2COMS

Recruitment • Staffing • Skill Development

Technology Compliance Monitoring

Policy Owner : Bobby Das (Functional Head - Technology)

Published – 12th September 2025

Version 1.0

1. Objective

2COMS conducts **internal audits and testing** to ensure regular **compliance monitoring** across all technology systems and processes. All cloud storage and data reside with Zoho India Datacenter (**ISO/IEC 27001 certified,** SOC2 Type 2 Compliant**)** and is under Zoho purview as it's a SaaS environment.

- Our aim is to validate compliance with **internal IT policies** and **regulatory requirements**. For hosted data, **Zoho's global compliance frameworks**, particularly for data hosted in Zoho's India Datacenters.
- Internal audit processes are not formally documented but run to ensure continuous monitoring. Incase of incidents or any gaps identified, Zoho support is formally informed over email to initiate a case and is taken up as per standard SLAs.
- This monitoring provides assurance to management, regulators, and clients that **data security, privacy, and integrity** are maintained.

---

2. Scope

- **Systems & Applications**: Cloud hosted Business-critical applications in Zoho environment.
- **Zoho Environment**: Data hosted in Zoho's India Data Centers, aligned with their global compliance commitments.
- **Infrastructure**: Cloud storage, databases, and integrations with Zoho services.
- **Data Security**: Data residency, transfer, and encryption as per Zoho Global Compliance.
- **Third-Party Vendors**: SaaS integrations, contractual obligations, and Zoho's sub-processor policies.

---

3. Monitoring & Testing Activities

a) Access Control & Identity Management

- Review user access to Zoho applications and integrations.
- Test single sign-on (SSO) and multi-factor authentication enforcement.
- Verify role-based access aligned with segregation of duties.

b) Data Security & Privacy

- Confirm encryption at rest/in transit as per Zoho's Security Practices.
- Test backup and recovery of Zoho data as performed by Zoho support Team.

c) Application & Infrastructure Security

- Audit Zoho app configurations for compliance with internal policies.
- Conduct vulnerability assessments on integrations with Zoho APIs.
- Verify patching and change management for connected systems.

d) Incident Response & Logging

- Review incident logs generated by Zoho services (via Zoho Security Practices).
- Test internal incident response escalation mapped to Zoho's shared responsibility model.

---

4. Testing Methods

- **Policy & Document Review**: Internal IT/Compliance policies + Zoho Compliance Repository.
- **Sampling & Interviews**: Verification of Zoho app users, admins, and IT stakeholders.

---

5. Audit Reporting

- **Findings**: Sharing of findings with Zoho on any Non-compliance or control gaps.
- **Impact/Risk Rating**: Based on criticality of Zoho-hosted data.
- **Root Cause**: Policy, process, or configuration issues as per Zoho Support Team.
- **Recommendations**: Mitigation aligned with Zoho's best practices and compliance standards.
- **Management Response**: Action owners in Zoho Team and remediation timelines.

---

6. Follow-Up & Continuous Monitoring

- Leverage Zoho's built-in audit trail and compliance reports for continuous monitoring.
- Track remediation through compliance dashboards and regular reviews with the cloud hosting and data teams of Zoho Support Team.

🔗 Key References for Zoho Compliance:

- Zoho Global Compliance Overview
- Zoho India Data Center Compliance
- Zoho Security Practices