ACOMdev, LLC
https://www.acomdev.com
+1.317.331.3038

ACOMdev - Technical and Organizational Measures
Aligned with ISO 27001 and SOX3

Contents

1. Aligned with ISO/IEC 27001 2
2. Organizational Measures (Administrative & Governance Controls) 2
Key Organizational Measures 2
3. Technical Measures (Logical & System Controls) 3
Key Technical Measures 3
4. Mapping TOMs to ISO 27001 Requirements 4
5. Evidence Expected by Auditors 4
6. Aligned with Sarbanes-Oxley Act (SOX – Sections 302 & 404) 5
7. Organizational Measures (Governance & Process Controls) 5
Key Organizational Measures for SOX 5
8. Technical Measures (IT General Controls – ITGCs) 6
Key Technical Measures for SOX 6
9. Mapping TOMs to SOX Sections 7
10. Evidence Expected by SOX Auditors 7

1. Aligned with ISO/IEC 27001

Technical and Organizational Measures (TOMs) are the **controls implemented to protect the confidentiality, integrity, and availability (CIA)** of information. ISO/IEC 27001 requires organizations to **define, implement, monitor, and continually improve** these measures as part of their **Information Security Management System (ISMS)**.

TOMs are derived from:

- **Risk assessments**
- **Legal, regulatory, and contractual requirements**
- **Business objectives**
- **Annex A controls (ISO/IEC 27001:2022)**

---

2. Organizational Measures (Administrative & Governance Controls)

Organizational measures define **how security is governed, managed, and enforced** across the organization.

Key Organizational Measures

- **Information Security Policies**
  - Information Security Policy
  - Acceptable Use Policy
  - Access Control Policy
  - Data Classification & Handling Policy
- **Risk Management**
  - Formal risk assessment and treatment methodology
  - Documented risk register
- **Roles & Responsibilities**
  - Defined security roles (e.g., ISMS owner, asset owners)
  - Segregation of duties
- **Human Resources Security**
  - Background checks where legally permitted
  - Security awareness and training
  - Disciplinary process for violations
- **Supplier & Third-Party Management**
  - Vendor risk assessments
  - Security requirements in contracts

- **Incident Management**
    - Incident response procedures
    - Logging, escalation, and post-incident review
- **Business Continuity & Disaster Recovery**
    - Business Impact Analysis (BIA)
    - Tested continuity and recovery plans
- **Compliance & Audit**
    - Internal audits
    - Management reviews
    - Corrective actions and continual improvement

Relevant ISO 27001 Annex A domains (2022):

- A.5 – Organizational controls
- A.6 – People controls

3. Technical Measures (Logical & System Controls)

Technical measures are **technology-based safeguards** that enforce security at the system and infrastructure level.

Key Technical Measures

- **Access Control**
    - Role-based access control (RBAC)
    - Least privilege
    - Multi-factor authentication (MFA)
- **Identity & Authentication**
    - Centralized identity management
    - Secure credential storage
- **Cryptography**
    - Encryption of data at rest and in transit
    - Key management procedures
- **Network Security**
    - Firewalls and network segmentation
    - Intrusion detection/prevention systems (IDS/IPS)
- **Endpoint Security**
    - Anti-malware
    - Device hardening
    - Patch management
- **Logging & Monitoring**
    - Security event logging
    - SIEM or centralized log review

- **Vulnerability Management**
  - Regular vulnerability scanning
  - Remediation tracking
- **Backup & Recovery**
  - Automated, encrypted backups
  - Regular restore testing
- **Secure Configuration & Development**
  - Secure baselines
  - Change management
  - Secure SDLC (if applicable)

Relevant ISO 27001 Annex A domains (2022):

- A.7 – Physical controls
- A.8 – Technological controls

4. Mapping TOMs to ISO 27001 Requirements

ISO 27001 Clause	TOM Focus
Clause 6	Risk-based selection of TOMs
Clause 7	Competence, awareness, documentation
Clause 8	Operational control of security measures
Clause 9	Monitoring, measurement, internal audit
Clause 10	Continual improvement

5. Evidence Expected by Auditors

ISO 27001 auditors typically look for:

- Documented policies and procedures
- Risk assessment and treatment records
- Technical control configurations (screenshots, logs)
- Training records
- Incident and audit logs
- Evidence of monitoring and review

6. Aligned with Sarbanes-Oxley Act (SOX – Sections 302 & 404)

Under SOX, **Technical and Organizational Measures** are the **controls implemented to ensure the integrity, accuracy, security, and reliability of financial reporting systems and data**. While SOX is not a cybersecurity standard, it **mandates effective Internal Controls over Financial Reporting (ICFR)**, which necessarily include both organizational and technical security controls.

---

7. Organizational Measures (Governance & Process Controls)

Organizational measures establish **management oversight, accountability, and procedural discipline** over financial systems and data.

Key Organizational Measures for SOX

- **Internal Control Framework**
  - Adoption of a recognized framework (commonly COSO)
  - Documented control objectives and control owners
- **Policies & Procedures**
  - Financial reporting policies
  - IT General Controls (ITGC) policy
  - Change management policy
  - Access management policy
- **Segregation of Duties (SoD)**
  - Separation of authorization, execution, and review
  - Conflict analysis and mitigation
- **Management Oversight**
  - Executive certification of controls (SOX §302)
  - Periodic control reviews and sign-offs
- **Risk Assessment**
  - Identification of risks to financial reporting
  - Control design and remediation plans
- **Change Management Governance**
  - Formal approval, testing, and documentation of system changes
- **Third-Party Oversight**
  - Controls over outsourced financial or IT services
  - SOC 1 report review where applicable
- **Audit & Compliance**

    - Internal control testing
    - Deficiency tracking and remediation
    - External auditor coordination

8. Technical Measures (IT General Controls – ITGCs)

Technical measures enforce **system-level controls** that protect financial data and support reliable reporting.

Key Technical Measures for SOX

- **Access Controls**
    - Role-based access to financial systems
    - Least privilege enforcement
    - Periodic access reviews
- **Authentication & Identity Management**
    - Unique user IDs
    - Strong authentication mechanisms
- **Change Management Controls**
    - Restricted access to production systems
    - Version control and change logs
- **System Logging & Monitoring**
    - Audit trails for financial transactions
    - Logging of privileged activities
- **Data Integrity Controls**
    - Input validation
    - Automated reconciliations
    - Error detection and correction mechanisms
- **Backup & Recovery**
    - Regular, tested backups of financial systems
    - Disaster recovery capabilities
- **Configuration Management**
    - Secure baseline configurations
    - Controlled system parameter changes
- **Interface & Batch Controls**
    - Reconciliation of inbound/outbound data
    - Exception handling for failed jobs

9. Mapping TOMs to SOX Sections

SOX Section	TOM Focus
Section 302	Executive accountability, disclosure controls
Section 404	Design and operating effectiveness of ICFR
PCAOB Auditing Standards	Evidence, testing, and documentation

10. Evidence Expected by SOX Auditors

Auditors typically expect:

- Control narratives and flowcharts
- Risk & control matrices (RCMs)
- Access review evidence
- Change management records
- System logs and audit trails
- Management sign-offs
- Deficiency remediation tracking