

## Cloud Platform Trust Center

# Ensure your data is secure and compliant

With a SOC 2, ISO 27001 and FedRAMP validated cloud platform.

Security teams face a critical dilemma: using data to drive innovation with AI and analytics while protecting an ever expanding cloud footprint. Data exposure, insider threats, growing third-party risks, and expanding privacy regulations make security and compliance harder than ever. Without verifiable, enforced controls, proving posture and compliance becomes a burdensome, manual exercise, leaving organizations vulnerable to regulatory fines and a critical loss of trust.

Collibra addresses these challenges with a secure cloud platform, featuring our unique Edge architecture that keeps sensitive data under your control. Global security standards and privacy regulations are rigorously met through continuous DevSecOps and independent third-party validation, streamlining due diligence and audit reporting for verifiable compliance and greater confidence.



## Benefits



### Protect customer data

Collibra provides comprehensive external threat prevention, vulnerability management, asset protection and incident response capabilities to mitigate threats and prove audit-readiness.



### Enforce security standards

Collibra implements COSO, COBIT and NIST standards within its cloud platform security framework, and obtains independent third party validation as proof our security posture meets the highest global standards.



### Ensure privacy compliance

Collibra strengthens privacy compliance with our Edge architecture that keeps PII in your environment, while comprehensive agreements, assessments and auditable controls continuously monitor and validate adherence to global privacy standards.



### Streamline compliance validation

Collibra streamlines due diligence and audit reporting, through continuous monitoring, third-party attestation, and actionable insights on activities, vulnerabilities, and incidents, enabling clear visibility of security posture and compliance.

## Product highlights

### Secure edge architecture

Processes data within your secure perimeter, eliminating data exposure risk and satisfying data residency and sovereignty requirements.

### Encryption and key management

Combines robust encryption for data in transit (TLS 1.3) and at rest (AES-256) with a separate, FIPS 140-2 compliant key management system for end-to-end protection.

### Role-based access control and single sign on

Integration with your Identity and Access Management provider enforces the principle of least privilege, ensuring users can only access the specific data they are authorized to see.

### Independently verified security and compliance

Broad certification and third party validation like SOC 2, ISO 27001, 27017, 27018, 42001 and FedRAMP streamline vendor due diligence and accelerate your auditing and compliance reporting.

### Continuous DevSecOps

Proactive application security testing (static, dynamic, and API analysis), software composition analysis for internal and third-party code, container security scanning, infrastructure as code analysis, and network penetration testing.

### Advanced privacy framework

Comprehensive legal and process support, including EU BCRs, SCCs, DPAs, and clear protocols for DPIAs, DSR fulfillment and breach notification, ensure global data transfer, processing, and audit obligations are fulfilled.



Want to learn more? Visit our Trust Center  
[collibra.com/company/trust-center](https://collibra.com/company/trust-center)