ISO 27001:2022

Transition Guide

Shelter from the Storm

ISO/IEC 27001:2022

Information Security, Cybersecurity and Privacy Protection

ISO 27001:2013, the world's leading information security standard, has been updated after nine years of being in circulation. During those years, the threat landscape has taken many twists and turns in the last nine years. Information security now extends into our work and everyday lives.

From critical infrastructure, small businesses to educational institutions being targeting by threat actors - it's essential for organisations of every size to protect intellectual property and critical data. The new standard offers a well-organised and flexible approach to build information security resilience in this age of modern cyberattacks and the ever-changing information security risks.

The revision has moderate modifications, but it is important to understand the changes to be prepared for transition. **Read on to discover the changes and get valuable information on how to plan a streamlined transition or first-time implementation.**

How Annex A Controls Have Changed

The most obvious change is the number of documented controls that are reduced from 114 to 93. This was achieved by merging some controls. For instance, three of the 2013 controls were merged into the single control 5.15 Management of access rights. See all changed controls on the next page.

Eleven new controls were added to the 2022 version to bring ISO 27001 up to the present day. Controls are grouped into four 'themes' rather than the 14 clauses used in the 2013 version. Each control will only appear in one theme and have five attributes.

The Key Changes

WHY THE CHANGE?

The Standard was updated to address best practices for managing information security risks. Changes to the standard were designed to update some controls, simplify others, and introduce some new ones to reflect the information security environment in 2022.

The list of information security controls in Annex A are now mirrored to ISO/IEC 27002:2022 to make it simpler for organisations to implement the two standards alongside each other.

THE IMPACT ON ORGANISATIONS

Even though all changes are noteworthy, they will not have much impact on the organisations that have already implemented ISO 27001. However, the new standard will require updates to the Statement of Applicability document, Internal Audit schedules. Additionally, the updates to clauses 4 through 10 will call for changes to ISMS documentation for most organisations.

ISO 27001:2022

5 Attributes
Control Types
Information Security Properties
Cyber Security Concepts
Operational Capabilities
Security Domain

4 Themes	93 Controls
Organisational	37
People	8
Physical	14
Technical	34

The New Controls

ISO 27001:2022	ISO 27001:2013 Equivalent Control
A.5.7 | Threat Intelligence	A.6.1.4 Contact with Special Interest Groups
A.5.16 | Identify Management	A.9.2.1 | User Registration and De-registration
A.5.23 | Information Security for Use of Cloud Services	A.15.x | Supplier Relationships
A.5.29 | Information Security During Disruption	A.17.1.x | Information Security Continuity
A.5.30 | ICT Readiness for Business Continuity	A.17.1.3 | Verify, Review and Evaluate Information Security Continuity
A.7.4 | Physical Security Monitoring	A.9.2.5 | Review of User Access Rights
A.8.9 | Configuration Management	A.14.2.5 | Secure System Engineering Principles
A.8.10 | Information Deletion	A.18.1.3 | Protection of Records
A.8.11 | Data Masking	A.14.3.1 | Protection of Test Data
A.8.12 | Data Leakage Prevention	A.12.6.1 | Management of Technical Vulnerabilities
A.8.16 | Monitoring Activities	A.12.4.x | Logging and Monitoring
A.8.23 | Web Filtering	A.13.1.2 | Security of Network Services
A.8.28 | Secure Coding	A.14.2.1 | Secure Development Policy

How Will the Transition Affect Organisations Implementing ISO 27001 for the First Time?

If your organisation is currently planning or have started implementation to get its ISMS certified for the first time in 2022 or early 2023, it's advisable to continue with ISO 27001:2013 standard. We recommend you take the below into account:

- Many certification bodies will not offer ISO 27001:2022 certification for at minimum six months after the 25 October 2022 publication date, as the 27001:2013 won't be retired for another three years.
- However, if you are just in your early planning stages, we advise you to consider starting with ISO 27001:2022. The new standard is more streamlined and easier to follow.

What Happens to Organisations that Are Already Certified to ISO 27001:2013?

Any current ISO 27001:2013 certificates are valid until they expire their 3-year lifetime. After it has expired, you will be assessed against ISO 27001:2022. For most, there is no rush to update documents and processes. We advise you to consider the following:

- If your organisation wants to become an early adopter ISO 27001:2022, it's easier to incorporate your security processes with the new way the controls are now organised by identifiable attributes.
- If you need to address Cloud Services risk, you may want to start transition early to allow for new control set to be implemented.
- Determine if upgrading to the new standard now makes sense to your organisation.

Tips to a Successful Transition

1. Updating Your Documents

The editorial changes to clauses 4 through 10 entails changes to the ISMS documentation. For example, the Statement of Applicability will need to reflect the changes to the Annex A controls. A **document review** should be conducted to make sure they reflect the changes.

2. Asset Register

It is always good practice to **reevaluate the asset register.** Sadly, it's often neglected and organisations will assume the same valuations and risk profiles for assets for years after they were first added to the register. This is a good opportunity to reassess those valuations and risk profiles while making sure the asset register is up to date.

3. Addressing Threats & Risk

The threat landscape is changing all the time as new threats emerge and existing threats recede. Changes to the Annex A controls reflect some of the new threats organisations now face. The **threats faced by a specific asset should be periodically revaluated** to make sure they are current and applicable.

4. Approaches to Considering the New Control Set

Organisations may find they have implemented most of the new controls already. For example, **control 8.12 Data Leakage Prevention will have been addressed** for a considerable period of time.

5. Reflect & Reset

This is a good time to conduct a maturity assessment as new controls will have not been included in previous internal and external audits. Even if the control reflects a practice the organisation has been doing for some time (e.g. data leakage prevention) the maturity level assessed years ago may not be accurate in the present day.

6. Considerations When Making the Transition to ISO 27001:2022

As we have alluded earlier in this document, transitioning to the new version will need a **comprehensive review of the existing ISMS** to identify where changes are required. Risk Assessments will need to be reassessed and internal audit schedules modified to include the 2022 control set.

7. Determine When You Are Transition Ready

The best way to gauge how ready your organisation is for a transition to the new version, is to **undertake a comprehensive audit of the existing ISMS**. This will identify what changes are required and allow you to estimate the effort needed to implement them.

It's Time to Run Faster

Now you're up-to-speed on the changes, what is required and best practices to follow. You can take the next step forward, at the right time, for your organisation to implement or update your ISMS to be audit ready – within the transition period.

Remember the changes were made to enable your organisation to defend against sophisticated security risks and ensure business continuity. Certifying to ISO 27001:2022 will help to ensure your information remains protected and give you an competitive edge. **Get more insight on ISO 27001 compliance on our website.**

How RISK CREW Can Help

When you choose Risk Crew, you're electing to work with qualified experts.

Risk Crew has two decades of hands-on skills and experience in successfully implementing cost-effective — security risk management compliance frameworks. All of our services come with our 100% satisfaction guarantee.

Best Practices

Risk Crew follows best practices including ISO 27001 and NIST

Accredited

Engineers carry CREST, C|EH and GIAC credentials

Certified

Engineers hold ISACA CISSP, CISM and CRISC certifications

Subject Matter Experts

Risk Crew engineers are SMEs with published articles in industry journals & magazines

CISA Certified Information Systems Auditor. An ISACA® Certification

CISM Certified Information Security Manager. An ISACA® Certification

CRISC Certified in Risk and Information Systems Control. An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification

LEAD AUDITOR ISO 27001

CISSP

Accelerate your ISO 27001 certification with the right crew, Risk Crew.

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234

riskcrew.com

info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom