

# bsi.

## ISO/IEC 27001:2022 What's changed?

The new ISO/IEC 27001 standard was published in October 2022, which means that you need to update your ISMS and revise your infosec security posture.

This interactive tool will provide an overview of the changes to help you support your transition. For a more detailed understanding of the changes, please see our on-demand trainings.

Editorial changes 




New requirements 




### Four new security categories



 **Clause 5**  
Organizational controls



 **Clause 6**  
People controls



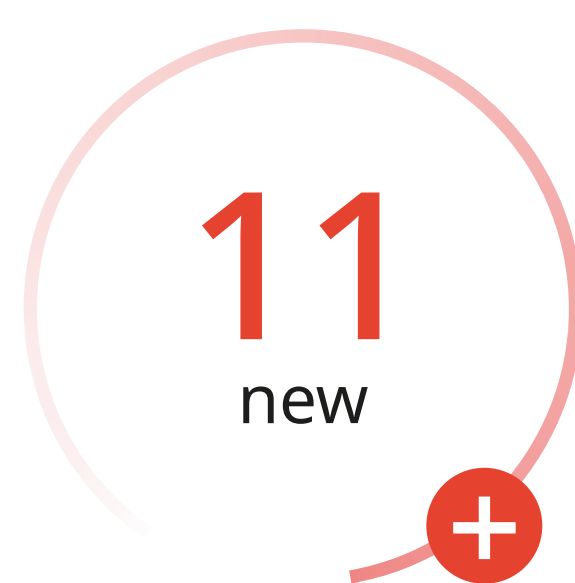
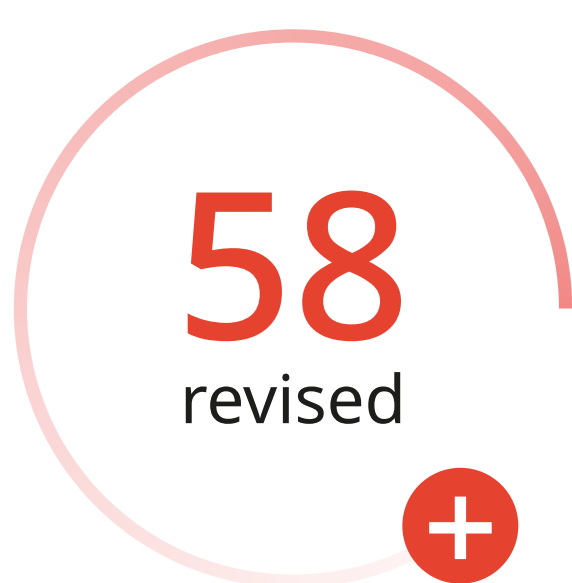
 **Clause 7**  
Physical controls



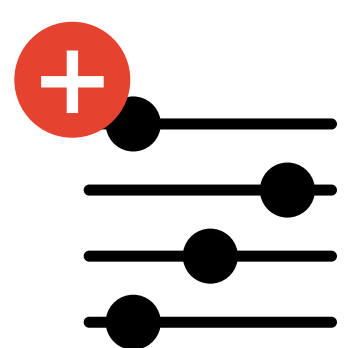
 **Clause 8**  
Technological controls

### Revised Annex A security controls

Number of controls reduced from 114 to 93



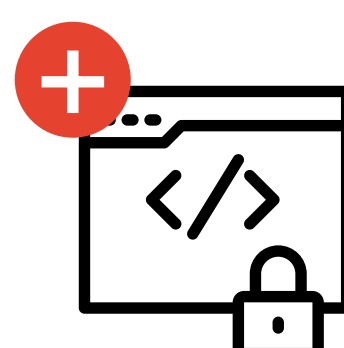
Five new control attributes to aid categorization and risk treatment



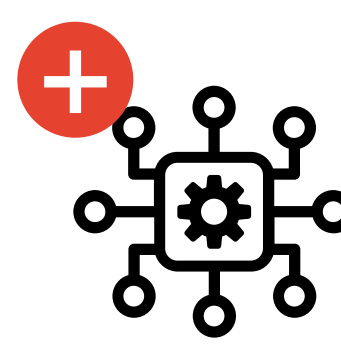
Control type



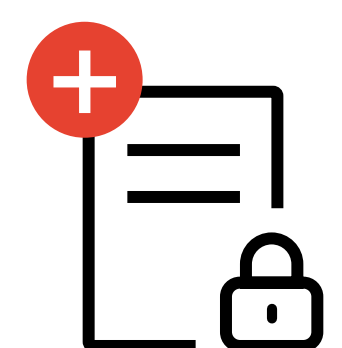
Information security properties



Cybersecurity concepts



Operational capabilities



Security domains

While the new standard allows for a three-year transition timeline, it is designed to address today's cyber and information security landscape. So, if you haven't started yet, it's time to take your first step now.

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





Go back to full view

Editorial changes and new requirements

Four new security categories

Revised Annex A security controls

Five new control attributes

## Editorial changes



- Full alignment with new ISO Harmonized Structure

A fundamental principle of ISO management system standards is that they can all work together. ISO/IEC 27001 has now been updated to ensure it can be implemented alongside other standards. This has meant adopting a far more process-driven approach that will bring clarity to stakeholders interacting with the management system, and enable a stream-lined and consistent approach across management system implementation.

- 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/IEC 27002
- New Clause 6.3 – Planning of Changes

## New requirements



- Define the processes and interactions needed to implement and maintain your ISMS
- Communicate organizational roles relevant to information security within 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 implement control of the processes in accordance with the criteria
- Ensure your organization controls all external products, processes and services relevant to InfoSec (not just third party processes)



# Four new security categories



## Clause 5 Organizational controls

These controls refer to broader organizational issues that do not fall into the other specific categories. That includes managing policies, or infosec in the supply chain, for example.

- 37 controls
- 34 existing
- 3 new

## Clause 6 People controls

These controls relate to individuals and cover issues ranging from training to terms and conditions of employment.

- 8 controls
- All existing

## Clause 7 Physical controls

These controls concern physical objects. That includes physical entry, secure disposal or reuse of equipment.

- 14 controls
- 13 existing
- 1 new

## Clause 8 Technological controls

These controls are in relation to technology. For example, secure authentication or configuration management.

- 34 controls
- 27 existing
- 7 new



# Revised Annex A security controls - Number of controls reduced from 114 to 93

## 24 merged

### Why have some controls been merged?

24 controls which were inseparable or closely related within the previous standard have now been merged. This has been facilitated by a more process-driven harmonized approach which is at the core of ISO/IEC 27001.

For example, where there were previously three separate controls referring to access and access control, there is now a single control requiring a completely defined process for developing, implementing and maintaining access control.

### Why is this important?

These mergers have resulted in some of the details within specific controls being removed as the detail is implied through the requirement to clearly define processes, interactions, and criteria for processes. That means it's essential that you have examined the main part of the standard, the context of your organization, its planning and operation first.

Only once you have determined your processes and interactions should you begin to address the newly merged control sets.

## 58 revised

### What kind of changes should I expect?

These 58 controls have been revised and updated to ensure they reflect the current business environment and relative threat. Remote work is now a major part of risk management, which means the relevant controls have been renamed and updated accordingly.

### What do I need to do?

While these revisions vary in severity, all have been reviewed and some have had extensive updates. It's essential that you check the updated guidance to ensure that you are fully embodying the revised controls, to address the new way your business is now working and the threats that it currently faces.

## 11 new

### Which new controls have been introduced?

In the last ten years, new areas of risk, such as cloud computing and privacy requirements, have resulted in new controls to address them. Other new controls formalize processes that have also grown more important, such as threat analysis and business continuity for both the IT department and the organization itself. The new controls are:

- Organizational controls
  - Threat analysis
  - Information security for use of cloud services
  - ICT readiness for business continuity
- Physical controls
  - Monitoring of physical security
- Technical controls
  - Configuration management
  - Information deletion
  - Data masking
  - Data leakage prevention
  - Monitoring activities
  - Web filtering
  - Secure coding

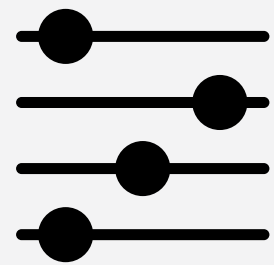
### What does best practice look like?

The latest edition of ISO/IEC 27002 has dedicated information regarding each new control, including best practice and how to ensure you remain compliant.



## Five new control attributes to aid categorization and risk treatment

### How does this control attribute help categorization and risk treatment?



#### Control type

The three basic types of controls are Preventative (stopping a vulnerability from occurring in the first place), Detective (alerting when a vulnerability occurs) and Corrective (remediating following a vulnerability). Understanding how your system is balancing these 3 aspects helps you understand your overall approach to risk management.



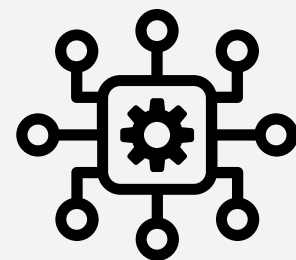
#### Information security properties

The three principles of information security are confidentiality, integrity and availability. Every control in the new standard is now tagged to demonstrate whether it supports one or more of these principles. This makes it significantly easier to assess your control implementation to ensure it covers the appropriate balance of confidentiality, integrity and availability for your business.



#### Cybersecurity concepts

This attribute enables you to categorize your controls according to whether they are contributing to a resilient security system beyond protection alone. That includes identifying existing and emerging threats, protecting your assets, detecting suspicious activity, responding to and recovering from a breach or attack.



#### Operational capabilities

There are a wide range of operational capabilities an organization can deploy to secure its information assets. By filtering your control implementation on these attributes it is possible to understand what capabilities are required in order to support your required mix of controls to address your organizational risk.



#### Security domains

Security domains can also be grouped into Governance and Ecosystem, Protection, Defence and Resilience. Filtering your control implementation based on these attributes allows you to ensure your implementation is suitably balanced against these domains as appropriate for your organizational risk.