WHAT WE KNOW SO FAR

ISO/IEC 27002: 2022

ADVENT IM

THE NEW UPDATE

The new update breaks down **ISO 27002** into 4 Clauses, which has been significantly reduced from 14 in the 2013 edition and with there now being 93 controls which has been reduced from 114 controls, but with the addition of 11 new controls. The Clauses have broken down into the following:

▶ Organization (Clause 5) –37 Controls

▶ People (Clause 6) – 8 Controls

▶ Physical (Clause 7) – 14 Controls

▶ Technological (Clause 8) 34 Controls

UPDATE

OPPORTUNITY FOR ISO 27001 TO BETTER ALIGN TO RISK MANAGEMENT

There are controls, that have not been removed but have been updated and renamed to the current environment we operate in.

2013

56 Controls

Although it may feel like that some controls have been deleted; it has been done to remove the repetition that exists throughout the 2013 edition.

2022

24 Controls

ATTRIBUTES

In the 3rd edition, we will see the introduction of attributes. Different attributes will fall under **5 categories...**

Control Type — Preventative; Detective; Corrective;

Information Security Properties — Confidentiality; Integrity; Availability

Cybersecurity Concepts — Identify; Protect; Detect; Respond; Recover

Security Domains — Governance and Ecosystem, Protection, Defence and Resilience

Operational Capabilities — Governance; Asset Management; Information Protection; Human Resource Security; Physical Security; System and Network Security; Application Security; Secure Configuration; Identity and Access Management; Threat and Vulnerability Management; Continuity Supplier Relationships Security; Legal and Compliance; Information Security Event Management; Information Security Assurance;

Attributes are not mandatory and organisations can define their own attributes which will be relevant to their own organisation.

Organisations can use attributes to filter, sort or present controls in a different view for different audiences and also for different purposes

OTHER CHANGES

For those who will be auditing organisations against this standard, BSI will be producing an advisory document that will assist auditors when working with the updated standard. Updated standard was due 13th January 2022, but there is uncertainty it may not be published in 2022. So for now we continue with its current iteration until told otherwise.

Up to date terms and definitions, introducing subheadings in some controls guidance text when it is long and can be structured and there are 2 informative annexes, Annex A, that looks at using attributes and Annex B, which is correspondence with ISO 27002:2013.

What we will be seeing with the new edition is an ISO 27002 that will be modernised, simplified and versatile

Modern – 11 new controls; Up to date guidance on existing controls;

Simplified – A lower number of controls (21 less controls than the 2nd edition);

Versatile – Introduction of attributes to help organisations and industry bodies apply the standard in their own context.