INFORMATION SECURITY: ISO 27001 HAS BEEN UPDATED

"ARE YOU READY?"

Your guide to a successful ISO 27001:2022 transition

LRQA

Introduction

In February 2022, ISO 27002:2022 – the standard which provides the best practice controls that organizations can implement to improve security – was updated. As a result, a new version of ISO 27001 – the international standard which outlines the requirements of an information security management system (ISMS) – was also published on October 25, 2022.

The new version of the standard features the controls outlined by ISO 27002:2022, and organizations will need to revisit their risk assessment to determine whether updates or new risk treatments need to be implemented.

Here, we outline ten key steps that an ISO 27001 certified organization can take to successfully transition to the new standard.

Ten steps to a successful ISO 27001:2022 transition

1 Understand the changes

2 Assess your training requirements

3 Perform a Gap Analysis on existing controls

4 Revisit your Risk Assessment

5 Update your Risk Treatment Plan (RTP)

6 Update your Statement of Applicability (SOA)

7 Book your transition audit

8 Complete your audit and implement any changes

9 Promote your ISO 27001:2022 certification

10 Focus on continual improvement

1. Understand the changes

Build an understanding of ISO 27002:2022 as the new security controls feature in Annex A of ISO 27001. This is the most significant revision to the new standard.

ISO 27002:2022 has been restructured, featuring 93 controls instead of 114, split between 4 different themes:

- Organizational
- People
- Physical
- Technological

53 controls from the previous version have been merged into 24 in ISO 27002:2022, with 11 new controls added. It should also be noted that the majority of controls are subject to some form of text change which could impact how the standard is interpreted and implemented.

2. Assess your training requirements

Create a training program for your team members to build their knowledge around the standard and ensure they can implement the changes effectively.

Updated versions of LRQA's ISO 27001 training courses will be available shortly with options for all experience levels including:

- An introduction to ISO 27001:2022
- ISO 27001:2022 Implementation
- ISO 27001:2022 Internal Auditor
- ISO 27001:2022 Auditor Conversion
- ISO 27001:2022 Lead Auditor Conversion
- ISO 27001:2022: Management Briefing

We can deliver our courses through multiple online, in-person or blended learning styles depending on what works best for you and your team members.

3. Perform a Gap Analysis on existing controls

A Gap Analysis that assesses your existing controls and risk treatments against those included in ISO 27002:2022 will help you identify focus areas that need to be addressed prior to your transition to ISO 27001:2022.

Annex B of ISO 27002:2022 is a good starting point as it includes a useful comparison of all available controls and how they correspond to those in the previous version (ISO 27002:2013). The updated standard divides controls into four key themes – organizational, people, physical, and technological – and we'd recommend forming a specialist team that can own and provide insight around these areas.

LRQA provide s optional pre-assessment services that are carried out by expert auditors in the form of a Gap Analysis or Preliminary Audit. We'll look at your existing controls and wider ISMS identifying any areas that need attention.

4. Revisit your Risk Assessment

It's necessary to check that your risk assessment, along with its objectives and context, remains well aligned with your business and risk appetite - if it isn't, changes need to be made. You may wish to consult ISO 27005 – the international standard that outlines the procedures for conducting an information security risk assessment.

5. Update your Risk Treatment Plan (RTP)

You'll need to update the RTP to reflect your decisions regarding threat response, selecting appropriate controls from the updated version of ISO 27002, which feature in Annex A of ISO 27001:2022.

You may wish to engage LRQA to perform an additional Gap Analysis at this point to ensure that the controls selected are justified and effective. Our independent insights give you confidence in your organization's readiness, and Nettitude, our cybersecurity specialists, can provide advice and guidance around technical controls and services.

6. Update your Statement of Applicability (SOA)

It's crucial to update your SOA to reflect the evidence and justification relating to the inclusion and exclusion of any controls or policies. You'll also need to highlight whether your business has implemented any controls in line with the RTP. If the answer is yes, a robust internal audit program should be carried out to assess the effectiveness of your activities.

7. Book your transition audit

By this point, the changes you've implemented will have strengthened your management system, information security and wider cyber resilience. It's time to get in touch with LRQA to discuss your dedicated transition audit, which can be carried out as a standalone activity or in line with any other scheduled visit.

Organizations with existing ISO 27001:2013 certification will have until October 2025 to transition to the new standard.

Get in touch →

8. Complete your audit and implement any changes

Your auditor will assess your ISMS and supporting documentation to determine whether it meets the requirements of ISO 27001:2022 – with a special focus on the changes to the controls in Annex A. Upon completion, you'll receive your Audit Report, which features your auditor's feedback and any findings that need to be addressed before certification is awarded.

9. Promote your ISO 27001:2022 certification

Your certification demonstrates a commitment to internationally recognized best practices and continual improvement – helping you win new business and meet customer demands. You can have confidence that your ISMS is robust and effective – utilizing controls and risk treatments that reflect the changing threat landscape.

10. Focus on continual improvement

Post-certification, it's important to keep the momentum to ensure that your ISMS remains effective and well maintained. We'll carry out surveillance audits annually which will focus on the status of your system – we'll also be looking to ensure that continual improvements are being delivered.

Our ISO 27001:2022 training and audit services

Training

Build your knowledge of ISO 27001:2022 with a range of courses designed for different experience levels – delivered via multiple learning styles.

Gap analysis

An optional service where one of our expert auditors will help you identify any critical, high-risk, or weak areas of your system prior to your transition audit.

Transition audit

We'll assess your ISMS in line with the requirements of ISO 27001:2022 – with a particular focus on the Annex A controls and how they impact your system.

Integrated audits

If you've implemented multiple management systems, you could benefit from an integrated audit and surveillance program which is more efficient and cost-effective.

Working with you to target every aspect of cybersecurity

Our deep experience in assurance, combined with award-winning cybersecurity services and threat-led intelligence, enables us to deliver bespoke insights into – and protection from – the unique threats facing your business. Keeping you one step ahead of cyber risk, today, tomorrow and beyond.

We provide audit, training and certification services against the world's leading international standards and schemes, complemented by a wide range of advanced cybersecurity services delivered by our specialists, Nettitude.

We work collaboratively with your business – helping you to identify the specific threats you face and build strategies to mitigate them. We'll work with you to certify your systems, identify vulnerabilities, and help prevent attacks and incidents that could impact your brand integrity, finances and operations.

Information security

Our compliance and certification services help you protect business-critical information and demonstrate internationally recognized best practices.

Find out more ❯

Operational resilience

Be ready to prevent, respond and recover from disruption with our certification, training and governance, risk and compliance services.

Find out more ❯

Cyber threat protection

Stay one step ahead of cyber threats, with tailored solutions that provide a first line of defense and response to all types of cyber attack.

Find out more ❯

LRQA

YOUR FUTURE. OUR FOCUS.

About LRQA:

Bringing together unrivaled expertise in certification, brand assurance and training, LRQA is one of the world's leading providers of food safety and assurance solutions. Working together with farms, fisheries, food manufacturers, restaurants, hotels, and global retailers, we help manage food safety and sustainability risks throughout supply chains and have become a leading global assurance provider.

We're proud of our heritage, but it's who we are today that really matters, because that's what shapes how we partner with our clients tomorrow. By combining strong values, decades of experience in risk management and mitigation and a keen focus on the future, we're here to support our clients as they build safer, more secure, more sustainable businesses.

From independent auditing, certification and training; to technical advisory services; to real-time assurance technology; to data-driven supply chain transformation, our innovative end-to-end solutions help our clients negotiate a rapidly changing risk landscape – making sure they're shaping their own future, rather than letting it shape them.

Get in touch

Visit **www.lrqa.com/us** for more information, email **inquiries-usa@lrqa.com** or call **866 971 5772**

LRQA
2101Citywest Blvd., Suite 100
Houston, TX 77042
United States

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

For more information on LRQA, click **here**.