RegScale

CUSTOMER LOGO HERE

Continuous Controls Monitoring:
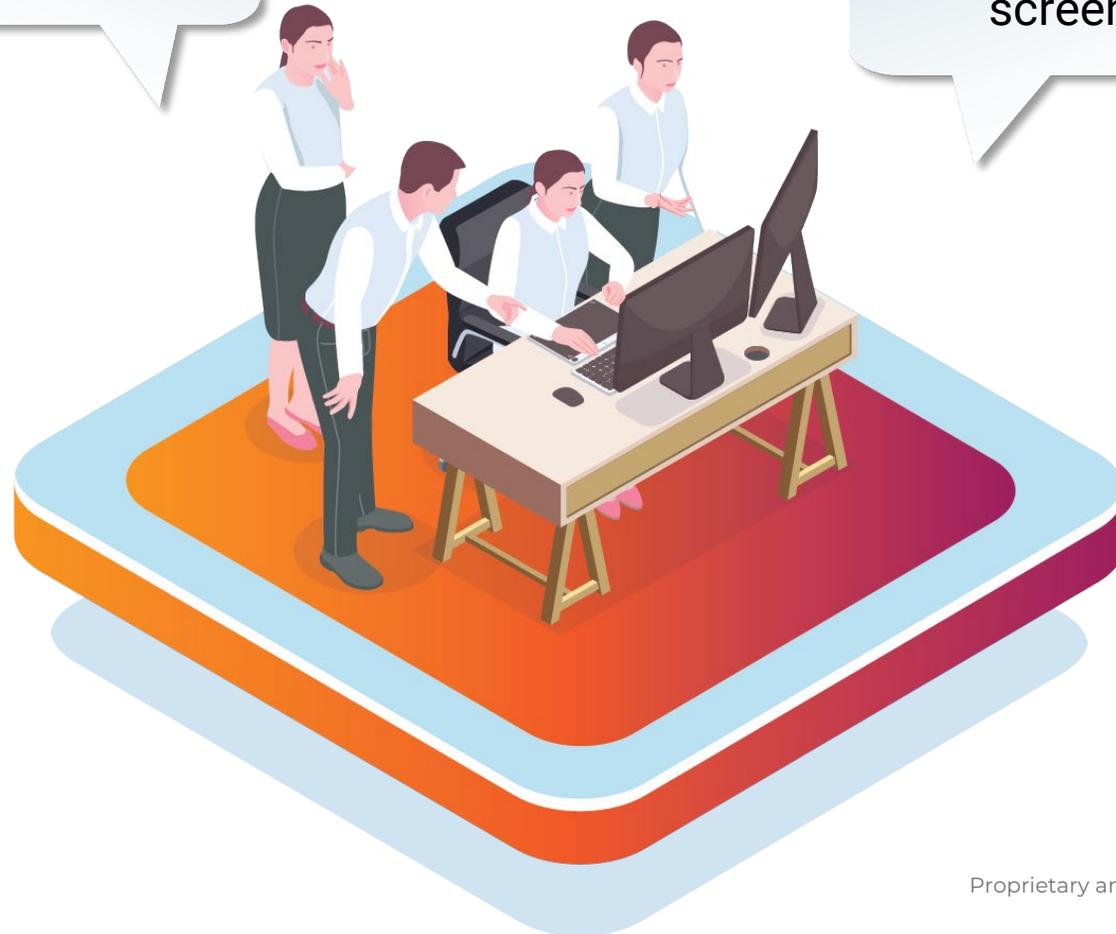## Faster, Budget-Friendly, and Always Audit-Ready

Name of Presenter

Data Dead Ends

Visibility Blackouts

Decision Blind Spots

Slow Response Ahead

Strategic Wins

90%

Reduction in effort to complete SOC 2 Type 1

Automation Pays

60%

Reduction in audit prep & response time

Visibility Victories

30%
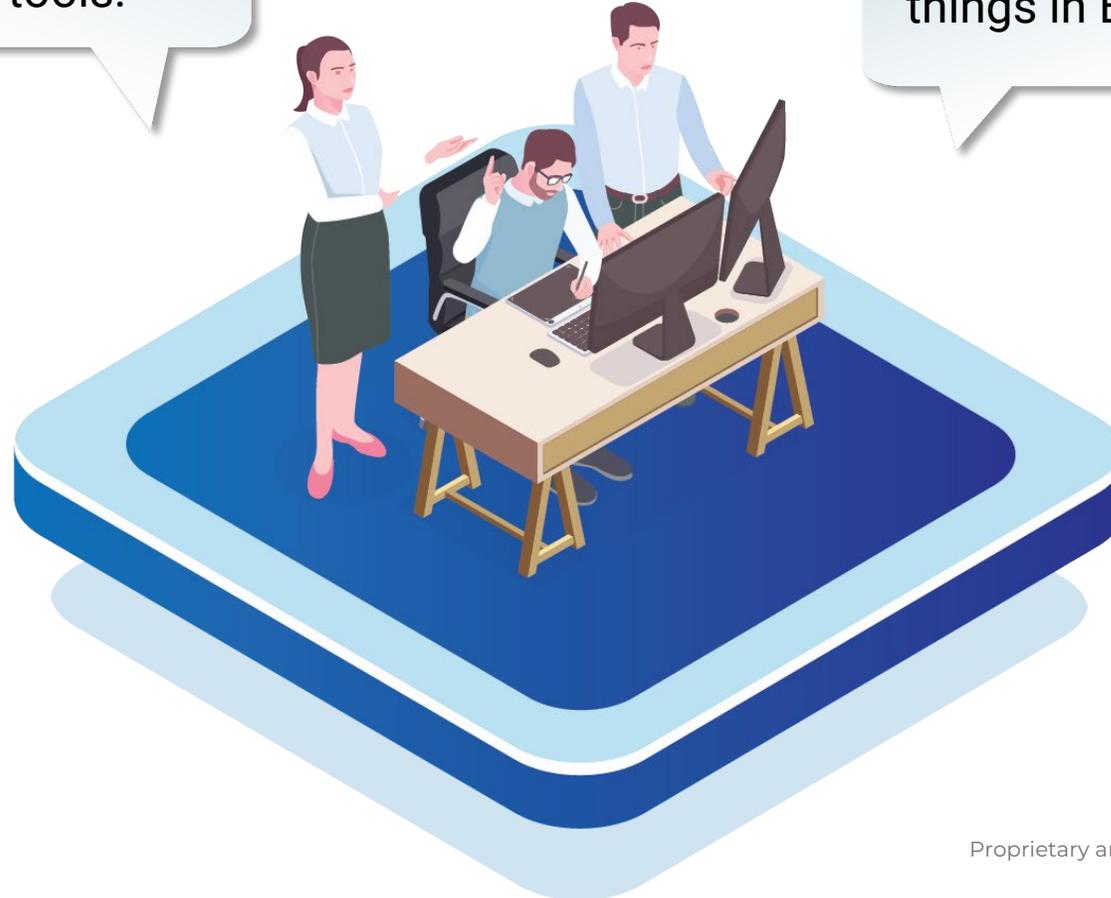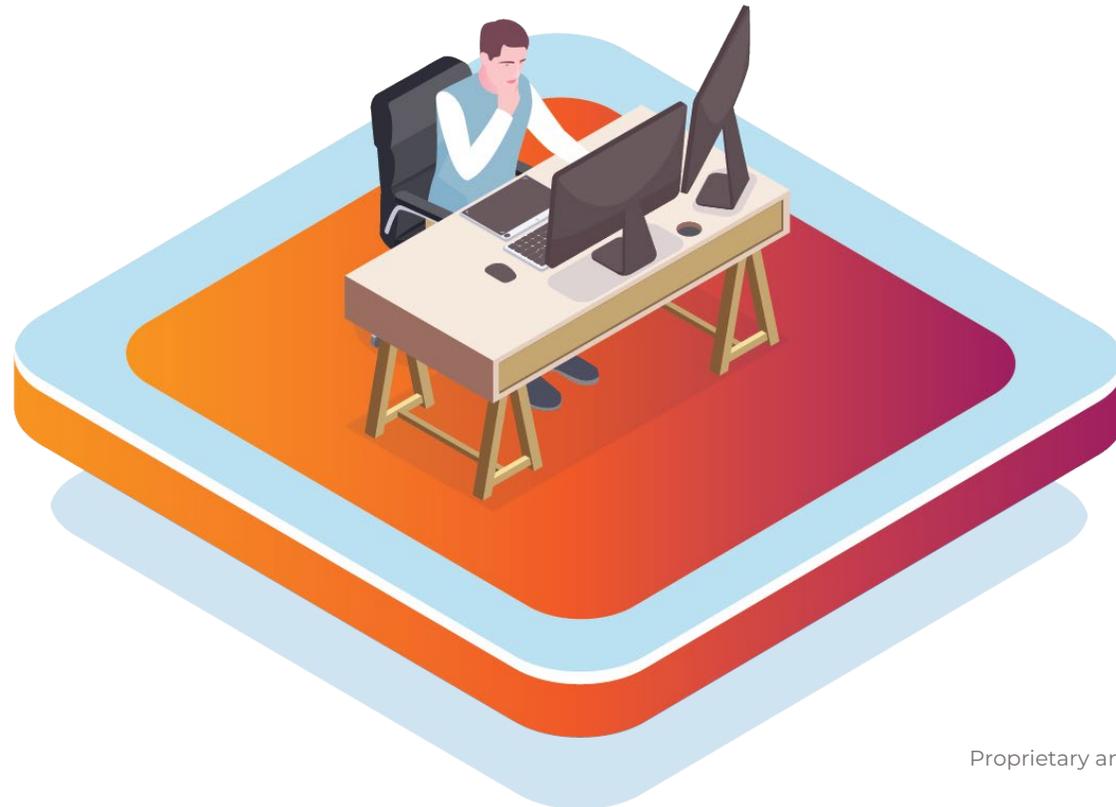
Lower costs & faster timeline for CMMC

Speed Conquers

3 months

Submission of FedRAMP High package

What Does the World Look Like in 2030?

AI Everywhere

Compliance As Code

Audit On-Demand

Collaborative
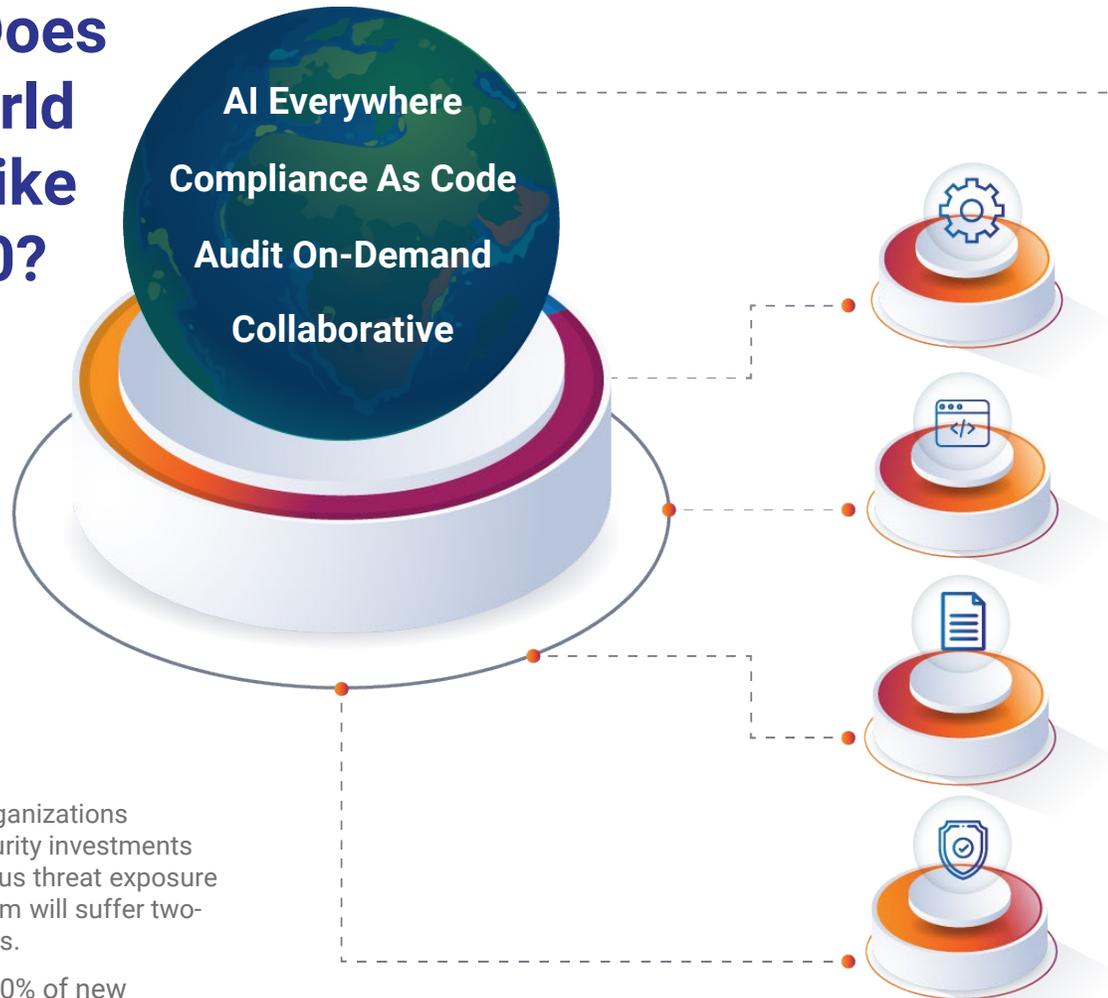
You Need These to Make it: Now and in the Future

AI integration everywhere**

Self-updating paperwork & compliance as code

On-demand, audit-ready documentation

Unified security, risk, and compliance*

* Gartner: By 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will suffer two-thirds fewer breaches.

** Gartner: By 2026, 30% of new applications will use AI to drive personalized adaptive user interfaces, up from less than 5% in 2023.

Establishing a Control Baseline –
Controls Can Be Established from a Compliance, Organization, or Risk-based Perspective

Regulators
(Compliance-based)

Policies
(Organization-based)

Threats
(Risk-based)

Frameworks

Requirements

Risks

Controls

With Continuous Controls Monitoring, controls become the center of the universe in the RegScale platform

Control Lifecycle Management

Control Lifecycle Management

Build the Program

- 50+ Supported Regulations
- Control Mapping
- Wizard-Driven Builders
- AI Author/ Explainer

Collect Evidence

- Evidence Locker
- Time Travel
- APIs + Graph
- SDK for Custom Integrations
- Automation Platform w/30+ integrations

Assess

- Lightning Assessments
- Office Automation w/ Word + Excel Exports
- Automation Platform w/30+ Integrations
- AI-Based Assessments

Fix the Issues

- ITIL Tool Integrations
- Screening + Phase Gating
- Kanban Board
- Scanner Integrations

Manage the Risk

- Threat Modeling
- Enterprise Risk
- Questionnaires
- 3rd Party Risk
- Automated Risk Scoring
- Financial Modeling

Governance

- Event-Driven Workflows
- Exception Management
- Change Management
- Alerts + Notifications
- Reporting + Dashboards

Automation Platform
(APIs, Graph, CLI, AI/ML, and SDK)

Reporting, Dashboards, and Analytics
(Office Automation, BI Integration, and In-app Visualizations)

Continuous Controls Monitoring

Rapid Certification

Automated Evidence Collection

Automated Controls Mapping

Automated Access Reviews

Simplified Risk Management

SOC 2
PCI
HIPAA
ISO 27001
CMMC
SOX

FedRAMP Authorization

Efficiency

Cost Savings

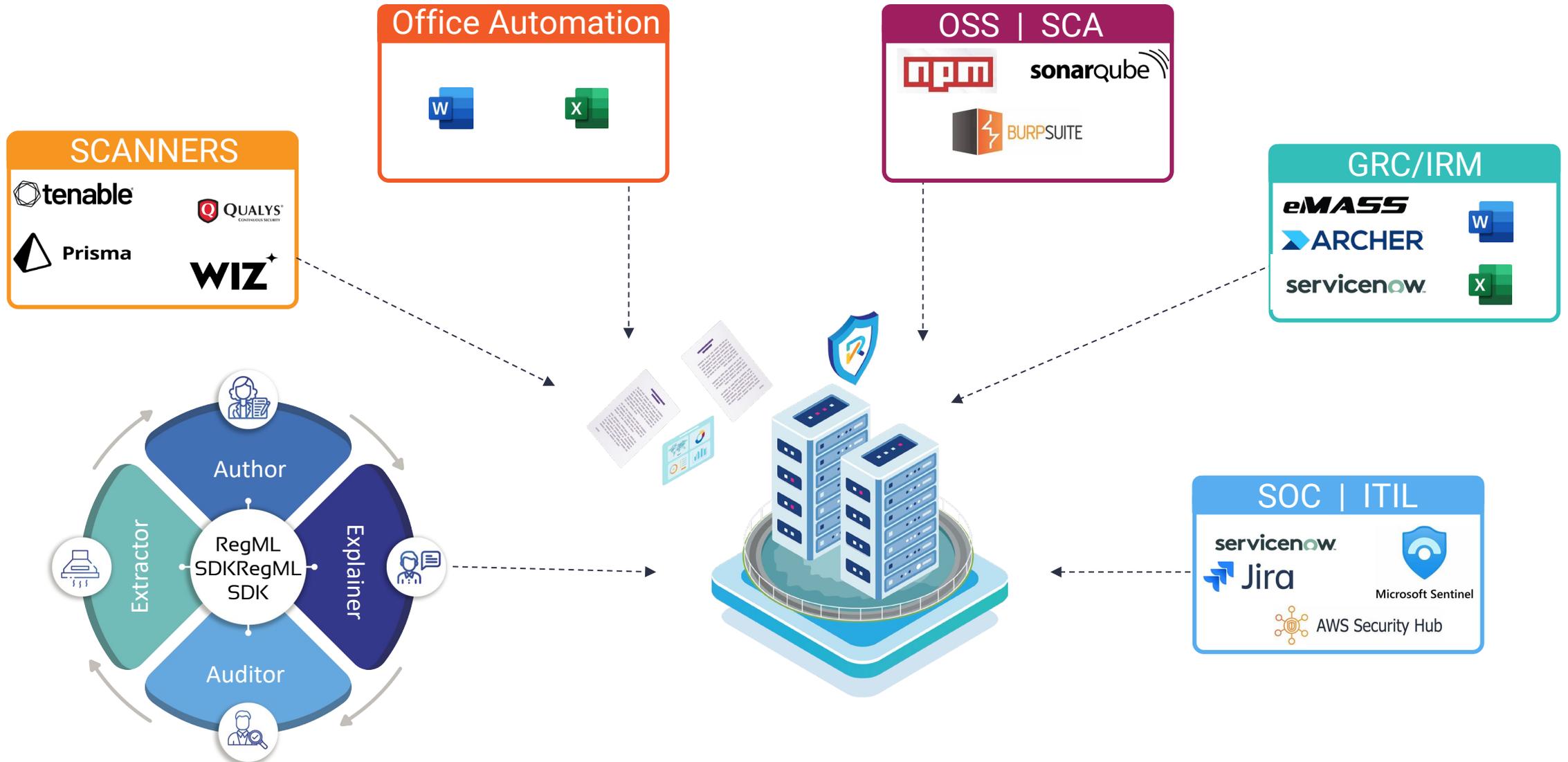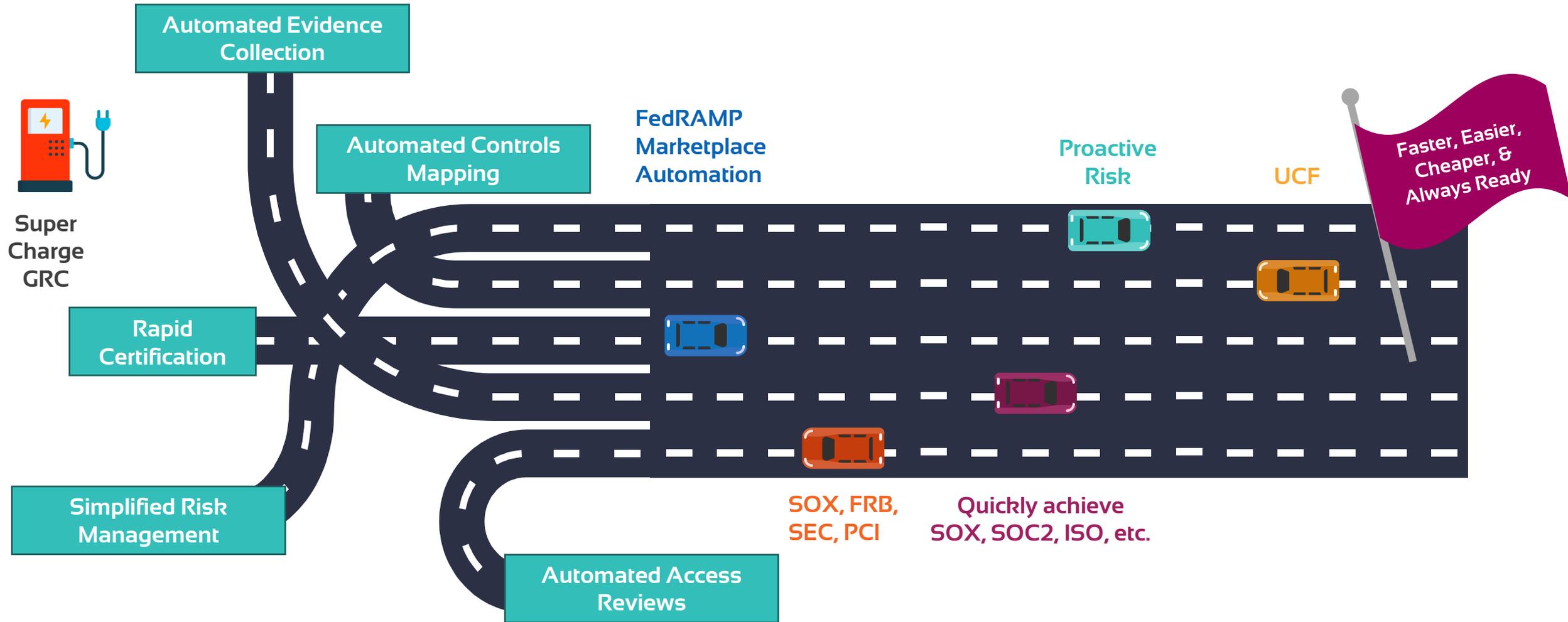Audit Risk Reduction

Assess Once, Leverage Many

SOX, FRB, SEC, PCI...

Issues

Portfolio Risk

3rd Party Risk

Automated Evidence Collection

Automated Controls Mapping

FedRAMP Marketplace Automation

Proactive Risk

UCF

Faster, Easier, Cheaper, & Always Ready

Super Charge GRC

Rapid Certification

Simplified Risk Management

Automated Access Reviews

SOX, FRB, SEC, PCI

Quickly achieve SOX, SOC2, ISO, etc.

Automation Pays

60%

Reduction in audit prep & response time

Speed Conquers

3 months

Submission of FedRAMP High package

Strategic Wins

90%

Reduction in effort to complete SOC 2 Type 1

Visibility Victories

30%

Lower costs & faster timeline for CMMC
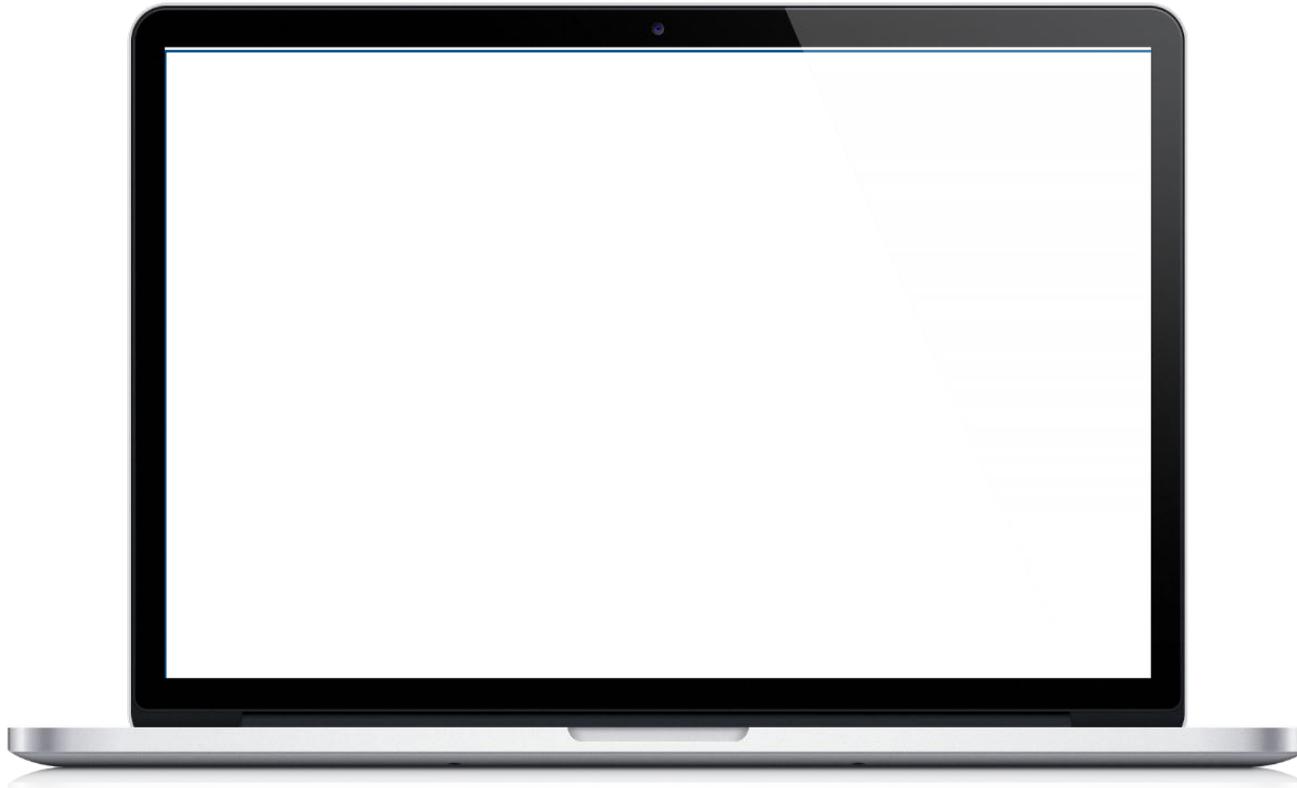
Summary and Next Steps

RegScale

Thank you!

FSD Supplemental Resources

Streamline Your Security, Elevate Your Oversight

Features

- Seamless Integration with IAM Tools
- Advanced CLI for Access Analysis

Benefits

- Automated, Efficient Reviews
- Enhanced Security & Compliance

Fortune 500 Company subject to Sarbanes-Oxley

Customer cut user access review time from 50 hours to just 2 per month using RegScale. This shift enabled a focus on high-value tasks and greatly mitigated non-compliance risks.

Get Out of the Muck: Lower Costs, Improve Security, and Reduce Audit Fatigue
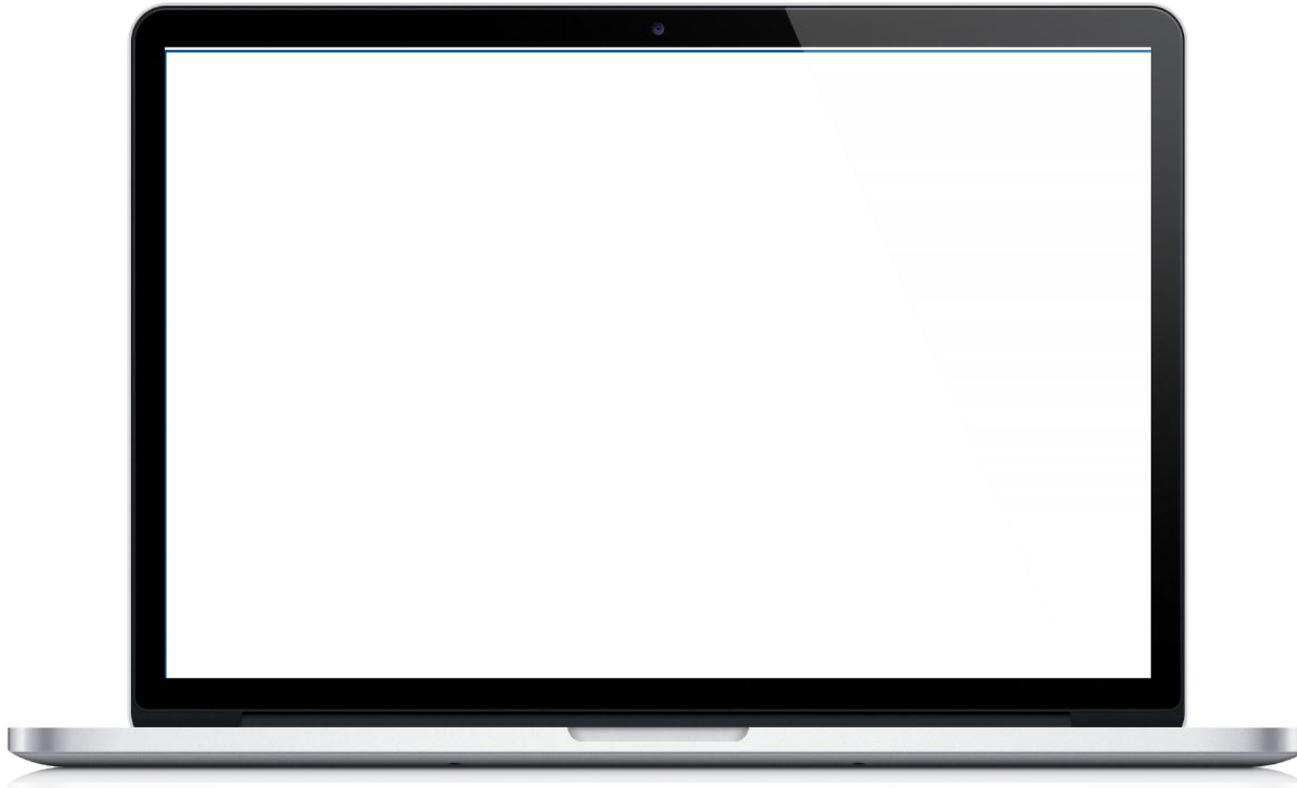
Features

- Regulatory Coverage
- Wizard Driven Builders
- Lightning Assessments
- Event Driven Workflows
- Reporting /Dashboards

Benefits

- Transparency
- Cost Savings
- Automate Manual Tasks

Advanced Cybersecurity Solution Company

Customer completed and submitted FedRAMP High package in 3 months.

Compliance Risk

Audit Failures (Issues)

Vulnerability Management Integrations

Configuration Management Integrations

Enterprise Risk

Threat Modeling

Risk Treatments/Controls

Risk Assessments

3rd Party Risk

Supply Chain Module

Questionnaires

Assessments & Requirements Modules

Rollup Reporting

Compliance Risk

| Audit Failures (Issues) | Vulnerability Management Integrations | Configuration Management Integrations |

Enterprise Risk

| Threat Modeling | Risk Treatments/ Controls | Risk Assessments |

3rd Party Risk

| Supply Chain Modules | Questionnaires | Assessments & Requirements Modules |

Roll Up Reporting
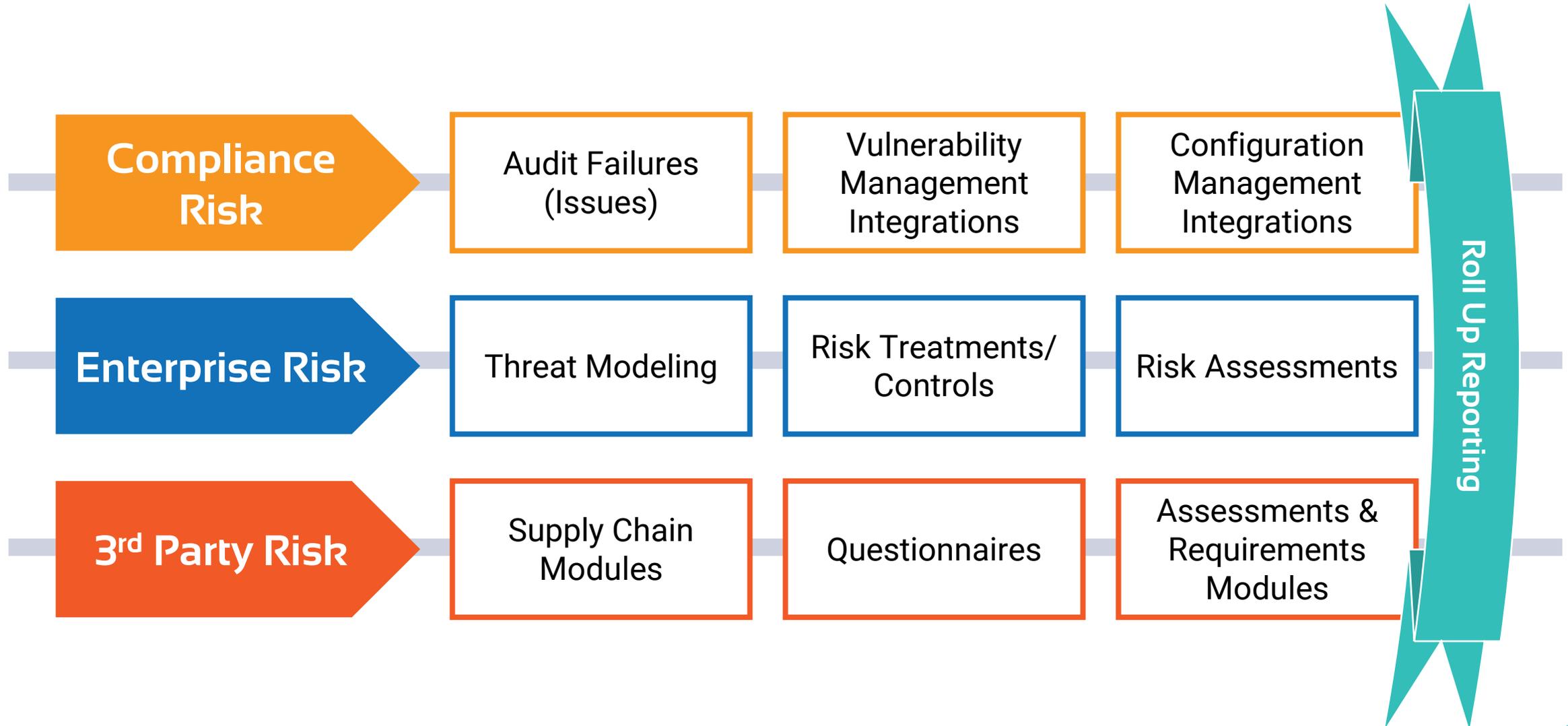
Expensive manual data transfer

Gaps in control visibility

Slow response

Misinformed decision-making

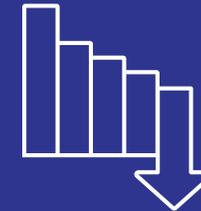**A reactive approach to security, risk and compliance results in higher risk and reduced visibility.**

Silos
Inefficiency & Unnecessary Expenses

Oprah Effect
Everyone Gets a Framework

Tool Sprawl

Lack of Clarity

Gartner: By 2026, 70% of enterprises in regulated verticals will have integrated compliance as code into their DevOps toolchains, reducing risk management and improving lead time by at least 15%

Gartner: By 2025, 70% of organizations will implement structured infrastructure automation to deliver flexibility and efficiency … from 20% in 2021

Ponemon: The average cost of non-compliance is nearly 3 times the average annual cost of compliance activities

Thomas Reuters: 67% of survey respondents expect to see an increased cost to manage risk issues in the next 12 months

97%
Organizations Facing Increased Cyber Threats

Rising Regulatory Demands

95%
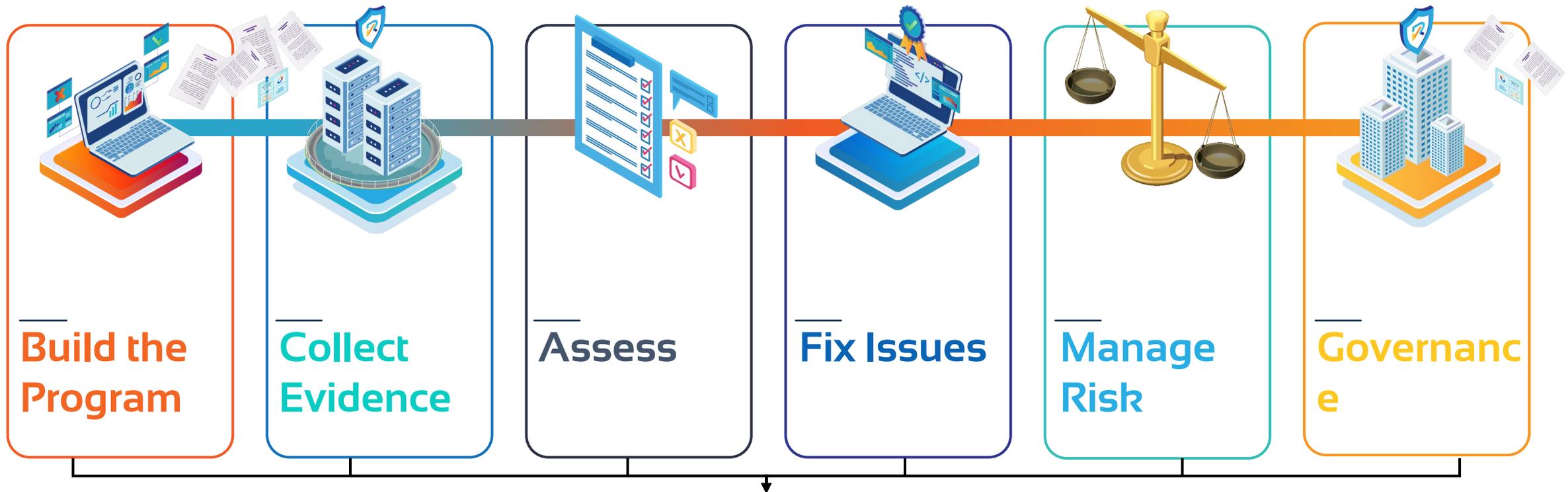Organizations Lack Crucial Tech Capabilities

Digital Transformation Results are Falling Short

Continuous Controls Monitoring (CCM) is the real-time assessment of controls to manage risks, ensure compliance, and enhance decision-making.

Control Lifecycle Management

Build the Program

Collect Evidence

Assess

Fix Issues

Manage Risk

Governance

Continuous Controls Monitoring ("CCM")
(APIs, Graph, CLI, and SDK)

Reporting, Dashboards, and Analytics
(Office Automation, BI Integration, and In Product Visualizations)

Desired Outcomes

- MRA remediation
- One system of record
- High integrity process
- Automated audit reports
- Real-time reporting on gaps and issues

Pain Points

- MRAs to be resolved by Q1'24
- 1,300+ assets need risk assessed for scoping
- Disparate systems of record
- No real-time reporting
- Lengthy timelines & error-prone

Current Solutions

- 8+ FTEs support assessments
- SNOW, Archer, ACW (control assessments), MS Office

Decision Making Process

- Integration with existing security and GRC tools
- Best practices and industry standards
- Real-time monitoring
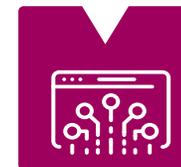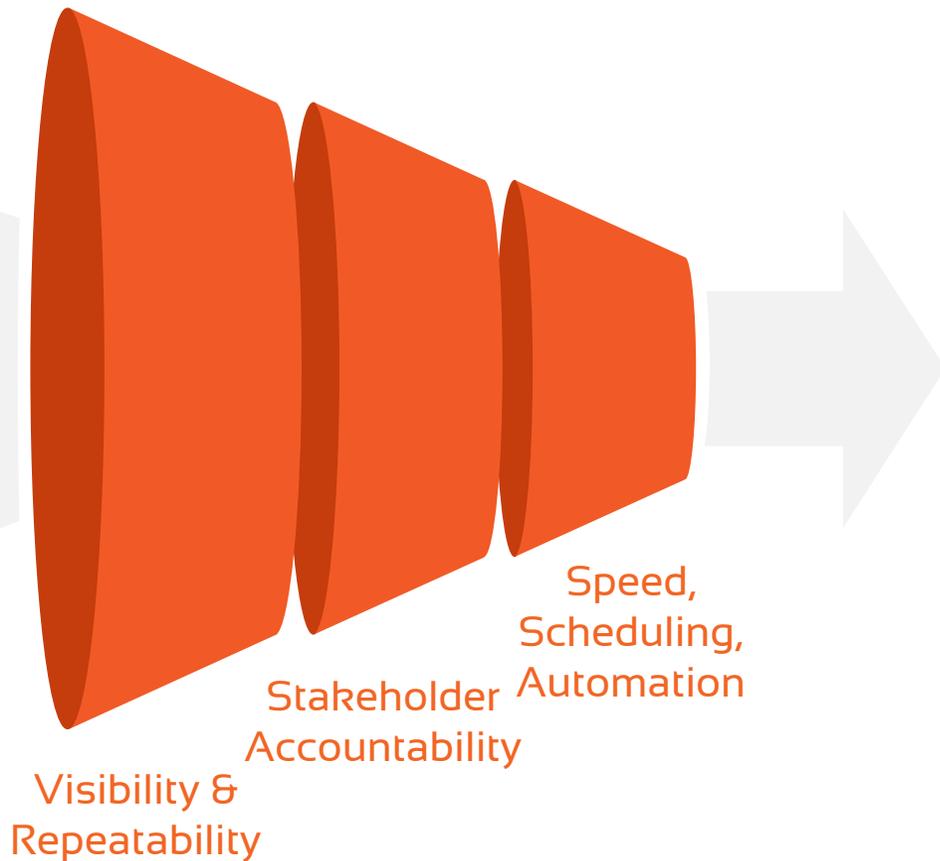- Reporting/dashboards
- Streamlined workflow

Timeline

- MRA remediated by Q1 2024
- Implement tool and begin remediation ASAP

Key Stakeholders

- CIO
- SVP, IAM
- InfoSec Manager
- Procurement
- TPRM Group (Vendor Risk)

Objective

Objective

Objective

Objective

Visibility & Repeatability

Stakeholder Accountability

Speed, Scheduling, Automation

Build

Collect

Assess

Fix Issues

Manage Risks / Governance

Lower Costs

Strengthen Security

Reduce Audit Fatigue

Scale with Ease

Lower Costs with Intelligent Automation

Strengthen Security through Actionable Insights

Always Audit-Ready with Automated Compliance

Scale Seamlessly Across Use Cases

Slash Costs, Ditch Manual GRC Drudgery

Compliance at the Speed of Now

End Audit Agony Manual Paperwork: : Streamline with Ease

Audit Proof or Bust: Tighten Control Visibility

Excel No More: Unlock True Tool Potential

Certify Swiftly, Expand Rapidly

With data spread across disparate systems, gathering accurate and up-to-date information for audits is time-consuming and difficult.

Customer reduced audit prep and response time by 60%.

The overwhelming 18 to 36-month timeline and draining demands on security and compliance teams for FedRAMP cripples operational efficiency.
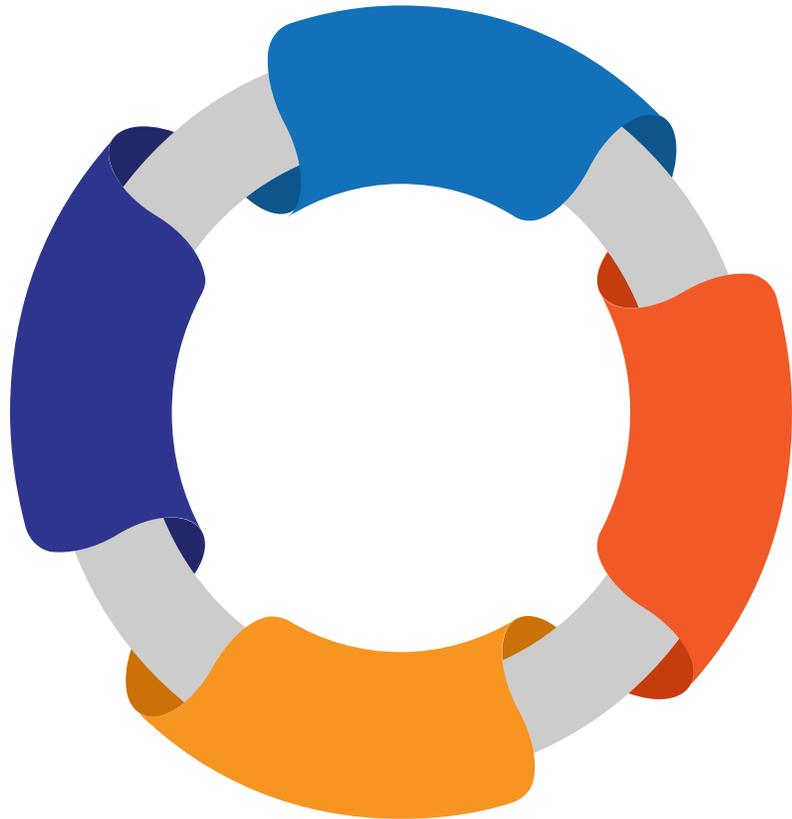
Customer completed and submitted FedRAMP High package in 3 months.

Establishing security program and passing initial SOC 2 Type 1 with limited resources to take 300 hours.
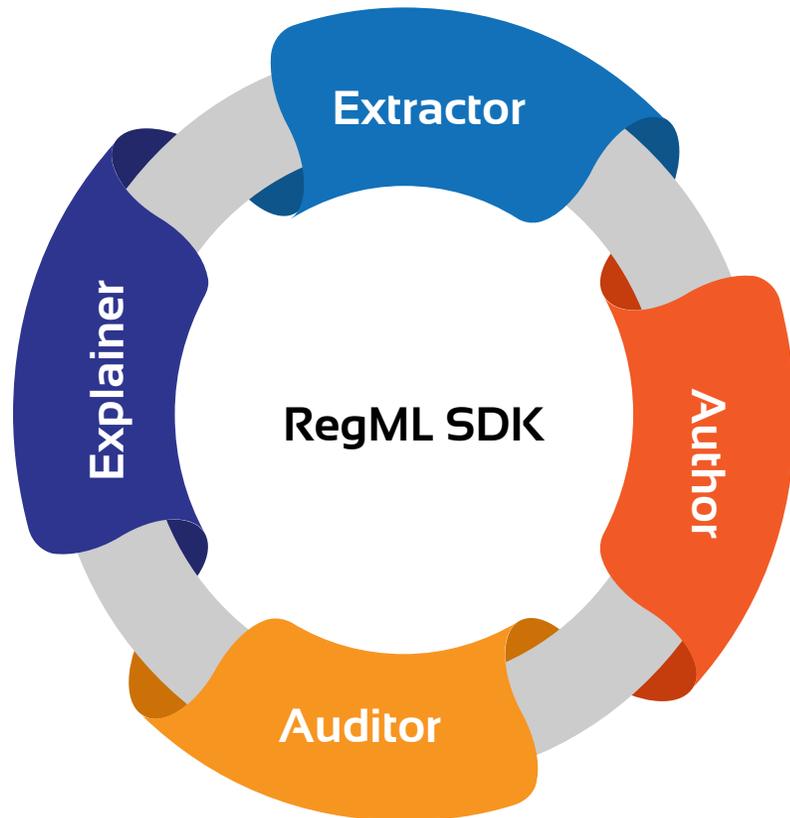
Attestation completed with only 25 hours effort, a 90% savings with RegScale.

AI-Driven Advantage

- ✓ Robust Control Implementations
- ✓ Improved Security Posture
- ✓ Reduced Risk of Audit Failure
- ✓ Continuous Improvement

RegML Bridges CCM with the LLM tool of Your Choice

- Extract draft control implementation from policies
- Generate draft control implementation statements
- Audit existing control implementations for completeness
- Explain controls in language understandable by user role

JIRA

Perform bulk processing of RegScale issues to create, update, and otherwise sync with Jira and vice versa to perform automated ticket assignment.

SonarCloud

Automates SonarCloud scans, generates assessments from detected code issues, and creates linked child issues with severities matching SonarCloud's vulnerability levels

Salesforce

Perform bulk processing of RegScale issues to create, update, and otherwise sync with Salesforce and vice versa to perform automated case assignment.

Catalog Updater

Automatically updates and synchronizes data elements between RegScale application and master catalogs at regscale.com

Tenable Vuln Management

Real-time asset and vulnerability updates from Tenable, enhancing cybersecurity responsiveness and proactive threat defense

STIG GUI

Ingest security checklists from STIG rules and automatically update SSP control and component implementations

Nessus Report Scan

Import and update assets and vulnerability data from Nessus scans into RegScale

CrowdStrike

Import incidents from CrowdStrike into RegScale for easier incident management and response for more proactive security

Sicura

Pull information from Sicura to create assets and "security checks" in RegScale

XML Import/Export FedRAMP SSP

Bulk process and load/export XML formatted FedRAMP SSP into/from RegScale

Before we begin, let's define the key RegScale modules and how they will build off one another to create a best in-class GRC solution. The below diagram highlights the key modules and functionalities you'll be interacting with but is not a comprehensive listing of what RegScale offers.
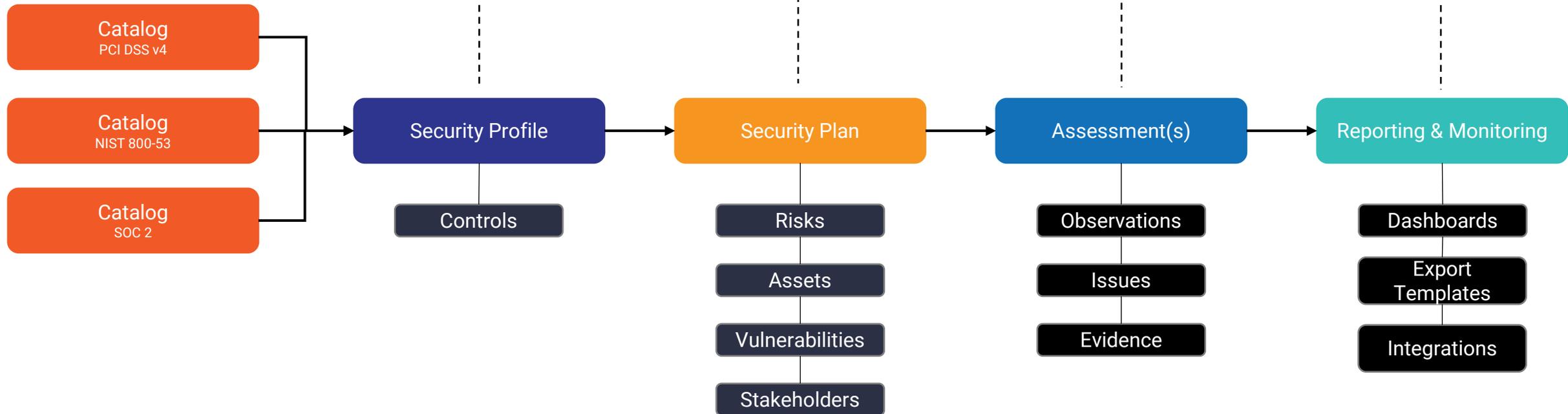
The **Catalog** module is a repository for industry / regulatory-aligned and/or bespoke control sets from which you will perform compliance testing.

A **Security Profile** serves as a baseline or scope for compliance testing. The Profile consists of one or more controls across one or more Catalogs.

The **Security Plan** is the central hub for compliance-related activities. Scoped by the **Security Profile**, practitioners can layer in risks, assets, issues and other key details to help define the compliance journey.

Control **Assessments** are performed to evaluate the design and operating effectiveness of in-scope controls. Assessments can be scheduled or performed ad-hoc via RegScale's *Lightning Assessment* feature.

Leveraging out of the box reporting and readily available API connectors, RegScale enables **real-time visibility** into the status of risk and compliance programs. Additionally, users can export custom-tailored reports with the click of a button.

Catalog PCI DSS v4				
Catalog NIST 800-53	Security Profile	Security Plan	Assessment(s)	Reporting & Monitoring
Catalog SOC 2	Controls	Risks	Observations	Dashboards
		Assets	Issues	Export Templates
		Vulnerabilities	Evidence	Integrations
		Stakeholders		

Regional Commercial Bank: 18,000+ Employees ~$180B Assets

In the face of multiple federal audit findings, a regional commercial bank partnered with RegScale to implement continuous controls monitoring to remediate the issues and modernize their compliance process.

THE PROBLEM

Assets, risks and controls data in disparate systems and no real-time visibility, reporting or metrics

THE SOLUTION

- Integration with security and GRC tools
- Establish single source of truth
- Real-time compliance & controls monitoring
- Reporting/dashboards for visibility

THE RESULT

- Integrated platform that can automatically scope, test and collect evidence
- Real-time reporting on compliance gaps and issues
- Automated audit reports
- Rapid time-to-value ensures remediation ahead of regulatory deadline

Audit issue remediation and future avoidance

Rapid time-to-value

AUDIT

Building Roadmap with RegScale to Modernize Compliance Program

A Leading Aerospace & Defense Company

A leading Aerospace & Defense company, facing compliance requirements with the DoD's Cybersecurity Maturity Model Certification (CMMC), and real-time security gap identification, turned to RegScale for assistance.

THE PROBLEM

Fill documentation gaps, improve cloud security, and expedite cloud migration efforts

THE SOLUTION

- Provide a real-time security control scorecard
- Build API integrations to automate ticket creation and compliance demonstration
- Enable enhanced cybersecurity in cloud operations

THE RESULT

30% reduction in cost and time for CMMC compliance-related effort

Visualize security controls and update risks in real-time

Rapid time-to-value

Swift data and document ingestion, versatile output in any format

Series A, Tech Company

Amid a competitive market, the aspiration to establish trust through SOC2 and FedRAMP certifications becomes paramount, and SOC 2 Type 1 is the first step. The ongoing journey includes SOC 2 Type 2, with the ultimate goal of being FedRAMP High Baseline ATO, signifying commitment to security excellence.

THE PROBLEM

- Series A start-up seeks a "real" SOC 2 Type 1 with limited people resources.
- Estimated effort: 260-300 hours

THE SOLUTION

- Security and GRC integration
- Quick time-to-value for program stand-up
- One-stop compliance truth
- Automated evidence collection
- Integrated controls testing
- Seamless auditor collaboration

THE RESULT

- SOC 2 Type 1 with RegScale: 25 hours
- Total Savings using RegScale: Up to 275 hours or ~90% effort

Reduce the cost of compliance

Rapid time-to-value

Building Roadmap for compliance expansion

Ready. Set. RegScale.

Your Name
Your_Email@regscale.com | XXX-XXX-XXXX

RegScale