Zendesk Security, Privacy & Compliance Framework

Comprehensive RFP / CISO-Level Overview

This document provides a detailed security and compliance overview intended for enterprise procurement processes, RFP responses, CISO evaluations, and regulatory due diligence. Information is based on Zendesk's official Trust Center documentation.

1. Security Governance & Risk Management

Zendesk maintains a formal Information Security Management System (ISMS) aligned with ISO 27001 standards, including executive oversight, risk committees, documented policies, and continuous monitoring.

- Annual enterprise-wide risk assessments
- Threat modeling for new services
- Third-party vendor risk management program
- Mandatory security awareness training
- Background checks and NDA enforcement
- Formal incident escalation procedures

2. Compliance Certifications & Regulatory Alignment

Framework	Scope & Relevance
SOC 2 Type II	Security, Availability, Confidentiality controls audited independently
ISO 27001:2022	Information Security Management System certification
ISO 27017 / 27018	Cloud security & personal data protection
ISO 27701	Privacy Information Management System (PIMS)
ISO 42001	AI governance and management controls
FedRAMP (LI-SaaS)	US Federal authorization baseline
PCI-DSS	Payment data protection support
HIPAA (via BAA)	Healthcare data protection support

3. Infrastructure & Cloud Security Architecture

- Hosted primarily on AWS with multi-region redundancy
- TLS 1.2+ encryption in transit
- AES-256 encryption at rest
- Web Application Firewall (WAF) and DDoS mitigation
- SIEM monitoring and logging
- Continuous vulnerability scanning and penetration testing

4. Secure Software Development Lifecycle (SSDLC)

- OWASP-aligned secure coding standards
- Static and dynamic code analysis
- Dependency vulnerability scanning
- Peer code reviews before production
- Segregation of duties
- Bug bounty and responsible disclosure program

5. Identity & Access Management (IAM)

- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)
- SAML 2.0 / OIDC Single Sign-On
- IP restriction capabilities
- Granular admin permissions
- Comprehensive audit logs

6. Data Protection & Privacy Framework

- GDPR and CCPA alignment
- Data Processing Agreements (DPA)

- Data subject access workflows
- Defined retention and deletion policies
- Subprocessor transparency
- Data redaction and configuration controls

7. Business Continuity & Disaster Recovery

Zendesk maintains formal Business Continuity Plans (BCP) and Disaster Recovery (DR) procedures, including defined RTO/RPO objectives and tested failover mechanisms. Public dashboards provide uptime transparency.

8. Incident Response & Transparency

- Documented incident lifecycle management
- Forensic investigation procedures
- Customer notification protocols
- Post-incident remediation tracking
- Coordination with external security bodies

9. AI Governance & Responsible AI Controls

AI-powered features are governed under formal control frameworks including monitoring, human oversight, access control, and alignment with ISO 42001 standards where applicable.

10. Executive Security Summary

Zendesk demonstrates a mature enterprise-grade security posture supported by international certifications, independent audits, cloud-native resilience, and strong privacy governance suitable for mission-critical deployments.