RISC Compass Security & Data Protection Overview

May 2026

Overview

RISC Compass is a cloud-based compliance technology platform designed to assist broker-dealers, registered investment advisers, consultants, compliance personnel, and related organizations with compliance administration, supervisory workflows, organization, attestations, reporting, document management, onboarding processes, and related operational functions.

RISC Compass is designed to help firms centralize and organize compliance-related information, workflows, supervisory reviews, records, and operational processes through configurable cloud-based applications and integrations.

RISC Compass utilizes established third-party cloud infrastructure, storage providers, software platforms, and related technology vendors in connection with operation of the platform.

Shared Responsibility Model

RISC Compass operates under a shared responsibility model.

RISC is responsible for maintaining commercially reasonable administrative, technical, and operational safeguards designed to support the security and availability of the platform environment utilized by RISC.

Clients remain responsible for:

- supervisory procedures,
- compliance obligations,
- cybersecurity programs,
- endpoint/device security,
- access management,
- user supervision,
- credential management,
- books and records obligations,
- retention obligations,
- data review and validation,
- and compliance with applicable laws and regulations.

Use of RISC Compass does not replace a firm's supervisory obligations, compliance program, cybersecurity program, or regulatory responsibilities.

Platform Infrastructure & Third-Party Providers

RISC Compass utilizes third-party software, cloud infrastructure, hosting environments, APIs, storage providers, and related technology vendors to support operation of the platform.

Third-party providers may include:

- cloud application providers,
- hosting providers,
- storage providers,
- data aggregation providers,
- communication providers,
- and related infrastructure vendors.

References to third-party certifications, security standards, or compliance frameworks relate to the applicable third-party provider's environment and controls and do not constitute a representation that RISC independently maintains certification under such standards unless expressly stated.

RISC periodically reviews vendors and providers utilized in connection with the platform as part of its operational oversight process.

Provider Security Controls

RISC Compass utilizes carefully selected third-party infrastructure and cloud software providers that maintain security-focused environments designed to support the protection, availability, integrity, and resilience of hosted systems and customer data.

RISC prioritizes providers that maintain established security programs, operational controls, and industry-recognized security or compliance frameworks appropriate for cloud-based business operations.

Applicable third-party providers generally maintain controls that include:

- physical data center security and restricted facility access,
- network monitoring and intrusion detection controls,
- encrypted data transmission,
- access logging and audit controls,
- malware and vulnerability management,
- backup and redundancy controls,
- disaster recovery and business continuity processes,
- and independent security or compliance reviews, such as SOC or ISO-based assessments.

RISC periodically reviews vendor security materials, operational practices, and publicly available compliance information as part of its vendor oversight and operational review process.

Access Controls & Authentication

RISC Compass supports role-based access permissions intended to allow organizations to restrict user access based on responsibilities and business needs.

Organizations are responsible for:

- assigning appropriate user access,
- maintaining access reviews,
- disabling terminated user access promptly,
- monitoring administrator accounts,
- safeguarding credentials,
- and maintaining appropriate internal security controls.

Clients are responsible for managing and monitoring activity occurring within their organization's accounts and user environment.

RISC Compass utilizes access control and authentication measures designed to support secure platform access and user management. Depending on the applicable environment and client configuration, such measures may include role-based access permissions, administrator-controlled user access, authentication controls, session management controls, and multi-factor authentication capabilities.

Data Handling & Storage

RISC Compass is intended to support compliance and operational workflows and may contain records, reports, attestations, supervisory documentation, communications, and related operational information uploaded or entered by users.

Clients remain solely responsible for determining:

- what information is uploaded,
- whether such information is appropriate for storage,
- applicable retention obligations,
- and compliance with applicable privacy and cybersecurity requirements.

RISC Compass is not intended to collect or store highly sensitive personal information such as full Social Security numbers, full payment card information, or banking credentials unless specifically required for authorized operational functionality or integrations.

Encryption & Transmission Security

RISC Compass utilizes commercially reasonable measures intended to help protect data transmissions and platform access.

Where supported by applicable providers and infrastructure, data transmissions may utilize encrypted communication protocols and security controls designed to reduce unauthorized access risks.

However, no system, network, software platform, cloud environment, API integration, transmission method, or electronic storage method can be guaranteed to be completely secure, uninterrupted, or free from vulnerabilities.

Brokerage Data Feed Services

Certain platform functionality may include optional third-party brokerage account aggregation, statement retrieval, holdings retrieval, transaction import, account monitoring, or related financial account data integration functionality (“Brokerage Feed Services”).

Brokerage Feed Services are intended solely as a technology facilitation and administrative support tool to assist organizations with supervisory review, compliance monitoring, personal trading review support, and related operational functions.

RISC does not act as:

- a broker-dealer,
- investment adviser,
- custodian,
- clearing firm,
- fiduciary,
- supervisory principal,
- financial institution,
- or discretionary manager

through Brokerage Feed Services.

Brokerage Feed Services rely upon external financial institutions, custodians, aggregators, APIs, and third-party providers outside of RISC’s control.

Availability, accuracy, completeness, formatting, timing, and continuity of account data cannot be guaranteed.

Financial institutions and third-party providers may:

- restrict,
- interrupt,
- throttle,
- revoke,
- modify,
- limit,
- or discontinue
  aggregation access, credential requirements, APIs, integrations, security protocols, or connectivity at any time without notice.

RISC is not responsible for:

- delayed or unavailable feeds,
- incomplete or inaccurate account data,
- unsupported institutions or account types,
- credential failures,
- interrupted integrations,
- revoked institution access,
- third-party provider outages,
- cybersecurity restrictions imposed by financial institutions,
- or technical limitations outside of RISC's reasonable control.

Clients remain solely responsible for:

- supervisory review,
- compliance determinations,
- books and records obligations,
- exception monitoring,
- account verification,
- cybersecurity obligations,
- and all required supervisory procedures and follow-up.

Use of Brokerage Feed Services does not guarantee regulatory compliance or satisfaction of supervisory obligations.

Business Continuity & Data Backup

RISC utilizes third-party providers and infrastructure intended to support platform availability, redundancy, and operational continuity.

Certain providers utilized by RISC may maintain:

- redundant infrastructure,
- backup systems,
- disaster recovery capabilities,
- and business continuity procedures.

Clients remain responsible for maintaining their own independent copies, exports, backups, and retention procedures for records required under applicable law or business policy.

Security Limitations

RISC maintains commercially reasonable, risk-based administrative, technical, and operational safeguards designed to support the security, confidentiality, availability, integrity, and resilience of the platform environment utilized by RISC.

However, no platform, network, cloud environment, API integration, software application, transmission method, or electronic storage system can be guaranteed to be completely secure, uninterrupted, error-free, or immune from evolving cybersecurity threats or operational disruptions.

Cybersecurity incidents, infrastructure failures, software vulnerabilities, credential compromise, malicious attacks, third-party outages, human error, and evolving technological risks may impact any cloud-based environment, including environments operated by third-party providers utilized in connection with the platform.

Accordingly, clients are encouraged to maintain appropriate cybersecurity programs, supervisory procedures, vendor oversight processes, business continuity planning, access controls, and internal safeguards consistent with their business operations, risk profile, and regulatory obligations.

Regulatory & Compliance Disclaimer

RISC Compass is intended to support compliance administration and operational workflows. The platform and related materials do not constitute legal advice, investment advice, accounting advice, cybersecurity advice, or regulatory approval.

Use of the platform does not guarantee compliance with any federal, state, self-regulatory organization, or international law, rule, regulation, examination requirement, supervisory obligation, cybersecurity obligation, or regulatory expectation.

Clients remain solely responsible for their own compliance, supervision, regulatory obligations, and internal controls.

Contact Information

RISC may make additional vendor due diligence information, operational documentation, or security-related materials available upon reasonable request, subject to confidentiality, security, legal, and operational limitations.

For questions regarding platform security, vendor due diligence, or operational controls, please contact RISC directly.