TRANSITION GUIDE: FROM ISO/IEC 27001:2013 TO ISO 27001:2022

INFO@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

Table of Contents

Purpose Statement

This guide was created to outline the procedures that certified organizations must follow when transitioning from ISO/IEC 27001:2013 to ISO/IEC 27001:2022. This document aims to ensure a smooth and efficient transition process in compliance with the updated standards.

Following these guidelines will help maintain the integrity of your Information Security Management System (ISMS) and continue to safeguard your organization's information assets.

Key Information

Updated Standard Issue: The new ISO/IEC 27001 standard was issued in October 2022, marking the beginning of the transition period. During this period, clients certified under ISO/IEC 27001:2013 must update their Information Security Management System (ISMS) to conform to the new standard. The transition period ends on October 31, 2025.

According to IAF MD 26, “All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period.” Updating to the new standard involves aligning your ISMS with revised control objectives and ensuring that new controls are appropriately implemented. This includes addressing gaps identified in the gap analysis and updating documentation, policies, and procedures to reflect the changes.

Certification Deadline: To remain certified, your ISMS must complete a transition audit and have the certificate issued by October 31, 2025. Any client needing to complete the transition audit by this date will have their ISO/IEC 27001:2013 certificate revoked, and the ISMS will no longer be certified.

This deadline underscores the importance of timely preparation and execution of the transition plan. It is crucial to begin the process well in advance to ensure all aspects of the ISMS are adequately addressed and compliant with the new standard by the deadline.

Transition Audit Program

We can assess your ISMS under the new version during your next scheduled assessment if it can be completed by October 31, 2025. If the transition audit can't be included with another already scheduled audit then it will need to be a separate Transition Audit completed by Oct 31, 2025.

There are three ways to complete the transition audit:

1. **During the Surveillance Audit:** Combine the transition audit with your regular surveillance audit. This approach allows the transition to seamlessly integrate into the ongoing review of your ISMS, minimizing disruption while ensuring compliance.
2. **During the Recertification Audit:** Integrate the transition audit with your recertification audit. This method provides an opportunity to comprehensively review and update your ISMS, aligning it with the new standard as part of the recertification process.
3. **Separate Transition Audit:** Conduct a separate transition audit independent of other scheduled audits. This option offers flexibility in scheduling, is a separate cost under their contract with a certifying body, and allows for focused attention on the transition requirements without the constraints of concurrent audit activities.

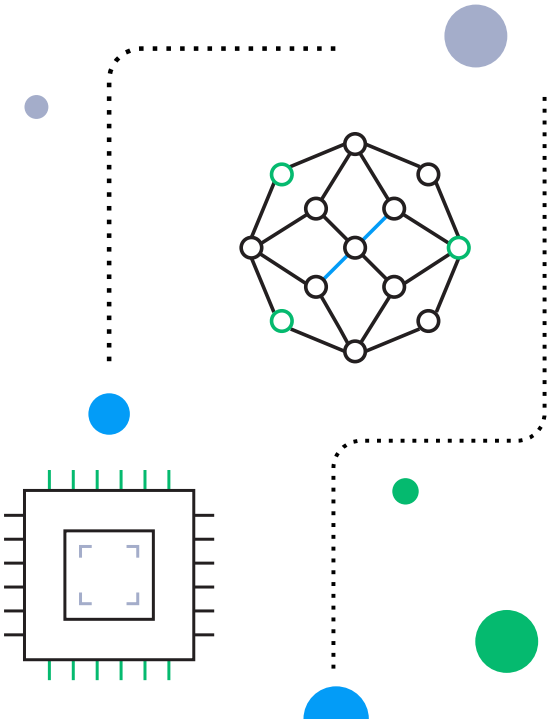
Choosing the appropriate method depends on your organization's audit schedule, resource availability, and ISMS readiness for the transition.

Conducting the Transition Audit

The transition audit will involve the following:

1. **Interviews with Personnel:** Engage with your team to assess understanding and implementing new standards. These interviews will help determine how well your staff comprehends and applies the updated controls and policies.
2. **Documentation Review:** Examine the documentation related to your ISMS, including policies, procedures, and records. The review ensures that all necessary documents are updated and comply with the new standards, reflecting accurate and current practices.
3. **Inspection of Implemented Controls:** Verify the effectiveness of implemented controls against the new standards. This involves checking the controls' implementation, effectiveness, and alignment with the ISO 27001 and 27002 standards as well as organization policies.

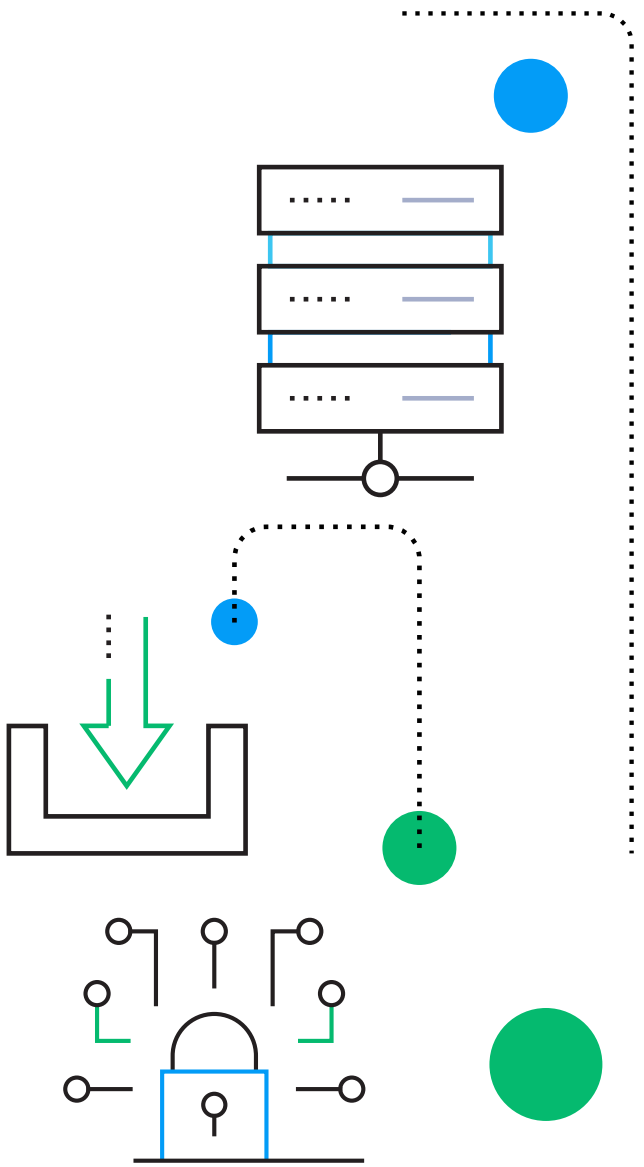
A thorough and detailed audit process will ensure that your ISMS meets the new standard's requirements and that all controls are effective and adequately implemented.



Audit Timing and Fees

- Based on ISO's auditor-day calculations, if conducted with a surveillance or recertification audit, there will be a slight increase in time required, at least half a day. This will also necessitate an accompanying rise in fees. The additional time ensures a thorough review and verification of the transition activities.
- If conducted as a separate audit, a contract must be completed, and the expiration of the current certification cycle will remain unchanged. Conducting a separate audit provides flexibility but may incur additional costs and scheduling considerations.

Planning for these timing and fee adjustments is crucial for budgeting and scheduling, ensuring the transition process is adequately resourced.



Transition Audit Requirements

The transition audit shall include, but is not limited to:

1. Gap Analysis

Review the gap analysis between ISO/IEC 27001:2022 and your current ISMS, identifying necessary changes to include the 11 new controls implemented under the new version. This analysis helps pinpoint areas that need updating and ensures that all changes are systematically addressed.

2. Updated Statement of Applicability (SoA)

Ensure the SoA reflects the new standard requirements. All Policies will need to be updated to reflect the new version and new controls. The SoA should accurately list all applicable controls and their implementation status, demonstrating compliance with the new standard.

3. Risk Treatment Plan

Update the risk treatment plan as needed. The plan should address any new risks identified in the gap analysis and ensure that all risks are adequately managed, mitigated and remapped.

4. Implementation and Effectiveness

Assess the implementation and effectiveness of new or changed controls determined by the client. This step ensures that all controls are implemented and achieve their intended security objectives effectively.

These requirements ensure a comprehensive transition process, aligning your ISMS with the updated standard and maintaining effectiveness.

Transition Audit Requirements

Clients currently certified under ISO/IEC 27001:2013 must submit the transition application for ISO/IEC 27001:2022 at least three months before the surveillance or recertification audit in which they wish to complete the transition audit.

This timeline ensures sufficient time for reviewing and processing the application, scheduling the audit, and preparing for the transition audit. Early submission helps avoid delays and ensures the transition is completed within the required timeframe.

Transition Certification Decision

The transition certification decision will be based on the transition audit results. This decision process will follow Compass Rose's established certification process, ensuring that all transition requirements are met and that the ISMS complies with ISO/IEC 27001:2022.

This decision process involves a thorough review of the audit findings, verification of compliance with the new standard, and approval of the transition by the certification body. Successful completion of the transition audit will result in the issuing of the updated ISO/IEC 27001:2022 certificate.

Questions

Please get in touch with our support team if you have any questions or need further assistance. We are here to help you navigate this transition smoothly and confidently so that you can maintain your certification. Our team of experts is available to provide guidance, support, and resources to ensure a successful transition to the new standard.

360ADVANCED

866-418-1708

INFO@360ADVANCED.COM