development through deployment.
- ✓ Replaces manual processes with real-time intelligent workflows.
- ✓ Centralizes and automates your vulnerability management, response, and reporting.
- ✓ Proactively monitors compliance and mitigates risks.

Download the one-pager
to learn more about RegScale's CCA offerings

RegScale

Ready to start **shifting left?**

Let's get started.

Visit RegScale.com to learn more.

Sales@RegScale.com RegScale.com