

Path to ISO 27001 Compliance with Timus SASE

timus
ZERO TRUST NETWORK PROTECTION

Introduction

This whitepaper outlines how Timus SASE assists organizations in achieving compliance with ISO 27001 ISMS Standard control points. Specifically, we will focus on how Timus SASE supports the fulfillment of control points which address critical aspects of threat intelligence, access control, supplier management, cloud services, evidence collection, policy compliance, and remote working security.
By leveraging Timus SASE, organizations can streamline their compliance efforts and strengthen their overall information security posture.
Timus SASE itself is SOC 2 Type 2 and ISO 27001 Compliant, and uses AES 256 bit encryption.

© Timus Networks, Inc. 2025. All Rights Reserved.



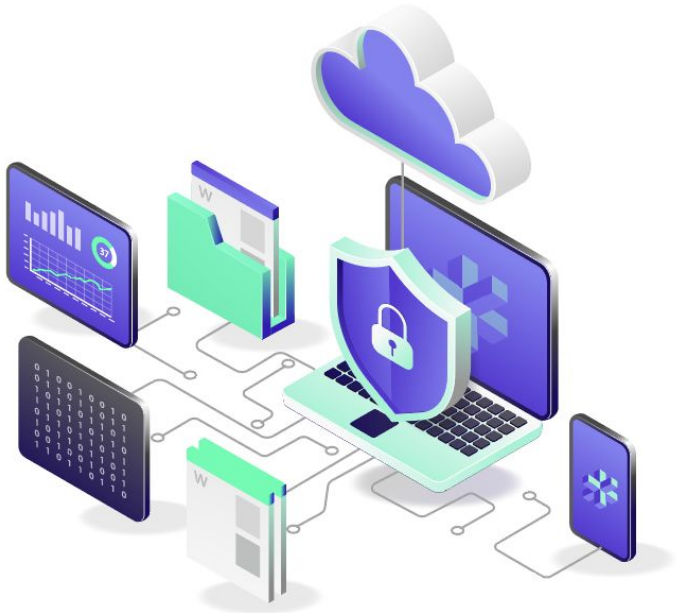
1. The Importance of ISO 27001 ISMS Compliance

The ISO 27001 ISMS standard provides a systematic approach to managing information security risks within organizations.
Compliance with ISO 27001 ISMS ensures the protection of sensitive information, strengthens customer trust, and enhances overall operational resilience.

Timus SASE Overview:

Timus SASE is a comprehensive network security product designed to provide secure connectivity for hybrid workforce of organizations.

It provides a centralized platform for managing and monitoring various aspects of information security, including risk assessment, policy enforcement, incident response, and compliance tracking.



© Timus Networks, Inc. 2025. All Rights Reserved.



2. Fulfilling ISO 27001 ISMS Standard Annex A Control Points

2.1. Threat Intelligence

Timus SASE facilitates the collection and analysis of information security threats to produce threat intelligence.

It integrates with external threat intelligence feeds and employs advanced analytics to identify potential threats.

Timus SASE enables organizations to proactively respond to emerging threats and implement appropriate countermeasures.

2.2. Access Control

Timus SASE enables organizations to establish and implement rules for controlling physical and logical access to information and associated assets.

It supports robust authentication mechanisms, role-based access control, and privileged access management.

Organizations can define access control policies based on business and information security requirements and enforce them consistently.



© Timus Networks, Inc. 2025. All Rights Reserved.

2.3. Monitoring, Review, and Change Management of Supplier Services

Timus SASE provides capabilities to monitor, review, evaluate, and manage changes in supplier information security practices and service delivery.

It offers a centralized repository for documenting supplier agreements, conducting risk assessments, and tracking compliance.

Timus SASE facilitates supplier relationship management, ensuring that suppliers adhere to information security requirements.

2.4. Information Security for Use of Cloud Services

Timus SASE assists organizations in establishing processes for acquiring, using, managing, and exiting from cloud services.

It helps define information security requirements specific to cloud services and ensures their integration into the organization's overall ISMS.

Timus SASE enables organizations to assess the security posture of cloud service providers and monitor compliance with relevant controls.



© Timus Networks, Inc. 2025. All Rights Reserved.

2.5. Collection of Evidence



Timus SASE supports the establishment and implementation of procedures for identifying, collecting, acquiring, and preserving evidence related to information security events.

It provides incident management capabilities to track and document security incidents, enabling organizations to collect evidence effectively.

Timus SASE helps organizations maintain an audit trail of events, facilitating compliance with legal and regulatory requirements.

2.6. Compliance with Policies, Rules, and Standards for Information Security

Timus SASE offers a centralized policy management module to define, review, and enforce information security policies, rules, and standards.

It provides automated workflows for policy review and approval processes and tracks compliance with policy requirements.

Timus SASE ensures that compliance with information security policies is regularly reviewed, reducing the risk of policy violations.

2.7. Remote Working

Timus SASE assists organizations in implementing security measures to protect information accessed, processed, or stored outside the organization's premises during remote working.

It provides secure remote access mechanisms, multi-factor authentication, encrypted communication channels (Timus uses AES-256 bit encryption method for maximum security), and device management capabilities.

Timus SASE helps organizations enforce remote working security policies and monitor compliance with relevant controls.



© Timus Networks, Inc. 2025. All Rights Reserved.



3. Conclusion

Timus SASE serves as a valuable tool for organizations seeking ISO 27001 ISMS compliance.

By leveraging Timus SASE, organizations can effectively address key control points such as threat intelligence, access control, supplier management, cloud services, evidence collection, policy compliance, and remote working security.

Timus SASE streamlines compliance efforts, enhances information security resilience, and strengthens overall risk management practices.

Incorporating Timus SASE into an organization's information security program empowers them to achieve and maintain ISO 27001 ISMS compliance, enabling robust protection of information assets and maintaining stakeholder trust.

timus

timusnetworks.com

About Timus

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.