ISTO Test of Understanding, Level 2 – Professional
ISO/IEC 27001:2022/Amd 1:2024
Test Description

What is an ISTO Test of Understanding?

I. General

ISTO Tests of Understanding are developed specifically for ISO management system standards (**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:

(1) Certification

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

(2) Analytics

- an analytics report which measures the candidate's level of understanding in the eight (8) A C C U R A T E domains.

(3) Ranking**

- an overall percentile rank, together with a star diagram which provides a visual indication as to the candidate's strengths and development opportunities, as measured against the test population.

Key Features

- Multiple choice test with no prerequisites
- Detailed syllabus with reference materials
- Robust test development process by international experts
- Insightful data analytics on the eight (8) A C C U R A T E domains
- Ranking against the test population

"Employers of ISO 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 organizations' 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
** indicative: subject to potential variations as the test population data may evolve over time.

Key Benefits

Organizations / Employers (MSS Team)	Conformity Assessment Bodies / Training Organizations / Consultants	Professionals
• Foster consistent understanding of ISO MSS across all levels and deliver predictable outcomes • Effectively implement MSS at strategic and operational levels • Upskill employees • Demonstrate training effectiveness • Facilitate recruitment	• Enhance your organization's credibility and consistency • Differentiate your offerings in the market • Provide evidence to meet accreditation requirements • Verify comprehensive knowledge and competence • Identify and bridge potential competence gaps	• Facilitate professional development and career advancement • Instil confidence in your expertise • Enhance competitiveness with a globally recognised qualification • Rank yourself against the test population • Identify and bridge potential competence gaps

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 ISO standard's practical implementation.

II. 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
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.

III. 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 **Ac**tual requirement in the standard related to documented information.

Co: **Co**ncept - 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 **C**lause reference of a specific requirement in the ISO management system standard

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

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

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

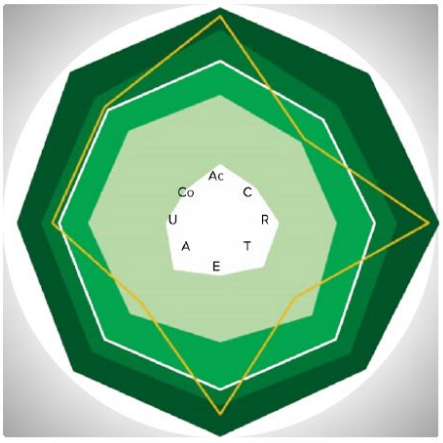
T: **T**erms and definitions used in the standard. Generally these are defined in Clause 3 of each ISO management system standard. In the case of ISO 9001 QMS, terms and definitions are defined in the ISO 9000 standard.

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

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

ACCURATE Analytics

Domain of Understanding	Score
Ac (Actual documentation)	92%
Co (Concept)	73%
C (Clause reference)	53%
U (Unspecified requirement)	75%
R (Requirement)	93%
A (Applicability)	50%
T (Terminology)	47%
E (Erroneous documentation)	85%
Overall score	71.0%



Each coloured band represents 25% of test population score.
White ring represents score of 50% of test population.
Golden ring represents the candidate score.

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

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

   A. document control procedure
   B. master list of relevant interested parties
   C. results of management review
   D. all of the above

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

2. Which of the following is not one of the CIA triad?

   A. confidentiality
   B. independence
   C. availability
   D. integrity

   *(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 7.2b
   D. none of the above

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

4. Which of the following is not an ISO/IEC 27001 requirement?
   A. conduct internal audit once per year
   B. assign responsibilities within the ISMS
   C. ensure internal auditors are competent
   D. conduct management review

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

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

   A. maintained
   B. signed by top management
   C. communicated to all interested parties
   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 control policy
   C. fixing a software bug
   D. none of the above

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

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

   A. internal audit procedure
   B. ISMS manual
   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

Additional information

www.isto.ch	*ISTO background; Test programme; Test Centres*
portal.isto.ch	*Create candidate account; Experience Free Trial Test*
J22	*Test syllabus and reference sources (downloadable from www.isto.ch)*

J21.27001L2/240601