

# Shared security management model

The following table outlines the shared security responsibilities between Collibra, Customers and Cloud Services Providers.

Security control or domain	Who is responsible?		
	Collibra customer	Collibra	Cloud services provider
Availability	•	•	•
Backup and restore	•	•	•
Business continuity and disaster recovery	•	•	•
Certifications, assessments and standards		•	•
Cloud infrastructure security management		•	•
Compliance: regulatory and legal	•	•	•
Data encryption: at-rest and in-transit	•	•	•
Data management - classification and retention	•	•	•
Encryption management	•	•	•
Human resources security	•	•	•
Identity and access management	•	•	•
Penetration testing: application and network	•	•	•
Physical media: disposal and destruction		•	•
Physical security		•	•
Secure SDLC processes		•	•
Security configuration: Collibra products	•	•	
Security configuration: Collibra infrastructure		•	•
Security incident management		•	•
Security monitoring and logging: Collibra products	•	•	•
Security monitoring and logging: Collibra infrastructure		•	•
Vulnerability management: Collibra products	•	•	•
Vulnerability management: Collibra infrastructure		•	•
Vulnerability management: Collibra third-party software		•	•

Note: This table is for informational purposes only, and the Collibra Security Policy governs Collibra's commitment with respect to the information security program and policies that protect customer data.