bsi.

The new ISO/IEC 27001:2022 standard

bsi.

ISO/IEC 27001 Transition Guide

A leap forward in ISMS effectiveness

ISO/IEC 27001, Information Security Management and ISO/IEC 27002, Controls for Information Security standards have been updated to reflect the global digital evolution and new business practices becoming more cloud and digitally reliant. The new standards will require you to implement changes to ensure you not only remain compliant but align your infosec posture with the digitalization of business practices and the accompanying threats.

Step 1 - Understand the changes

Buy a copy of the ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards and train your team to help them understand and apply the changes as necessary. Our training and resources page can help support you on your learning journey.

Skills updated

By taking the new BSI Understanding and auditing the changes training course you and your team will be prepared to go through the transition journey.

Step 2 - Check the impact on your organization

Do a Gap Analysis against the changes in ISO/IEC 27001:2022 using your learnings from the BSI training and ISO/IEC 27002 to help you, and take a look at your risk assessment. Is it aligned with your organization's objectives and context? Ensure that it is.

See the benefits

Even this early in the process, you'll begin to see the benefits of the changes you've identified based on your understanding on how your current business practice and associated risks has evolved.

Step 3 - Implement the changes

Take a look at the evidence and justification for the inclusion or exclusion of necessary controls, and update your SoA accordingly. Be sure to implement the applicable changes based on your risk treatment plan and new controls, and validate the changes through an internal audit. Have they been implemented effectively? Make sure you have implemented the changes effectively. This step will help you reduce the likelihood of failing. Contact us for a **Readiness review**.

Update-ready

By this point, you're almost ready to update your ISO/IEC 27001 certificate.

Step 4 - Transition your certificate

Get in contact and schedule your transition audit with your BSI representative. To transition to ISO/IEC 27001:2022, your Auditor will confirm the implementation of any new necessary controls that you have chosen and their alignment with your ISMS. Get your audit report, take a look at your auditor's feedback and act based on the results.

Congratulations!

You've made it, get your updated ISO/IEC 27001:2022 certificate.

Ongoing conformance and improvement

Keep your process improvement cycle and embed information resilience within your organization.

bsi.

bsigroup.com/en-za | +27 12 004 0279 | bsi.za@bsigroup.com

bsi.

ISO/IEC 27001:2022 What's changed?

So, what can you expect from the new standard? This simple infographic will help you to understand the key changes.

ISO/IEC Changes summary

Editorial changes

- Full alignment with new ISO Harmonized Structure
- Re-arranging of some English to allow for easier translation
- Minor numbering re-structure to align with the harmonized approach
- Removal of reference to control objectives as they no longer exist either in Annex A or ISO 27002

New requirements

- Define the processes and interactions needed to implement and maintain your ISMS
- Communicate organizational roles relevant to information security within in your organization
- Monitor information security objectives
- Ensure your organization determines HOW to communicate as part of clause 7.4
- Establish criteria for operational processes and implementing control of the processes
- New clause 6.3 - Planning of Changes

Contact us to learn how we can help you complete the transition seamlessly and effectively.

bsigroup.com/en-za | +27 12 004 0279 | bsi.za@bsigroup.com

bsi.

Revised Annex A security controls

Number of controls reduced from 114 to 93

Four new security categories

Clause 5
Organizational controls

37 controls | 34 existing | 3 new

Clause 7
Physical controls

14 controls | 13 existing | 1 new

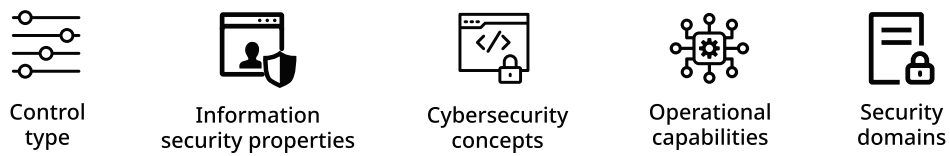
Clause 6
People controls

8 controls | All existing

Clause 8
Technological controls

34 controls | 27 existing | 7 new

Five new control attributes to aid categorization



ISO/IEC 27001:2022 Transition Timeline

1st November 2022 start of 3 years transition period to 31st October 2025

When to transition

- During a routine surveillance audit
- At your re-certification audit
- Special audit

Notes

- All audits require additional time to complete
- Additional time calculated on an individual basis, based on size and complexity of your scope.

bsi.

ISO/IEC 27001:2022 Information Security

It's more than information security, it's the camera cover for your company.

What is ISO ISO/IEC 27001?

ISO 27001 helps organizations manage and protect their information assets so that they remain safe and secure. Protecting personal records and commercially sensitive information is critical to your business. The standard can help you to continually review and refine practices, not only for today but also for the future. Certifying to ISO/IEC 27001 sends a clear signal to customers, suppliers, and the industry that your organization handles information confidentially and securely.

Why has the standard changed?

ISO/IEC 27001 has been updated to reflect the evolution of business practices such as remote working and increased dependencies on cloud services. With all the flexibility and efficiency these technologies offer comes increased risk, involving the whole business.

These updates provide more robust controls, enabling your organization to address increasingly sophisticated security risks, ensure business continuity, and gain a competitive advantage. Understanding these changes and their impact on your organization as soon as possible will ensure your information remains protected, and that you continue to maximize your competitive edge.

The key changes:

The changes will simplify how organizations map the controls for different stakeholders. This update was published in October 2022.

- Updated controls aligned with current business practices and associated threats
- New "attributes" to enable alignment with different risk management methodologies including global cybersecurity frameworks
- Simplified and streamlined grouping of controls
- Greater clarity on management requirements in line with ISO Harmonized Structure

bsigroup.com/en-za | +27 12 004 0279 | bsi.za@bsigroup.com

Strengthen your information security posture

By completing the transition and adopting the ISO/IEC 27001:2022 standard, you strengthen your organization's information security posture, support your digitization strategy, reduce the risks of information breaches, build trust in your brand, and build your organization's information resilience.

Making a smooth ISO 27001 transition

By completing the transition and adopting the ISO/IEC 27001:2022 standard, you strengthen your organization's information security posture, support your digitization strategy, reduce the risks of information breaches, build trust in your brand, and build your organization's information resilience.

Training benefits:

- Keep your Information Security knowledge up to date to ensure effectiveness and ongoing robustness
- Better inform your senior management team of the new standards requirements
- Strengthen your information security practices across the board – including minimizing the risk of costly information breaches
- Help your organization be future ready and more resilient to risks
- The new auditor training course is now live

bsigroup.com/en-za | +27 12 004 0279 | bsi.za@bsigroup.com