RegScale

ONE-PAGER

The Governance Layer Your Zero Trust Strategy Is Missing

How RegScale Advances Maturity Across the CISA ZTMM

The CISA Zero Trust Maturity Model gives organizations a structured path from static, perimeter-based security to a fully automated, continuously verified posture. But technical controls alone won't get you there.

RegScale's Continuous Controls Monitoring platform supports Zero Trust progress across all five ZTMM pillars and three cross-cutting capabilities. Built on a Compliance-as-Code foundation and serving as the system of record for risk and compliance across the enterprise, RegScale gives security teams and leadership a clear picture of where they stand in real time.

1 Identity

- Enforces role-based and attribute-based access controls (RBAC, ABAC) and MFA via Microsoft Azure Active Directory
- Offers real-time anomaly detection through Azure Monitor and Sentinel SIEM
- Integrates with external identity providers (Azure AD, AD/LDAP, SSO) to enforce role-based and record-level access across tenants.
- Implements just-in-time privileged access elevation via Azure PIM as well as approval workflows, automatic expiration, and automated revocation tied to identity lifecycle events
- Supports both manual and automated identity orchestration through IAM integrations, coordinating control validations, evidence management, and remediation tracking across IAM-related controls

2 Devices

- Maintains device and system inventories and manages third-party risks through a TPRM module
- Provides a centralized view into systems, assets, and associated controls and risks
- Correlates assets to controls, risks, and issues through governance and monitoring integrations, serving as the system of record for oversight and compliance

3 Networks

- Governs network security controls by maintaining documentation, monitoring compliance evidence, and tracking risks and remediation activities
- Leverages Azure-native resilience capabilities, including geo-redundancy, regional failover, backup, and recovery
- Enforces network segmentation and tenant isolation, and encrypts all inbound and outbound traffic via HTTPS/TLS 1.2+
- Enables centralized governance of network security policies, mapping them to technical controls and continuously monitoring compliance evidence

4 Applications & Workloads

- Implements a Secure SDLC with threat modeling, secure design reviews, OWASP coding guidelines, dependency scanning, and automated SAST, DAST, and SCA integrated into Azure DevOps pipelines
- Uses CI/CD pipelines and containerized workloads with logically separated dev/test/production environments and least-privilege access to production
- Aggregates control status, security findings, and risk information across applications via Continuous Controls Monitoring, serving as the system of record for risk-aware decision-making
- Supports policy and control mapping with continuous monitoring, evidence collection, and automated issue identification and remediation workflows

RegScale

ONE-PAGER

5 Data

- Enables near-real-time, bi-directional sync with external data inventories with 2,000+ REST APIs and 70+ out-of-the-box commercial tool integrations
- Provides pre-loaded data categories aligned to NIST 800-60 and FIPS 199
- Supports flexible deployment (public/private SaaS, on-prem, air-gapped) with tightly controlled record-level access and detailed history logs
- Enforces least-privilege data access through SSO, RBAC, multi-tenancy, group- and role-based permissions, and more
- Protects all data at rest and in transit using current standards (AES-256, TLS 1.2+) and enables enterprise-wide visibility into cybersecurity posture
- Leverages a Compliance-as-Code foundation built on OSCAL and OCSF, with enforcement extending through integrated security tools and CLI/API-driven automation

Cross-Cutting Capabilities: Visibility & Analytics, Automation & Orchestration, Governance

- **Visibility & Analytics:** Integrates with SIEM solutions to ingest security-relevant data and combines it with policy, control, and regulatory requirement data to support better decision-making
- **Automation & Orchestration:** Ingests incident, vulnerability, and security telemetry from existing tools to enrich cyber hygiene metrics and integrate with incident management and orchestration platforms
- **Governance:** Enables enterprise-wide Policy-as-Code enterprise-wide and monitors policies continuously through 70+ commercial tool integrations, with enforcement extending through the customer's security stack and CI/CD pipelines

sales@regscale.com

regscale.com

Ready to get started?