This high level summary covers the implications to an existing ISMS of the changes within the October 2022 update to ISO27001:2022, and of the control changes made within ISO27002:2022.

Certification Implications

Organisations that are already certified to ISO 27001:2013 may transition to ISO27001:2022 at any time before October 31 2025.

Structural changes

The overall changes to the 27001:2022 standard from the last version are relatively small, and practically moderate in terms of intent and implementation objectives.

These changes must however be seen as a completion of the transitions started in the previous update and are now better adapted to a business view of current technologies and information risks.

The largest obvious change is in the structure of Annex A, with the grouping of controls into four categories:

1. Organisational Controls;
2. People Controls;
3. Physical Controls;
4. Technological Controls.

This allows a simpler alignment of information and cyber security actions across relevant business and risk management functions.

Control Changes

The number of controls has reduced from 114 to 94, but the renaming and merging of previous controls means that no controls were actually deleted, the addition of 11 completely new controls allows previous mappings to easily be maintained, and a focus on new controls be more readily achieved.

New Controls

5.7 Threat Intelligence	5.23 Information Security for use of cloud services
5.30 ICT Readiness for business continuity	7.4 Physical Security monitoring
8.9 Configuration Management	8.10 Information deletion
8.11 Data Masking	8.12 Data Leakage prevention
8.16 Monitoring activities	8.23 Web Filtering
8.28 Secure Coding	

Control Terminology

Terminology changes used in control naming reflect contemporary business perspectives on identity, privacy, monitoring, and the risk exposure of evolving business models, cyber resilience, and governance.

The most significant change to these controls within ISO27002:2022 though is their transition into a generic set of information security controls, from the code of practice style of previous versions. The most practical aspect of this being the addition of standardized control attributes for every control. This greatly improves the ability to reference and monitor control effectiveness against technical and business risk within and across all four control domains.

Recommended Transition approach

1. Review the scope of the current ISO27001 based ISMS, adjust the statement of applicability as required.
2. Re-assess the current business risk environment in context with the new controls; Select, confirm, and adjust required controls and their metrics as appropriate
3. Perform a gap assessment to address any business process and risk implications due to the new controls, and address simplifications to existing/updated controls
4. Update the risk treatment process to accommodate detail provided with new controls
5. Review and update the content of any existing policy and guidelines to refer to updated references.