Compliance Mapping

Version: 2.0
Last Updated: 1st September 2026
Classification: Public

Compliance Mapping

This document maps Concord's security, privacy, operational resilience, and AI governance controls to selected industry standards and regulatory frameworks, to support due diligence, procurement, and vendor risk assessment. It does not constitute a certification or legal opinion unless expressly stated.

Our Compliance Philosophy

Our customers operate across financial services, insurance, and other regulated industries. Concord's governance framework is built as one unified control set that supports multiple regulatory and industry requirements, rather than bespoke controls per regulation.

Control Domains

Domain	Description
Information Security	Governance, risk management, access control, cryptography, monitoring
Privacy & Data Protection	Personal information management, data lifecycle, privacy governance
Identity & Access Management	Authentication, authorization, privileged access, identity lifecycle
Secure Software Development	SSDLC, code review, testing, vulnerability management
Cloud Infrastructure	Secure architecture, networking, resilience, monitoring

Domain	Description
Operational Resilience	Business continuity, disaster recovery, incident response
AI Governance	AI inventory, risk management, human oversight, auditability
Vendor Risk Management	Third-party oversight, subprocessors, supplier governance
Compliance & Audit	Policies, evidence management, control documentation

---

Framework Alignment Summary

Framework / Regulation	Alignment Focus
ISO/IEC 27001	Information Security Management System principles
ISO/IEC 27017	Cloud security guidance
ISO/IEC 27018	Protection of personal information in cloud environments
ISO/IEC 27701	Privacy Information Management
ISO/IEC 42001	AI Management Systems
ISO/IEC 23894	AI Risk Management
NIST Cybersecurity Framework (CSF)	Cybersecurity governance and operational controls
NIST AI Risk Management Framework	AI governance and risk management
OWASP ASVS / Top 10	Secure application development
PIPEDA	Canadian privacy obligations
GDPR	European data protection principles
CCPA / CPRA	California privacy obligations

Framework / Regulation	Alignment Focus
DORA (where applicable)	Operational resilience for financial institutions
OSFI Guidelines (where applicable)	Technology, cyber, and third-party risk governance

Unless explicitly stated otherwise, these references indicate alignment objectives, not formal certification or regulatory approval.

Certification Status

Concord is not currently certified against SOC 2 or ISO/IEC 27001. Our control environment is designed with these frameworks as reference points, and a formal certification program is underway. Current certification status should always be confirmed through up-to-date Concord compliance documentation rather than assumed from this overview.

Information Security Alignment

Security governance, risk management, identity and access management, encryption, secure software development, vulnerability management, logging and monitoring, incident response, business continuity, and vendor management — see the Security Overview.

Privacy Alignment

Lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability — consistent with PIPEDA, GDPR, and similar privacy law. See the Privacy & Data Protection Overview.

Responsible AI Alignment

Human oversight, transparency, explainability, accountability, risk management, AI inventory management, lifecycle governance, and auditability, designed with reference to the NIST AI RMF and ISO/IEC 42001. See the AI Governance & Responsible AI Overview.

Audit Readiness

Concord maintains governance documentation and operational evidence to support due diligence and audit activity. Available documentation may include security policies, architecture documentation, incident response summaries, privacy documentation, AI governance documentation, a Data Processing Addendum, subprocessor information, and a Service Level Agreement — availability depends on contractual arrangement and information sensitivity.

Shared Responsibility

Concord is responsible for: platform security, privacy safeguards, infrastructure operations, AI governance capability, and vendor governance.

Customers are responsible for: configuring the platform appropriately, defining their own governance policies, assigning user permissions, managing their regulatory obligations, and reviewing AI-generated outputs.

Additional Information

Available on request, subject to confidentiality obligations: Trust Center Guide, Security Overview, Privacy & Data Protection Overview, AI Governance & Responsible AI Overview, Infrastructure & Architecture Overview, and Data Processing Addendum.
