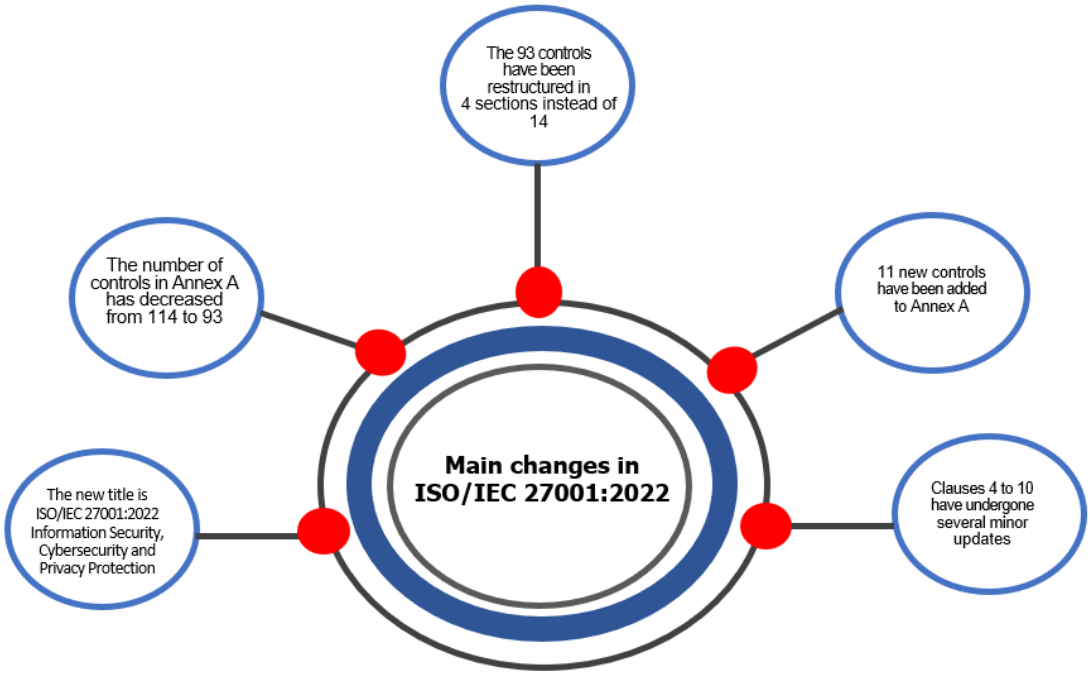
Transition Requirements & Policy on ISO/IEC 27001:2022

A. Overview of the Changes in the New Standard - ISO/IEC 27001:2022:-

The new ISO/IEC 27001:2022 has been published on October 25, 2022. The title of the standard has been changed to Information security, cybersecurity and privacy protection - Information security management systems.



The changes in the standard can be classified in to two areas as below:-

1. **Changes in the standard clauses 4 to 10 (regarded as minor changes):-**
   i. In clause 4.2 (Understanding the needs and expectations of interested parties), item (c) was added requiring to determine which of the interested party requirements must be addressed through the ISMS.
   ii. In clause 4.4 (Information security management system), now must include the planning for processes needed and their interactions as part of the ISMS.
   iii. In clause 5.3 (Organizational roles, responsibilities and authorities), a phrase was added that communication to be done internally within the organization.
   iv. In clause 6.2 (Information security objectives and planning to achieve them), item (d) was added that requires objectives to be monitored. Item (g) required the IS objectives and plans to be available as documented information.
   v. Clause 6.3 (Planning of changes) new clause was added, requiring that any change in the ISMS needs to be done in a planned manner.
   vi. In clause 7.4 (Communication), items (d and e) were deleted, there is new para (d) now regarding how to communicate.
   vii. In clause 8.1 (Operational planning and control), last para which stated "the organization shall ensure that outsourced processes are determined and controlled."

Has been replaced with "the organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled."

The requirement to plan how to achieve information security objectives has been deleted, it has been replaced by clause 6.2 (g) as above.

viii. In clause 9.1 (Monitoring, measurement, analysis and evaluation), the note which was under the in Para (c) has now been added in the requirement which says "The methods selected should produce comparable and reproducible results to be considered valid".

ix. In clause 9.3 (Management review), the new item 9.3.2 (c) is added in the management review inputs - related to the changes in needs and expectations of interested parties that are relevant to the ISMS.

x. In clause 10 (Improvement), the subclauses 10.1 and 10.2 have changed places. Now Continual improvement is 10.1), Nonconformity and corrective action is (10.2), while the text of those clauses has not changed.

2. Changes in the Annex A (regarded as major changes)

Annex A of ISO/IEC 27001:2022 has the most significant changes. Annex A has been completely restructured and revised. As a result, the number of controls has decreased from 114 to 93. Also, these security controls are now divided into four sections instead of the previous 14.

The new Sections and Controls of ISO/IEC 27001:2022 are:
5 Organisational (has 37 controls)
6 People (has 8 controls)
7 Physical (has 14 controls)
8 Technological (has 34 controls)

While most of the controls have been merger and renamed blow controls have been added and were not part of the previous version:-
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

B. Transition Timelines and Process: -

RICI is announcing below policy in order to ensure the timely transition of all client.

1. **Timeline for clients which are already certified on ISO/IEC 27001:2013.**
   i. RICI strongly recommended all ISO/IEC 27001:2013 certified clients to complete their transition process prior to their due surveillance or re-audit. The deadline for conducting transition audits along with a due surveillance or re-audit is 31st of October 2024.
   ii. All transition audits will require extra man-days to verify the additional transition requirements (a typical Surveillance + Transition audit would need 1 extra man-day and a re-audit + Transition audit would need .5 extra man-day).
   iii. The clients for which transition process is not completed by 31st of October 2024 would need to undergo a special transition audit. All such audits would be of 1 man-day duration. These special transition audits must be completed before 30th of August 2025.
   iv. Certificates of any remaining clients who have not been able to complete the transition as per above timelines shall be withdrawn on 1st of November 2025.
   v. All transition audits will be onsite audits.

2. **Transition Process:**
   i. Certified clients may do a gap analysis and identify the gaps in the current system versus the changed requirements of ISO/IEC 27001:2022.
   ii. Once their documentation is updated and changes are implemented, the clients are required to do an internal assessment of the changes in the system.
   iii. Once ready the clients may communicate to the RICI's operations teams to plan their transition audits.
   iv. The operations teams of RICI will confirm with the client before planning the transition audit that the new system is implemented. The audit plans for such audits will reflect the transition objectives also.
   v. The preferred approach should be to get the transition done along with due surveillance or re-audit as explained in para 1 above.
   vi. All transition audits by RICI will focus on verifying the changes in the documentation as well as the implementation of these changes. Some of the key areas to be verified will include:-
      - Verification of the transition planning and it's execution.
      - Verification of the requirements related to training and competence of the resources on the new version.
      - Verification of the updated SoA.

- Verification of the changes in any procedures or controls and their implementation.
- Verification of any changes in the risk assessments or risk treatment plans
- Verifying how the organization checked the effectiveness of the new system using internal audits, management review and other monitoring processes.

vii. A revised certificate will be issued once the audit findings are closed and a technical review has been done. The expiry of the certificate will be as per the original certification cycle (in-case audit was standalone special transition audit, the certificate will have same expiry as of last issued certificate).

3. Timeline for new initial audits on ISO/IEC 27001:2013.

i. Any initial audits on ISO/IEC 27001:2013 version must be completed by 30th of April 2024.

ii. All initial audits after 1st of May 2024 must be conducted on the ISO/IEC 27001:2022 Version only.