RegScale

Powering Your Journey to Continuous Compliance and Continuous ATO

Does your organization want to lower compliance costs, reduce the risk of audit failure, and deliver audit-ready compliance documentation on demand?

Do you want to accelerate your FedRAMP or NIST/FISMA paperwork and processes to achieve a continuous Authorization to Operate (cATO)?

With the right strategy and technology, you can automate, transform and scale your compliance program to shift compliance left – and achieve continuous compliance.

Table of Contents

The Challenges of Compliance

Compliance data is literally everywhere, especially for organizations in highly regulated industries such as finance, energy and government. Organizing all that information into a set of artifacts and evidence that can be used to pass an audit and achieve a FedRAMP or NIST/FISMA Authorization to Operate (ATO) is an intense, largely manual effort. Manually applying that documentation to multiple regulatory frameworks becomes exponentially challenging. (See Figure 1.)

These challenges are exacerbated by additional factors, depending on role:

- For information assurance and internal audit, processes are highly paper-based, with evidence contained in structured and unstructured formats. Teams are saddled with a nonstop effort to manually copy and paste data from one system to another. The workload is growing and must be handled by a limited number of staff with equally limited budgets.
- For the vice president of risk and compliance or chief information security officer (CISO), nonstop external audits disrupt operations and distract from strategic focus. Growing regulatory burdens and rising fines and penalties for violations continually raise the stakes. Meanwhile, separate artifacts must be developed for every regulation, slowing responsiveness and hindering efforts to carve out time for proactive risk management.
- For the chief information officer (CIO) and owners of the lines of business (LoBs), regulations differ across regions and locations, while each business unit juggles multiple systems of record. This lack of consistency and standardization makes compliance hard to achieve and threatens business success.

For startups and small businesses, the challenges of compliance drive up costs to hire lawyers, accountants and subject-matter experts. They also create barriers to market entry, making it difficult to grow business.

For midsize and large enterprises as well as government agencies, the challenges of compliance produce a status-quo culture that resists change. Embedded risk aversion coupled with inefficient but ingrained processes results in cultural barriers to digitization, automation and business expansion.

But what if there were a better way to do compliance? What if you could integrate and simplify compliance processes – enabling compliance teams to work more efficiently and effectively, while empowering compliance decision-makers with real-time insights and actions? What if you could deliver audit-ready compliance documentation on demand and reduce the risk of audit failure and the subsequent fallout — all while lowering compliance costs? (See Figure 2)

FIGURE 1

Manual, Reactive Compliance Processes

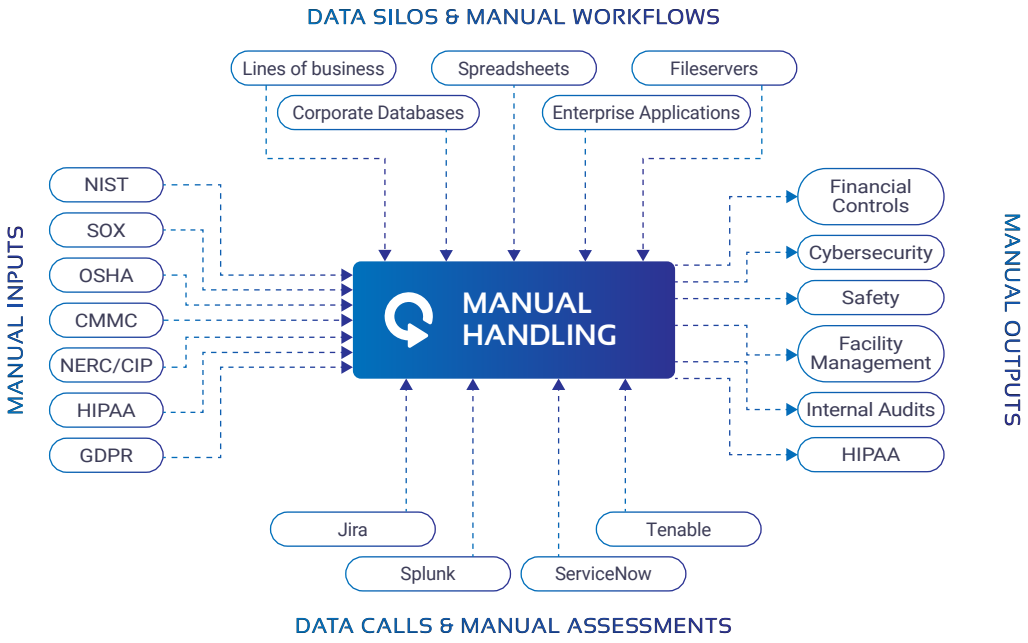
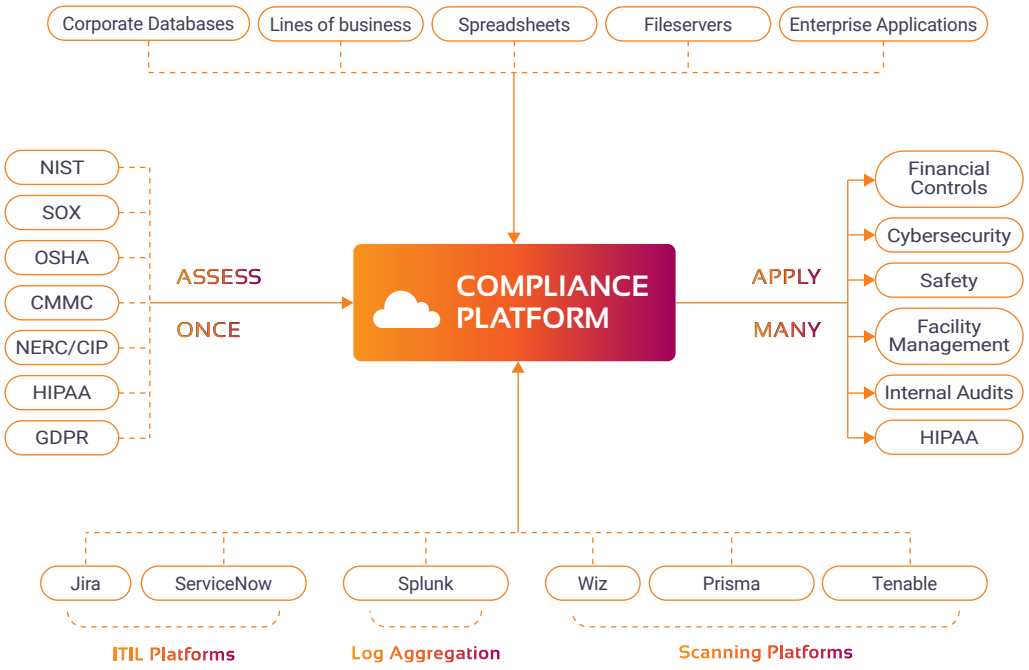


FIGURE 2

Continuous Compliance



6–10% Of revenue is spent on compliance costs at nearly 50% of banks surveyed by ABA[1]

A Better Way to Do Compliance

There's a better way to do compliance, and it's achievable today. To realize this goal, organizations need to:

- **Digitize –** Put in place tools that standardize and accelerate compliance processes.
- **Automate –** Make compliance assessments accurate and automatic where applicable, freeing up decision-makers to focus on the compliance steps that need to remain manual and expert-based, all logged into a system of record.
- **Transform –** Implement the technology and strategies that transform your compliance practice and drive cultural change throughout your organization.
- **Scale –** Extend your compliance strategy across the enterprise, with consistent but tailored approaches that meet the needs of every business unit and LoB.

The good news is that many compliance functions have already embarked on this process through digitization. More systems, data sources and workflows have been digitized, creating a foundation for automation and improvement.

An effective compliance platform can further advance your digitization efforts through:

- **Wizards and builders –** Replace copy and paste with a guided approach to easily create compliance artifacts.
- **A compliance "concierge" –** Apply turnkey onboarding of existing compliance artifacts into a compliance platform to avoid repeated tasks.
- **Rapid time to value –** Quickly and cost-effectively deploy compliance platforms in any environment — on-premise, in the cloud or in an air-gapped environment — with the ability to achieve real return on investment measured in weeks as opposed to years.

The next step is to truly automate, standardize and transform compliance effectiveness across the enterprise. Achieving that goal calls for four inter-related strategies:

1. Start compliant by shifting compliance left.
2. Embrace a RegOps methodology.
3. Drive cultural transformation.
4. Achieve continuous compliance.

The Tangible Benefits of Continuous Compliance

A growing number of forward-looking organizations are advancing on their journey to continuous compliance – and achieving real-world results in the process.

Business-enhancing outcomes include:

CONSOLIDATION AND AUTOMATION

Lower complexity and cost for managing compliance, with simplified system integrations and more predictable milestones.

SIMPLIFIED EVIDENCE GATHERING AND COMPLIANCE PROCESSES

Eliminate compliance headaches and become more proactive in your compliance management. Meet stringent compliance requirements and deliver audit-ready NIST/FISMA/FedRAMP paperwork on demand and achieve a cATO for federal government agencies.

REAL-TIME, ON-DEMAND INSIGHTS

Deliver accurate information around the state of compliance to the decision-makers who need it, when they need it, with greater assurance you're consistently taking the right actions at the right times.

GREATER TRANSPARENCY AND CONTROL

Progress from intermittent knowledge to continual understanding and assured accountability allowing your programs to always be "audit ready".

FASTER RESPONSE, REDUCED RISK

Replace frantic reaction to audit events with proactive, continuous compliance for lower overall risk and gain a greater ability to respond to business opportunities.

$14.8M vs. $5.47M

Annual cost of non-compliance to businesses on average compared to compliance costs[2]

Beyond Digitization: Shifting Compliance Left

Till now, organizations that have invested budget, time and effort in digitizing compliance processes have failed to realize optimum returns on those investments. The problem is twofold: Compliance elements that have been digitized are still largely disconnected, and compliance workflows that have been digitized are still interrupted by too many manual steps.

The way to move beyond mere digitization is to adopt a concept from cybersecurity, which is "shift left." In cybersecurity, shifting left means refocusing security efforts earlier in the event chain, well before a data breach occurs. Instead of reactively remediating after a security incident, you proactively put security measures in place to prevent an incident from occurring.

Ideally the shift left occurs early in application development, where security can be built in from square one. This concept is the impetus behind DevSecOps – development, security and operations – allowing these different organizations to work together seamlessly thereby rendering security as near real-time, continuous and complete as possible.

Compliance teams need to achieve a similar objective, advancing compliance as early in the process as possible, well before an audit event. That means digitizing and automating regulatory inputs, evidence gathering, and outputs and reporting to achieve an always audit-ready business posture. (See Figure 3.)

The solution is an entirely new concept in compliance management: Regulatory Operations (RegOps). RegOps applies an integrated portfolio of digital tools, best practices and compliance culture to ensure the compliance of applications and services against regulatory standards at high velocity. RegOps evolves compliance and trust at a measurably faster pace than organizations stuck in manual artifact development and traditional compliance management.

For government agencies and the IT providers that serve them, RegOps can also help automate and deliver a continuous Authorization to Operate (cATO) under the Federal Risk and Authorization Management Program (FedRAMP) or the NIST Risk Management Framework (RMF).

FedRAMP is the government initiative that specifies a methodology for security assessments, authorizations and ongoing monitoring of government-operated and commercial cloud products and services. ATO is the authorization by a senior agency official to operate an IT system, based on NIST's RMF. By many estimates, it can take a year or more to get an ATO, though several former officials at the National Geospatial Intelligence Agency (NGA) have posited that we should be aiming for the ATO process to take just one day to match the speed of the mission.

Achieving "continuous" ATO requires ensuring compliance with security and risk management frameworks on a real-time basis.

RegOps can help agencies and IT providers to achieve and even automate cATO by making sure compliance is actually built into the process, not bolted on later.

RegOps becomes achievable with an effective compliance platform. Such a platform delivers the capabilities you need to shift left, enabling:

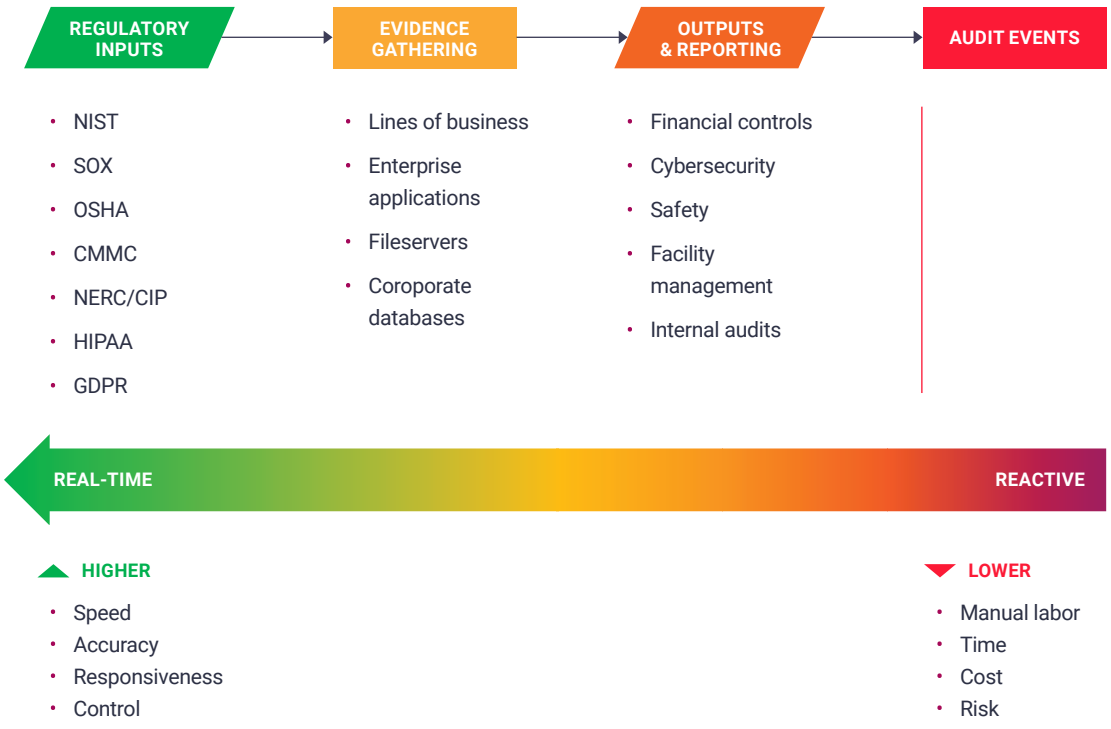
- **Up-to-date understanding –** Keep documentation up to date through API integrations and automation, with little or no manual effort.
- **Proactive stance –** Maintain an always-ready audit posture through integrations with security platforms and analytics that provide actionable insights into compliance risk.
- **Real-time action –** Gain holistic visibility into your state of compliance through real-time dashboards that empower you to take the right actions at the right times.

US $401M

Cost of a mega breach (50-66M records) on average[3]

FIGURE 3

Shifting Compliance Left



Welcome to RegOps and Automation

RegOps is a new concept that puts in place the methodology and technology to achieve true compliance automation, in the same way DevOps automates and accelerates development and operations.

A key DevOps concept is "CALMS":

- **Culture –** Embrace responsiveness and change.
- **Automation –** Ensure repeatability and reliability.
- **Lean –** Eliminate unnecessary manual tasks.
- **Measurement –** Track effectiveness.
- **Sharing –** Work together toward the same goals.

Applying these DevOps concepts to compliance means leveraging the same kinds of technologies, processes and techniques in compliance that have proved successful in IT operations. Any activity that's highly repetitive is automated to make the compliance team more efficient and effective. Compliance teams and decision-makers benefit from complete, accurate information at a lower cost, enabling them to make proactive, risk-based decisions and address small problems before they become major issues.

Key DevOps technologies that apply to RegOps include:

- **APIs –** Interconnect systems with modern representational state transfer (REST) APIs to self-attest to the state of compliance in near real time.
- **Scripting/DevOps –** Connect APIs with custom scripts such as Ansible playbooks and other mechanisms to provide low-cost, bespoke integrations based on unique needs.
- **Continuous integration and continuous delivery (CI/CD) –** As new systems are developed or existing systems are modified, tools attest to the state of compliance in real time.
- **IoT –** IoT sensors provide the ability to monitor systems and deliver data to attest to the state of compliance for physical systems and non-traditional IT systems.

RegOps Manifesto

RegScale is creating more than just software. We are starting a compliance movement that is based on a set of well-defined principles that establish a new discipline known as RegOps. RegOps is the combination of cultural philosophies, practices and tools that increases an organization's ability to ensure compliance of applications and services against regulatory standards at high velocity: evolving and improving compliance and trust at a faster pace than organizations using traditional compliance artifact development and compliance management processes.

THE REGOPS MANIFESTO IS:

1. Regulations exist to maintain our privacy while keeping us safe and secure – we should honor them.
2. Maintaining compliance as a business should be affordable, transparent, and easy.
3. Compliance processes that are boring and repetitive should be automated – it is good for the business, good for the regulator, and good for the employee.
4. Audits should be simpler and less risky for the business.
5. Evidence should always be readily accessible and as near real-time as possible.
6. Producing high quality compliance artifacts should be more profitable for the producer while consuming these same artifacts should be cheaper for the consumer – driving mutually beneficial incentives.
7. Technology will change over time, so any solutions must be extensible to take advantage of future innovations and minimize technical debt for the future.
8. Getting started with compliance should be free with the goal of pulling out costs and accelerating business.
9. We should build on industry compliance standards while accelerating their adoption.
10. Do no harm – if the solution doesn't improve privacy, safety and/or security, we should not do it.

Crucially, RegOps promotes handoffs between cybersecurity and operations when cyber issues are detected.

This integration enables cyber assurance and engineering teams to collaborate in automated workflows. As cybersecurity grows even more essential to overall compliance and risk management, bringing together compliance and cyber teams will be increasingly necessary.

Just as important, RegOps doesn't only improve automation. It also optimizes any compliance workflows and decision-making that of necessity must remain manual and expert-based. By combining the strengths of both machine and human performance, RegOps lays the groundwork for continuous compliance.

17%

Increase in data breaches in the first three quarters of 2021 compared to all of 2020[4]

4 weeks to 18 months

Needed to complete the SOC 2 reporting process based on project complexity and organization maturity.[5]

Success Story: Fortune 100 Financial Institution

An innovative Fortune 100 financial services organization wanted to move its compliance documentation out of spreadsheets and into a compliance system of record.

Leveraging a sophisticated compliance platform, the organization achieved continuous compliance automation, implementing:

DIGITAL CATALOGS

Catalogs for Enterprise Risk Management (ERM)-IT, Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, and New York State Department of Financial Services Cybersecurity Regulation (NYDFS)

RISK ASSESSMENTS

New features for lightning assessments and overall audit tracking

SECURITY AND TRACKING INTEGRATIONS

Integration with Wiz (Cloud Security Posture Management) and Jira (Ticket Management) to push and pull compliance information across systems and auto-assign remediation tickets

DYNAMIC REPORTS

Near real-time Board reports in Tableau as opposed to reports manually created in Microsoft PowerPoint to dynamically reflect the state of compliance across the enterprise

---

The organization now has the visibility and automation it needs to shift compliance left and enable continuous compliance.

Transform to Enable Cultural Change

Another key element of RegOps is a concept we call "bring your own mapping" (BYOM). With the right technology, you can apply outputs across all your standards and frameworks.

After all, many organizations create their own mappings against multiple compliance frameworks. Industry-accepted authoritative sources include the Cloud Security Alliance's Cloud Controls Matrix (CCM). By plugging your preferred mappings into your compliance platform, you can create an assessment package against one standard and then apply it to any other mapped standard.

62%

Of compliance pros expect more compliance involvement in cyber resilience[6]

To this end, an effective compliance platform should include foundational capabilities such as:

- **Control compatibility –** Best-in-class support for digital tools such as NIST's Open Security Controls Assessment Language (OSCAL) to automate compliance checks and output documentation in a standardized machine-readable language.
- **"Transformer" capability –** Drag-and-drop mapping allows you to reuse artifacts from one framework to another in real time. You reduce the burden of manual compliance with multiple regulations, all while leveraging the same evidence and audits.

With a complete compliance platform, you can define each regulatory requirement, and identify the specific, relevant control. You can achieve outputs in both machine- and human-readable formats and you can apply those outputs to compliance, cybersecurity, internal audit and more.

With RegOps, automation and proactive compliance in place, you're now positioned to transform your compliance and your culture.

You can move beyond repetitive, rote work across multiple standards to assess-once, apply-many reuse. You can progress from last-minute audit prep and self-assessments to a real-time, always-prepared compliance posture. And you can transform from constant compliance remediation to business-enabling discussions about true risk management.

Ultimately, you can work smarter, remain audit-ready and make sound risk decisions. (See Figure 4.)

FIGURE 4

Shift-Left Compliance Transformation

Success Story: Government Contractor

A successful government contractor sought to achieve real-time visibility into Cybersecurity Maturity Model Certification (CMMC) control assessments and related issues. It implemented a robust compliance platform to realize continuous compliance automation.

Integrations with Prisma (Cloud Security Posture Management) pull scan results into the compliance solution as assessments. Automated ticket creation in ServiceNow (Ticket Management) assigns engineers to address open issues. A complete security scorecard enables decision-makers to holistically visualize control status and an associated compliance score.

The company now has the capabilities it needs to meet objectives for greater compliance insights and control across the enterprise.

Scale and Achieve Continuous Compliance

Shift-left compliance — via a RegOps methodology and built on a complete, cost-effective compliance platform — gives you the foundation to scale across your enterprise. You can deploy compliance automation and achieve compliance transformation across every business unit, for every regulation and standard you need to meet, and for every regulatory framework you manage.

A robust compliance platform enables scale and continuous compliance through two key mechanisms:

- **Autonomous business intelligence –** Each business unit and LoB should be able to use the business intelligence engine of its choice to visualize risk and compliance in real time, without the need for manual reporting and without compromising the original data source.
- **Multi-tenancy architecture –** You should be able to stand up tenants for each business unit, enabling consolidation of tools while allowing business units the freedom to execute their own unique processes. Compliance teams and decision-makers can easily access dashboards and reports for each stakeholder group, without having to manually seek out multiple data sources. Each group can maintain its own workflows, data schemas and application modules, optimized for their specific requirements – and all without the need for custom development.

You have now achieved true, continuous compliance. Continuous compliance means:

- ✓ You capture regulatory inputs across key regulations that apply to your business such as NIST, SOX, OSHA, CMMC, NERC/CIP and others.
- ✓ You leverage digitized workflows to gather information from enterprise applications, corporate databases and other data streams.
- ✓ You benefit from API integrations with enabling technologies such as Jira, Tenable, Splunk, Wiz and ServiceNow.
- ✓ You assess once and then apply in a repeatable manner to all your compliance frameworks across financial controls, cybersecurity, internal audits and more.

A Proven Approach to Continuous Compliance

RegScale offers an innovative, cost-effective platform for achieving continuous compliance. RegScale is the only solution that holistically manages compliance programs at scale.

In order to benefit from these capabilities, you need to:

- **Digitize –** Save time and reduce risk by moving your compliance artifacts into a digital system of record.
- **Automate –** Integrate your existing security and compliance tools to keep compliance documentation continuously up to date.
- **Transform –** Assess once and use across many standards and frameworks, with output in both human- and machine-readable formats.
- **Scale –** Deploy in any environment with tenants for every business unit, plus enterprise reporting across the organization in your business intelligence platform of choice.

With RegScale, you gain a proven platform that equips you to shift compliance left, adopt a RegOps methodology, drive compliance cultural change, and scale continuous compliance throughout your organization.

Your organization can proactively demonstrate compliance with any compliance standard or framework including NIST, SOX, OSHA, CMMC, NERC/CIP, HIPAA, GDPR, and over 70 other key regulations available out of the box (and growing!). You can likewise deliver audit-ready, on-demand system security plans (SSPs) and achieve a FedRAMP and NIST/FISMA continuous Authorization to Operate (cATO).

Contact RegScale today to begin realizing continuous compliance in your organization:

SCHEDULE A LIVE DEMO

Get your questions answered by our world class compliance professionals.

Schedule a Live Demo

PURCHASE ENTERPRISE EDITION (EE)

Learn about our deployment options for enterprise customers.

Contact Us

DOWNLOAD COMMUNITY EDITION (CE) FOR FREE

Download and install RegScale CE to get started for free.

Download Container

PLAY IN REGSCALE SANDBOX

Play for free in our cloud sandbox to get hands-on experience with no obligation.

Request Account

RegScale experts have the knowledge, experience and proven track record to help you achieve continuous compliance in your organization.

ANIL KARMEL, CO-FOUNDER AND CEO

Anil was previously deputy CTO of the National Nuclear Security Administration (NNSA). He has served as a technical staff member of Los Alamos National Laboratory (LANL), where he developed the organization's cloud and collaboration technologies. Anil and his team have garnered such accolades as the SANS National Cyber Security Innovators Award for Cloud Security, InformationWeek 500 Top Government IT Innovators, ACT-IAC Excellence.gov Award, and the DOE Secretary's Achievement Award. Anil is president of the Cloud Security Alliance's Washington DC Metro Area Chapter and a member of the CSA's CxO Trust Advisory Council.

TRAVIS HOWERTON, CO-FOUNDER AND CTO

Travis has held executive leadership roles in some of the largest public and private sector IT organizations in the United States. He served as CTO and Cyber Sciences Lab director at NNSA, as well deputy director, Information Technology Services Division, at Oak Ridge National Laboratory (ORNL). At Bechtel Corp. he held senior positions related to transformation and global strategic programs. With more than 20 years of experience delivering "no fail" missions, he is a winner of the Fed 100 Award and the ACT-IAC Award for Most Innovative Project in Government. Travis holds a Master of Science degree in Computer Information Systems from Boston University and maintains PMP, ITIL, CISSP and Harvard Credential of Readiness certifications.

Appendix

1 "2nd Annual Bank Survey" Risk Management Association, 2018

2 "True Cost of Compliance with Data Protection Regulations" HIPAA Security Suite, March 2020

3 "Cost of a Data Breach Report," IBM, July 2021

4 "ITRC 2021 Q3 Data Breach Analysis," Identity Theft Resource Center, September 2021

5 "What is SOC 2 Compliance?," Office1, July 2021.

6 "Cost of Compliance 2021: Shaping the Future," Thomson Reuters, 2021


RegScale