MAIN CHANGES

IN ISO 27001:2022

- Main part of ISO 27001, i.e., clauses 4 to 10, are not changing, just slight amendments
- The security controls listed in ISO 27001 Annex A have been updated
- Number of controls has decreased from 114 to 93
- Controls are placed in 4 sections instead of previous 14 (Annexes 5-18)
- There are 11 new controls, while none of the controls were deleted, and many controls were merged

11 NEW CONTROLS INTRODUCED IN THE ISO 27001 2022 INFORMATION SECURITY CONTROLS:

•A.5.7 - Threat intelligence

Threat intelligence is the process of gathering, analysing and considering information about current and future cyberattacks, providing organisations with a deeper understanding of threats.

•A.5.23 - Information security for use of cloud services

Organisations should scrutinise cloud service agreements and ensure that four main operational requirements are met: Confidentiality, Security/data integrity, Service availability and Information handling

•A.5.30 - ICT readiness for business continuity

Recovery time objective (RTO) and the overall Business impact analysis (BIA). The overall goal is to ensure that information integrity and availability is maintained before, during and after a period of business disruption.

•A.7.4 - Physical security monitoring

A control that requires organisations to detect and prevent external and internal intruders who enter into restricted physical areas without permission by putting in place suitable surveillance tools to protect the following: - Theft of sensitive data, Loss of information assets, Financial damage, Theft of removable media assets for malicious use, Infection of IT assets with a malware, Ransomware attacks that may be conducted by an intruder.

•A.8.9 - Configuration management

Configuration management is a key part of an organisation's wider asset management operation. Configurations are key in ensuring that a network is not only operating as it should be, but also in securing devices against unauthorised changes or incorrect amendments on the part of maintenance staff and/or suppliers/vendors.

•A.8.10 - Information deletion

As a general rule, Control 8.10 asks organisations to delete data when it is no longer needed, in order to minimise what is referred to as undesirable disclosure – i.e. data being viewed by, or passed on to, individuals and organisations that are not authorised to access it.

•A.8.11 - Data masking

Data masking or data obfuscation is the process of modifying sensitive data in such a way that it is of no or little value to unauthorized intruders while still being usable by software or authorized personnel. Data masking can also be referred to as anonymization, or tokenization, depending on different context.

•**A.8.12 Data leakage prevention**

Organisation's need to: -

- Classify data in line with recognised industry standards (PII, commercial data, product information), in order to assign varying risk levels across the board.
- Closely monitor known data channels that are heavily utilised and prone to leakage (e.g. emails, internal and external file transfers, USB devices).
- Initiative-taking measures to prevent data from being leaked, through sticked file permissions and adequate authorisation techniques.
- Restrict a user's ability to copy and paste data (where applicable) to and from specific platforms and systems.
- Require authorisation from the data owner prior to any mass exports being carried out.
- Consider managing or preventing users from taking screenshots or photographing monitors that display protected data types.
- Encrypt backups that contain sensitive information.
- Formulate gateway security measures and leakage prevention measures that safeguard against external factors such as (but not limited to) industrial espionage, sabotage, commercial interference, and/or IP theft.

•A.8.16 - Monitoring activities

It is immensely important for organisations to promote a proactive approach to monitoring and ensure that it aims to prevent incidents before they happen, and works in conjunction with reactive efforts to form an end-to-end information security and incident resolution strategy that ticks every box

•A.8.23 - Web filtering

This control is a preventive type of control that requires organisations to put in place appropriate access controls and measures to prevent access to malicious content on external websites.

•A.8.28 - Secure coding

Requires organisations to establish and implement organisation-wide processes/procedures that cover secure coding that applies to both software products obtained from external parties and to open-source software components. It must also keep up to date with ever changing real-world security threats and with the most up-to-date information on known or potential software security vulnerabilities. This will help organisations to improve and implement robust secure software coding principles that are effective against evolving cyber threats.

The 27001-2013 version has 14 sections that detailed the 114 controls and these have been changed in the 27001-2022 standards to the 4 sections below.

NEW ISO 27002 HAS 93 CONTROLS IN THE FOLLOWING 4 SECTIONS

- **Organizational controls (clause 5)**
- **People controls (clause 6)**
- **Physical controls (clause 7)**
- **Technological controls (clause 8)**