# Box Security, Privacy & Compliance Framework

## Comprehensive RFP / CISO-Level Executive Overview

This document provides an expanded executive-level overview of Box’s security, privacy, governance, and compliance posture, based on information published in the official Box Trust Center. The content is structured to support enterprise procurement processes, CISO evaluations, risk committees, and regulatory due diligence reviews.

## 1. Security Governance & Risk Management

Box operates a formal enterprise Information Security Program with executive oversight and structured governance mechanisms. Security risk is continuously assessed across infrastructure, application layers, vendor ecosystem, and operational processes.

The governance framework is aligned with internationally recognized standards and incorporates preventive, detective, and corrective controls.

- Documented Information Security Management framework
- Annual and ongoing enterprise-wide risk assessments
- Formal Vendor Risk Management program
- Security awareness and training programs
- Background screening and confidentiality agreements
- Defined incident escalation and executive reporting structure

## 2. Certifications & Global Regulatory Alignment

Box maintains a broad portfolio of international certifications demonstrating mature operational controls and validated compliance with globally recognized frameworks.

- SOC 1 Type II, SOC 2 Type II, SOC 3
- ISO 27001 Information Security Management
- ISO 27017 Cloud Security Controls
- ISO 27018 Protection of PII in Cloud
- ISO 27701 Privacy Information Management
- FedRAMP Moderate Authorization

- HIPAA support (BAA available)
- GDPR and CCPA regulatory alignment

## 3. Infrastructure & Cloud Security Architecture

Box leverages a resilient cloud-native infrastructure designed for enterprise scalability and high availability. Security is embedded across network, compute, storage, and application layers.

- Encryption in transit via TLS 1.2+
- Encryption at rest using AES-256
- Customer-managed key options (KeySafe)
- Multi-region redundancy and high availability
- Web Application Firewall and DDoS mitigation
- Continuous monitoring, logging, and SIEM integration
- Regular penetration testing and vulnerability assessments

## 4. Secure Software Development Lifecycle (SSDLC)

Security is integrated into the product development lifecycle from design to deployment. Box applies industry best practices and secure coding methodologies.

- OWASP-aligned development standards
- Static and dynamic application security testing
- Peer code review prior to production release
- Dependency and open-source vulnerability monitoring
- Segregation of duties in development workflows
- Responsible disclosure and bug bounty program

## 5. Identity & Access Management (IAM)

Box provides granular identity and access management controls suitable for large enterprise environments with complex collaboration requirements.

- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)
- SAML 2.0 / OIDC Single Sign-On
- Granular folder-level and file-level permissions

- External collaboration governance controls
- Comprehensive audit trails and activity logs
- IP-based access restrictions and device trust controls

## 6. Advanced Data Protection & Encryption

Box enables layered data protection strategies including encryption flexibility and governance enforcement. Organizations can align content protection with internal compliance mandates.

- Customer Managed Encryption Keys (Box KeySafe)
- Integration with Hardware Security Modules (HSM)
- Data classification and governance tools
- Retention management and Legal Hold policies
- Integration with Data Loss Prevention (DLP) systems
- Configurable data residency options

## 7. Privacy & Data Governance Framework

Box operates a global privacy program aligned with major regulatory frameworks. Privacy controls are embedded into system design and operational procedures.

- Data Processing Agreements (DPA)
- Subprocessor transparency and disclosures
- Data subject rights workflows
- Defined retention and deletion mechanisms
- Privacy by Design principles

## 8. Business Continuity & Disaster Recovery

Box maintains structured Business Continuity and Disaster Recovery programs to ensure resilience in the event of service disruptions.

- Formal BCP and DR plans
- Defined Recovery Time Objectives (RTO)
- Defined Recovery Point Objectives (RPO)
- Periodic failover testing
- High availability architecture

- Public service status transparency

## 9. Responsible AI Governance (Box AI)

Box AI capabilities are governed by enterprise-grade security and privacy controls ensuring responsible deployment within regulated environments.

- Logical isolation of customer content
- No model training on customer data without authorization
- Access controls for AI-enabled features
- Monitoring and usage governance
- Alignment with enterprise AI governance frameworks

## 10. Executive Security Summary

Box demonstrates a mature, globally certified security posture suitable for highly regulated industries including financial services, healthcare, public sector, and academic institutions.

The platform combines encryption flexibility, governance depth, audit transparency, and enterprise collaboration controls to support mission-critical content management deployments.