TRANSITION APPROACH :
ISO 27001:2013 ISO 27001:2022

GENERAL

- As a part of continuous review and improvement process, ISO standards are being revised and updated periodically.

- Information technology — Security techniques — Requirements ISO 27001:2013 - has been revised to ISO 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems — Requirements

- Final version of ISO 27001:2022 was published 25th Oct'2022.

- Three year transition period from the publication date of ISO 27001:2022

TRANSITION APPROACH

- Certifications to ISO 27001:2013 shall be valid only up to 36 months from publication of ISO 27001:2022. No existing active ISO 27001:2013 certificates shall have a validity beyond 25th Oct'2025.

- All existing certified clients shall update their respective Management system to meet requirements of ISO 27001:2022 as applicable and shall obtain certificate during their next surveillance audit or recertification audit or through exclusive upgrade audit.

- Certification migration can happen during a routine surveillance, recertification audit or a special / upgrade audit.

- Transition Audits duration estimation shall be done as follows –
  - During routine surveillance :
    - Single site : 20% of SA mandays or 1 manday, whichever is higher
    - Multi-site : Min 1 manday for Central Location & min. 0.25 mandays for sampled site (Sample size = 0.6 x SqRt(no. of sites)
  - During Recertification – Additional 10% of RC mandays or 0.5 manday, whichever is higher
    - Single site : 10% of RC mandays or 0.5 manday, whichever is higher
    - Multi-site : Min 0.5 manday for Central Location & min. 0.25 mandays for sampled site (Sample size = 0.8 x SqRt(no. of sites)
  - Special Audit for Transition :
    - Single site : 20% of SA mandays or 1 manday, whichever is higher
    - Multi-site : Min 1 manday for Central Location & min. 0.25 mandays for sampled site (Sample size = 0.6 x SqRt(no. of sites)

Note - Recognizing that each client and transition audit is unique, the audit duration may be increased above the minimum as needed to sufficiently demonstrate conformity to ISO 27001:2022.

TRANSITION APPROACH

- TUV India to accept contracts (new/re-cert/transfer) for ISO 27001:2013 till 25th April'2024.

- For the above, TUV India to perform audits for ISO 27001:2013 till 31st July'2024 (in case any contract is signed, as per earlier versions, but yet to be executed till 31st July'2024, the same shall be amended as per the 2022 version requirements).

- For existing contracts (within the surveillance cycles), all audits after 31st July'2024 will be done as per ISO 27001:2022.

- No certification decisions will be taken for ISO 27001:2013 versions beyond 24th October'2024.

- During the transition period (up to 25th Oct'2025), if client wants to undertake transition audits for the 2022 version – Determine the man-days as per the TUV India transition policy & respective accreditation rules - Issue certificate as per 2022 version subject to fulfillment of all requirements for 2022 version

TRANSITION APPROACH

- In case the client completes the transition during surveillance the certificate validity shall be as per the existing period of the cycle. In case transition is done with recertification man-days, the cycle can be re-set.

- For contracts signed for 2022 version – non-compliance to new requirements as per 2022 version will be raised as NCRs & certification to 2022 version will be recommended after satisfactory closure of NCRs.

- In the eventuality of previous certification continuity at stake, the client may choose to remain certified for earlier ISO 27001:2013 version. In this case, the contract to be amended & findings related to previous version be closed. In this case findings related to ISO 27001:2022 version will be regraded as observations till 24th October'2024 or the next immediate surveillance (incl. any additional audit resulting in re-issuance of certificate), whichever is later, but not later than 30th June'2025.

- Subsequent to the above deadline getting over, all such observations would be converted to NCRs. All such cases would require prior approval from Technical HO team. In the eventuality of above point being true, the client will have to undertake the transition audit during the balance period for transition (such that the certification decision date is before 25th Oct'2025). The transition man-days as per TUV India guidelines will be followed / repeated.

TRANSITION APPROACH

- In case the organization is unable to complete the transition process (including certification / re-certification decision) prior to 25th Oct'2025, then

  - If audit is already completed & certification decision is done beyond 25th Oct 2025 – there will be break in continuity.

  - If audit is not performed till 25th Oct'2025 – Fresh Stage 1 & Stage 2 would be done with a new certification cycle.

- Clients may opt for a readiness review to verify readiness for the 2022 versions prior to the transition audit.

- Any ISO 27001:2013 version certificates, if not transitioned by 25th Oct'2025, shall be rendered invalid.

- ISO 27001:2022 Certificates can be issued after successful Transition of Accreditation.

ADDITIONAL INFORMATION FOR ORGANIZATIONS ALREADY CERTIFIED TO ISO 27001:2013

- Identify organizational gaps which need to be addressed to meet new requirements.
- Develop an implementation plan.
- Provide appropriate training and awareness for all parties that have an impact on the effectiveness of the organization.
- Update the existing Information Security management system (ISMS) to meet the revised requirements and provide verification of effectiveness.
- Where applicable, liaise with nearest TUV India Office for transition arrangements.
- Perform at least one internal audit and one management review to assess adequacy & preparedness for the external (transition) audit.
- Certification migration can happen during a routine surveillance, recertification audit or a special audit
- Transition Audits duration estimation shall be done as follows –
  - During routine surveillance :
    - Single site : 20% of SA mandays or 1 manday, whichever is higher
    - Multi-site : Min 1 manday for Central Location & min. 0.25 mandays for sampled site (Sample size = 0.6 x SqRt(no. of sites)
  - During Recertification – Additional 10% of RC mandays or 0.5 manday, whichever is higher
    - Single site : 10% of RC mandays or 0.5 manday, whichever is higher
    - Multi-site : Min 0.5 manday for Central Location & min. 0.25 mandays for sampled site (Sample size = 0.8 x SqRt(no. of sites)
  - Special Audit for Transition :
    - Single site : 20% of SA mandays or 1 manday, whichever is higher
    - Multi-site : Min 1 manday for Central Location & min. 0.25 mandays for sampled site (Sample size = 0.6 x SqRt(no. of sites)

  Note - Recognizing that each client and transition audit is unique, the audit duration may be increased above the minimum as needed to sufficiently demonstrate conformity to ISO 27001:2022.
- ISO27001:2022 Certificates can be issued after successful Transition of Accreditation.

TUV SUPPORT FOR TRANSITION

- 1 Day Awareness Training (Open House)
- 2 Days NBQP Internal Auditor Course
- 5 days CQI-IRCA Lead Auditor Course

QUALIFICATION OF INTERNAL RESOURCES

- Training of Auditors and Veto-Person
- Training of other persons involved in certification process (e.g. administrative staff, ATEA Team).
- Training on ISO 27001:2022 done by different techniques or a combination of it (e.g webinar, e-learning, Exchange of Experience)
- Content of the Training:
  - Understanding the changes in Requirements
  - Understanding the changes in the Controls, Themes and Attributes (ISO 27002:2022)
  - Understanding the New Controls (ISO 27002:2022)

VERIFICATION OF TRAINING

- Learning objective directly after the training (e.g.: effectiveness control, technical discussion) – through On-line test
- Short-term: competence assessment after the audit by document check / review
- Medium-term: exchanges of experience and other events
- Long-term: Monitoring and customer feedback
- Recognition other Qualifications - Equivalent qualification measures and parts of any previous training courses (e.g. for the ISO 27001:2022 Transition course by other CBs)
- Qualification, Evidence and the verification of competence must be documented.