Aptivaa

ISO 27001: 2022

What has changed?

What is ISO 27001?

- ISO 27001 provides the requirements to establish, implement, maintain, and continue improvement of an information security management system, which is referred to as an "ISMS."
- To implement an ISMS, following should be considered:
  - Goals and objectives,
  - Security requirements,
  - The organizational processes used, and
  - The size and structure of your organization—all of which will change over time.
- ISMS is integrated with business processes and the management structure—because the ISO 27001 standard requires to continuously improve your ISMS. Information security becomes a main factor in the further design of processes, information systems, and controls.
- Establishing and maintaining an ISMS can help you securing the confidentiality, integrity, and availability of information, through its required risk management process.
- Certifying ISMS against the ISO 27001 standard can reassure your interested parties about the risk management capabilities.

The New ISO/IEC 27001:2022:

ISO 27001:2022 was published in late October 2022. There will be a transition period of 3 years, commencing from 1st November 2022 to 31st October 2025. The new standard provides a flexible controls structure which aligns to various modern day cyber threats.

A New Name:

- As the world is facing new evolving security challenges, the internationally recognized standard ISO 27001, which protects the confidentiality, availability, and integrity of organizations' information assets has been updated and its relevant, and up-to-date.
- The standard has got a new title – "Information security, cybersecurity and privacy protection"

Timeline:

- Organizations that are currently certified to ISO/IEC 27001:2013 will have three years to transition to ISO/IEC 27001:2022. The transition must be completed by October 2025.
- Organizations can continue to be certified to the 2013 version of the standard, which is possible until 31st October 2023.

Updated Control Set for ISO/IEC 27001:2022:

- Minor changes to Clause 6 of the ISMS framework introduced as well. These are mostly wording changes.
- New requirement introduced to ensure the organization determines, "how to communicate" as part of clause 7.4.
- The structure has been consolidated into 4 key areas: Organizational, People, Physical and Technological instead of 14 in the previous edition.
- The new set consolidates the controls (previously referred to as "Annex A") from 14 control domains in A.5-A.18 to four control categories (or themes).
- Controls listed have decreased from 114 to 93.
  - A.5 Organizational controls - contains 37 controls
  - A.6 People controls - contains 8 controls
  - A.7 Physical controls - contains 14 controls
  - A.8 Technological controls - contains 34 controls
- ISO/IEC 27001:2022 has added the below-mentioned 11 new controls to its Annex A:
  - Threat intelligence
  - Information security for the use of cloud services
  - ICT readiness for business continuity
  - Physical security monitoring
  - Configuration management
  - Information deletion
  - Data masking
  - Data leakage prevention
  - Monitoring activities
  - Web filtering
  - Secure coding

Importance and Impact

- With the ever-evolving technology adoption and security landscape, the global security standards and baseline requirements should be adaptable and cover the new age threats and controls.
- The new ISO 27001 standard which has the global reach, has updated it to make it simple, versatile and aligned it to the modern technology environment.
- The domains and controls have been modernized, easy to use and understand, for all the sets of employees.
- The key impact will be, the need to revisit the risk assessment and statement of applicability, to ensure the revised set of controls are applied appropriately and effectively, bringing the ISMS in line with your digital business risk.
- Taking into consideration these changes, we believe that, if your ISMS has been staying up to date with technology and regulatory trends, it will be well-positioned to absorb this update.

Next Steps for ISO/IEC 27001:2022

- This is the first major change for the ISO 27001:2013 standard in nearly ten years.
- The standard's prominence has only grown during the time since then, and with this shift, organizations will be looking to discern how they need to proceed in order to maintain or obtain the certification.
- The organizations shall conduct a gap assessment against the new requirements and design an implementation roadmap for transitioning to new certification.

Building blocks for ISO27001

- Scope and Objective: The first step in ISMS is to understand the scope of what you want to protect and why. The ISMS objectives shall align to the business objectives and technology landscape.
- Risk Management: The scoping of ISMS helps the organization to define the various risk scenarios. Design and implement a proven risk management framework to identify the threats and vulnerabilities and overall risk posture.
- Policies: Policies are complementary to risk management. It captures industry best practices and drives security culture in the organization.
- KPI's, Metrics & Management reporting: The KRI designed will help the organization to implement and periodically monitor the overall risk posture.
- ISO 27001 Internal audit: Before going for ISO/IEC 27001 certification, organization will need to conduct an internal audit on the effectiveness of the ISMS and the relevant controls.
- ISO 27001 Certification: ISO/IEC 27001 is the internationally recognized standard for information security management. It specifies requirements for establishing, maintaining, and improving an Information Security Management System (ISMS). The certification is conducted by independent body and the certificate is issued for a period of 3 years with sustenance audit conducted every year.

Aptivaa

LEADING THROUGH INNOVATION

To explore about how can we assist with your risk management initiatives, please e-mail us at info@aptivaa.com

: www.aptivaa.com

: www.linkedin.com/company/aptivaa

: https://www.youtube.com/c/AptivaaTV

Our Locations

UAE | USA | INDIA