Cyolo

How Cyolo Helps You Achieve Compliance: ISO/IEC 27001

Achieving ISO/IEC 27001 certification can help many companies improve their information security management practices, comply with legal and regulatory requirements, build customer trust, gain a competitive advantage, and improve their overall business operations. As an internationally recognized standard, ISO/IEC 27001 sets out the requirements for an Information Security Management System (ISMS). The standard is based on the Plan-Do-Check-Act (PDCA) model and is designed to help organizations of all sizes and types establish, implement, maintain, and continually improve their ISMS. By doing so, they usually make measurable progress towards their organizational goals and dramatically improve their cybersecurity.

ISO/IEC 27001 specifies a framework for managing and protecting sensitive information and data assets. It provides a systematic approach for identifying and managing risks to the confidentiality, integrity, and availability of information. The standard covers a wide range of security controls, including physical, technical, and organizational measures, and it provides a comprehensive risk management process that includes risk assessment, risk treatment, and risk monitoring and review.

Cyolo can support an enterprise in an ISO/IEC 27001 audit by providing solutions that help them comply with the standard. Cyolo provides a critical layer of security to an enterprise's network, applications, and data by ensuring that only authorized users are allowed to access them.

SECURE SOLUTION

With its zero-trust access solution, Cyolo delivers three layers of controls to better manage scenarios in which user access could cause enormous damage to the business. Deploying Cyolo materially helps support ISO/IEC 27001 compliance during an audit.

HERE ARE SOME WAYS THAT CYOLO SUPPORTS ISO/IEC 27001 COMPLIANCE:

- **Implement access control mechanisms:** Cyolo implements control mechanisms that limit access to enterprise resources based on user identity, device posture, and other contextual information.
- **Provide secure remote access:** Cyolo provides secure remote access to enterprise resources and critical infrastructure, enabling employees to work from anywhere while maintaining security.
- **Help manage identity and access:** Cyolo manages user identities and access, ensuring that only authorized users are granted access.
- **Provide visibility and analytics:** Cyolo provides visibility and analytics into user behavior and access patterns, enabling the enterprise to detect and respond to security threats. Additional layers of session monitoring or recording, along with full access logs, ensure compliance with any regulatory reporting needs

HOW CYOLO HELPS

Cyolo is designed to give users access to the resources they need while maintaining the zero-trust model. It is built to support the real world, enabling companies to protect their entire network. With Cyolo, you can securely access the resources you need to get your work done, while keeping your network and data safe.

ACCESS CONTROLS

- **Multi-Factor Authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- Control **Activity Permissions**
- **Terminate Connection** once work is completed

OVERSIGHT CONTROLS

- Full **Audit Trail** & complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery** for **Business Continuity**

(Figure 1. Cyolo Zero-Trust Access controls that support compliance with ISO/IEC 27001)

CYOLO ALIGNMENT WITH ISO/IEC 27001 INFORMATION SECURITY CONTROLS

ORGANIZATIONAL CONTROLS
5.8 Information security in project management
5.9 Inventory of information and other associated assets
5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the information and communication technology (ICT) supply chain
5.22 Monitoring, review and change management of supplier services
5.23 Information security for use of cloud services
5.26 Response to information security incidents*
5.28 Collection of evidence*
5.30 ICT readiness for business continuity*
5.31 Legal, statutory, regulatory and contractual requirements*
5.33 Protection of records
5.34 Privacy and protection of personal identifiable information (PII)
5.36 Compliance with policies, rules and standards for information
5.37 Documented operating procedures
PEOPLE CONTROLS
6.5 Responsibilities after termination
6.7 Remote working

TECHNOLOGICAL CONTROLS
8.1 User end point devices*
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.7 Protection against malware
8.15 Logging
8.16 Monitoring activities
8.20 Networks security
8.21 Security of network services
8.22 Segregation of networks
8.23 Web filtering*
8.24 Use of cryptography*
8.26 Application security requirements*
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management

For brevity, ISO/IEC 27001 Section 7 (Physical Security Controls) was excluded from this document.
**Cyolo can augment compliance in this area as a part of a wider strategy.*