AssureTechnical

ISO 27001:2022 Upgrade Guide

Introduction

ISO 27001, the globally recognised standard for information security management, has recently been updated to its 2022 version.

This update includes revised requirements and controls to better align with the evolving landscape of information security threats and technologies. It particularly focuses on changes within the specific security controls an organisation should implement.

The deadline for implementing ISO 27001:2022 is rapidly approaching. From **31st October 2025**, certifications based on the older ISO 27001:2013 standard will no longer be valid. To maintain certification and compliance, organisations must complete the transition in time. However, many are finding the process challenging.

Are you struggling with ISO 27001 compliance? Don't worry—Assure Technical provides award-winning ISO 27001 Consultancy services. We're here to support you, every step of the way.

The Challenges of Upgrading to ISO 27001:2022

Transitioning to the ISO27001 2022 standard is not without its hurdles. Common challenges include:

Understanding the New Requirements - Interpreting the changes and how they apply to your organisation can be complex.

Updating Policies and Procedures - Revising documentation to align with the updated framework requires time and expertise.

Resource Constraints - Many businesses lack the internal capacity to manage the transition effectively while trying to balance other pressing business priorities.

Meeting Tight Deadlines - The October 31st 2025 deadline is fast approaching!

Key Updates

One of the most significant updates in ISO 27001:2022 relates to Annex A. These include:

Consolidation of Controls - The number of controls has been consolidated from 114 to 93.

New Thematic Structure - The 14 clauses have been consolidated into 4 key themes. These are:

- People
- Organisational
- Technological
- Physical

11 New Controls Introduced - Details are listed overleaf

Trustpilot
★★★★★
Excellent 4.9 out of 5

How Assure Technical Can Help

At Assure Technical, we understand the complexities of achieving ISO 27001:2022 certification and can help make the upgrade process seamless. Our experienced Lead Auditors provide tailored support to ensure you meet your deadline and maintain compliance with minimal disruption.

Here’s how we can assist:

1. Internal Audits: We conduct pre-certification audits to identify any areas needing improvement before the external assessment, reducing the risk of non-compliance.

2. Gap Analysis: We assess your current security framework against the updated standard, identifying any gaps and providing clear recommendations for compliance.

3. Documentation Support: Our team helps you update policies, procedures, and risk assessments to align with the new requirements, ensuring nothing is overlooked.

4. Implementation Assistance: We guide you through the practical steps needed to meet the updated controls, offering hands-on support where necessary.

5. Ongoing Compliance Support: Following certification, we offer continued support to help you maintain compliance and adapt to future changes.

Don’t Leave It Too Late – Upgrade to 27001 2022 Now!

ISO 27001 compliance is a critical component of your organisation’s security strategy. With the transition deadline approaching, now is the time to act. By partnering with Assure Technical, you can ensure a smooth, stress-free upgrade that keeps your business secure and competitive.

The 11 New Controls

- **A5.7** – Threat Intelligence – Implement processes to collect and analyse threat intelligence.
- **A5.23** – Information Security for Cloud Services – Establish policies for acquiring, managing, and exiting cloud services.
- **A5.30** – ICT Readiness for Business Continuity – Maintain and test ICT readiness in line with business continuity objectives.
- **A7.4** – Physical Security Monitoring – Continuously monitor premises for unauthorised physical access.
- **A8.9** – Configuration Management – Establish and maintain security configurations for hardware, software, and networks.
- **A8.10** – Information Deletion – Implement secure deletion processes for information that is no longer required.
- **A8.11** – Data Masking – Use data masking to protect sensitive information in compliance with organisational policies.
- **A8.12** – Data Leakage Prevention – Apply data leakage prevention measures to protect sensitive data.
- **A8.16** – Monitoring Activities – Continuously monitor networks, systems, and applications for anomalies.
- **A8.23** – Web Filtering – Manage access to external websites to reduce exposure to malicious content.
- **A8.28** – Secure Coding – Apply secure coding principles in software development.

GET IN TOUCH WITH OUR CYBER EXPERTS

Telephone: **+44 (0)1684 252 770**
Email: **hello@assuretechnical.com**
www.assuretechnical.com

Trustpilot
★★★★★
Excellent 4.9 out of 5