Thoropass™

Compliance Overview

Step-by-Step ISO 270011

thoropass.com →

1. Determine framework scope

Identify the teams and systems within the scope of ISO 27001 requirements. If you're a smaller organization, we recommend including everyone.

2. Perform a gap analysis

The first step to any strategic compliance implementation is executing a gap analysis. Your team will need to determine which controls have already been fulfilled by your organization, and which ones still need to be implemented or optimized. Based on your findings, you'll be able to move onto the next step.

3. Create network architecture and data flow diagrams

By creating diagrams of your network architecture and how the data flows through your systems, you'll gather an understanding of where, when, and how data could be vulnerable.

4. Build an asset inventory

An asset inventory should depict each aspect of your organization's technology. From databases to data warehouses, web applications, and accounting systems, the inventory is meant to identify the types of data, who has access to that data, and what risk is incurred in each.

5. Establish a remediation plan

This is your strategic approach to implementing the ISO 27001 compliance framework. Our experts recommend slotting in heavy technical tasks first, like endpoint security, and moving through to the easier lifts.

6. Implement ISO 27001 controls

To pass an ISO 27001 audit, you'll need to implement requirements outlined in your strategic remediation plan. These controls could include:

- Screening for candidates
- Formalize onboarding and termination processes
- Organize and hold information security awareness training
- Clean desk policy
- Cryptographic security controls
- Endpoint security

To get a better understanding of all the controls outlines by ISO 27001, download our guide.

7. Perform a risk assessment

Before stepping into the first audit cycle, your compliance team will need to assess and accept the amount of risk associated with control efficacy, or lack thereof. This helps a business understand vulnerabilities to risks like fraud, data loss, or regulatory risk, and plan to answer questions from auditors.

8. Demonstrate readiness

Round one of the ISO 27001 audit cycle. You'll need to complete an internal readiness assessment by an independent team or auditor. This assessment will determine if your organization and ISMS are ready for the formal, external audit.

9. Submit ISMS for audit

Showtime. An ISO 27001 audit involves submitting your newly developed ISMS for inspection. Auditors will look for a full story of how your organization operates securely and actively protects internal and external information.

10. Maintain ISO 27001 certification

ISO 27001 requires regular security audits, every twelve months. In the meantime, continue to maintain and monitor controls, and implement new ones as your business grows.

Let Thoropass guide you from zero to audit for ISO 27001.

Thoropass™

Get in touch →