ISTO Test of Understanding, Level 2 - Professional
ISO/IEC 27001:2022
Test Description

1. What is an ISTO Test of Understanding?

1.1. General

ISTO Tests of Understanding have been developed specifically for ISO management system standard (MSS) professionals. This includes middle and senior management personnel, responsible persons*, internal auditors, third party certification body auditors, advisors and consultants.

Each Test of Understanding has three (3) outputs:

Certification

- a certificate of achievement for candidates who pass the test which recognizes the candidate's understanding of the respective standard at one (1) of three (3) levels (Practitioner, Professional, Expert)

Analytics

- an analytics report which measures the level of understanding in the eight (8) A C C U R A T E domains

Ranking

- a star diagram which provides a visual indication as to the candidate's strengths and development opportunities, as measured against the candidate population.

Key Features

- No prerequisites
- Multiple choice test
- Detailed syllabus
- Test preparation support
- Robust test development process by international experts
- Insightful data analytics on the eight (8) A C C U R A T E domains

Employers of ISO management system standard (MSS) auditors/consultants/tutors would find the ISTO Test of Understanding certification a good benchmark in their selection process, as the ISTO Test adds value to the organisations' performance excellence and consistency. A course tutor with an ISTO Test of Understanding credential is able to offer learners a more accurate and comprehensive presentation of the standard.

* as defined under clause 5.3

Key Benefits

For Certification Bodies	For Employers	For Individuals
• Verify auditors possess a sound understanding of all areas of the Standard • Use ISTO certification to evidence accreditation requirements are met • Target training at those specific areas where an auditor's competence needs to be developed.	• Upskill your employees • Ensure the competence of your auditors and staff • Demonstrate the result of training • Facilitate recruitment • Strengthen process control • Reduce non-value-adding processes and documented information	• Propel your career • Receive a globally recognized qualification • Stand out among your peers • Identify knowledge gaps using our exclusive, industry-leading analytics report • Rank yourself against the candidate population

ISTO Tests focus not only on understanding the requirements of a standard but are also designed to ensure that those who pass the test have demonstrated a knowledge of the underlying management system principles, definitions, applicability, commonly held misconceptions and the Standard's practical implementation.

1.2. Structure of the Test of Understanding - Level 2 – Professional

All ISTO Tests are closed-book and online. They consist of multiple choice questions with four (4) possible options, of which only one (1) represents the 'best' response. Candidates are allowed to refer to an unmarked copy of the respective ISO standard which is the only permitted reference material during the test.

Time allowed: 180 min. **No of questions:** 120 **Pass criteria:** 70%

Section	No. of questions	Focused areas
1	30	Principles and definitions, applicability, clause 4.3
2	30	Management system requirements based on clauses 4, 5, 6, 9 and 10 (except clause 4.3)
3	30	Operational requirements based on clauses 7 and 8 and the Appendix A information security controls
4	30	Six (6) scenarios with five (5) questions each focusing on the practical aspects of the requirements of the standard

Candidates who meet or exceed the Pass criteria at 70% will be awarded a Certificate of Achievement. All candidates will receive the **A C C U R A T E** analytics report indicating their level of understanding and relative ranking in each of the eight (8) domains in the star diagram.

1.3. A C C U R A T E Analytics

Based on ISTO's research, endorsed by the ISTO Technical Advisory Board, the level of comprehension of an ISO management system standard can be grouped into 8 domains of understanding. These form the acronym **A C C U R A T E**.

Ac: an Actual requirement in the standard related to documented information.

Co: Concept - the management principles on which the management system standard is based. This includes the sequence of activities as required in the standard.

C: the unique Clause reference of a specific requirement in the ISO management system standard

U: an Unspecified requirement in the standard (a requirement that does not exist).

R: a certain Requirement in the standard (i.e. the text of the requirement).

A: the Applicability of the standard. This includes the intent of a requirement, and the scope of the standard.

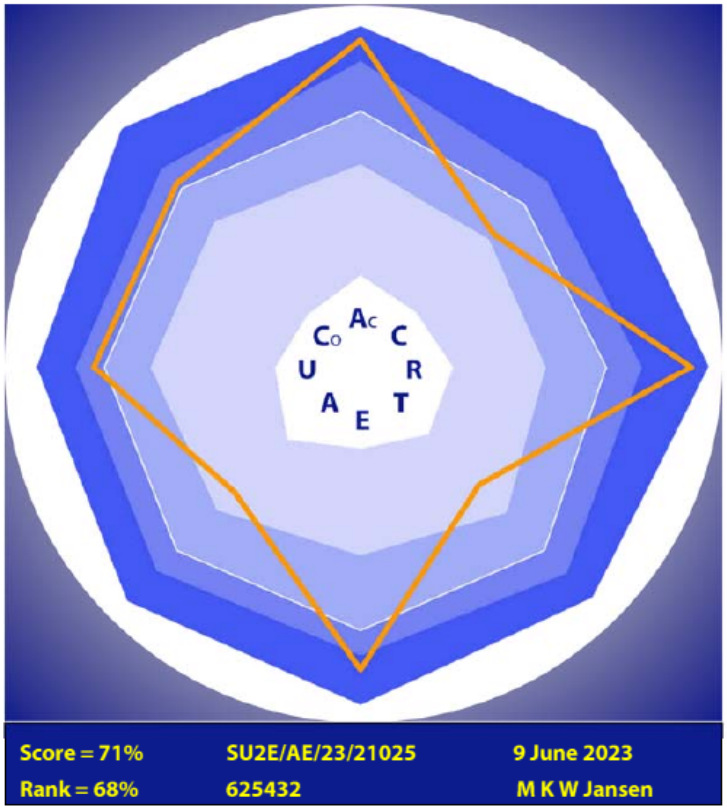
T: Terms and definitions used in the standard. Generally these are defined in Clause 3 of each ISO management system standard. In the case of ISO 9001 QMS, terms and definitions are defined in the ISO 9000 standard.

E: an Erroneous requirement in the standard related to documented information.

A sample A C C U R A T E Analytics (Star Diagram)

ACCURATE Analytics

Domains (of Understanding)	Score, %
Ac (Actual documentation)	92%
Co (Concept and principles)	73%
C (Clause reference)	53%
U (Unspecified requirements)	75%
R (Requirements)	93%
A (Applicability)	50%
T (Terminologies)	47%
E (Erroneous doc. requirements)	85%
Total =	**71%**



Sample questions (A C C U R A T E)

1. ISO/IEC 27001:2022 requires which of the following documented information be retained?

   A. definition of the process environment
   B. infrastructure maintenance records
   C. management review
   D. all of the above

   *(Question related to and actual requirement in documented information, **Ac**)*

2. Which of the following is <u>not</u> one of the CIA triad?

   A. confidentiality
   B. independence
   C. availability
   D. none of the above (all of them are part of the CIA triad)

   *(Question related to concept & principles, **Co**)*

3. The requirement to ensure that internal auditors are competent is given in:

   A. clause 9.2.1
   B. clause 9.2.2
   C. clause 7.2.b
   D. none of the above

   *(Question related to clauses, **C**)*

4. Which of the following is <u>not</u> an ISO/IEC 27001:2022 requirement?
   A. conduct internal audit once per year
   B. assign responsibilities within the ISMS
   C. ensure internal auditors are competent
   D. none of the above (all of the above are ISO/IEC 27001 requirements)

   *(Question related to an **u**nspecified requirement in the standard, **U**)*

5. ISO/IEC 27001:2022 requires that the information security policy be:

   A. maintained
   B. recited by everybody within the organization;
   C. communicated to competitors
   D. all of the above

   *(Question related to requirement, **R**)*

6. The employment of third party cloud service can be excluded from the ISMS if:
   A. the ISMS scope is documented
   B. the exclusion is approved by the top management
   C. the service provider is the No. 1 cloud service provider globally
   D. none of the above

   *(Question related to applicability, **Ap**)*

7. Which of the following is a potential corrective action?

   A. providing training to an incompetent worker
   B. revising a physical security policy
   C. fixing a software bug
   D. none of the above

   *(Question related to terminologies, **T**)*

8. ISO/IEC 27001:2022 requires which of the following documented information be maintained?

   A. internal audit procedure
   B. people awareness
   C. approved supplier list
   D. none of the above

   *(Question related to an erroneous requirement related to documented information, **E**)*

The suggested answers are Q1=C, Q2=B, Q3=C, Q4=A, Q5=A, Q6=D, Q7=B, Q8=D

*

A D D I T I O N A L I N F O R M A T I O N

www.isto.ch	*ISTO background; Test programme; Test centres*
portal.isto.ch	*Create candidate account; Experience Free Trial Test*
J62	*Test syllabus and reference sources (downloadable from www.isto.ch)*