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

1. What is an ISTO Test of Understanding (the "TOU")?

1.1. Test of Understanding, Level 2 – Professional

This test is developed for ISO management system standards (the "MSS") professionals such as middle and senior management personnel, responsible persons (as defined under clause 5.3), internal auditors, third party certification body auditors and advisors/consultants who are instrumental in the effectiveness of the MSS implementation. It is a multiple choice test designed with three (3) outcomes:

Certification
- certifying the candidate on the understanding of the respective standard

Analytics
- measuring the level of understanding in the eight (8) A C C U R A T E domains

Ranking
- ranking a candidate's performance against the candidate population

Key Features
- No prerequisite requirements;
- Simple multiple choice test;
- Detailed syllabus with test preparation support;
- Robust test development process by international experts;
- Easily accessible; and
- No limitation on re-takes.

An ISTO Test focuses not only on understanding the requirements of a standard but is also designed to ensure that those who pass the test have demonstrated a knowledge of the underlying management system principles, definitions, applicability, distinguishing requirements from unspecified requirements and the standard's practical implementation.

Key Benefits
- Acquire the ISTO TOU certification;
- Assess the level of understanding;
- Identify potential weakness(es) in the A C C U R A T E domains;
- Know where one stands relative to other candidates; and
- Get prepared for next level of career advancement.

Employers of ISO/IEC 27001 ISMS auditors/consultants/tutors would find the ISTO TOU certification a good benchmark in their selection process, as the ISTO TOU adds value to the organizations' performance excellence and consistency. A course tutor with an ISTO TOU credential is able to offer learners a more accurate and comprehensive presentation of the standard.

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

The ISTO TOU consists of multiple choice questions with four (4) possible options of which only one (1) represents the 'best' option. The ISTO TOU is a closed-book online test, however candidates are allowed to refer to an unmarked copy of the respective ISO standard which is the only permitted reference material during the test. In an online test, the standard copy will be provided in a separate window, in addition to the test window.

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, together with controls specified in Annex A.
4	30	Six (6) scenarios with five (5) questions each focusing on the practical aspects of the requirements of the standard

Candidates who meet 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. See Appendix II.

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 documentation.

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/IEC 27001 ISMS, terms and definitions are defined in the ISO 9000 standard.

E: an Erroneous requirement in the standard related to documentation.

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

1. ISO/IEC 27001:2022 requires which of the following documentation 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 documentation, **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 documentation, **E**)*

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

J21.2701L2/230818 draft 1

Certificate of Achievement

Test of Understanding

Level 2 - Professional

SU2E/AE/23/21025

This is to certify that

Michael K W Jansen

625432

has demonstrated a clear understanding of the

ISO/IEC 27001:2022

Information security management systems requirements

by passing the

International Standardized Testing Organization's Test

on

9 June 2023

Secretary, Test Panel
International Standardized Testing Organization
www.isto.ch

Test Analytics Report

SU2E/AE/23/21025

Test date: 9 June 2023

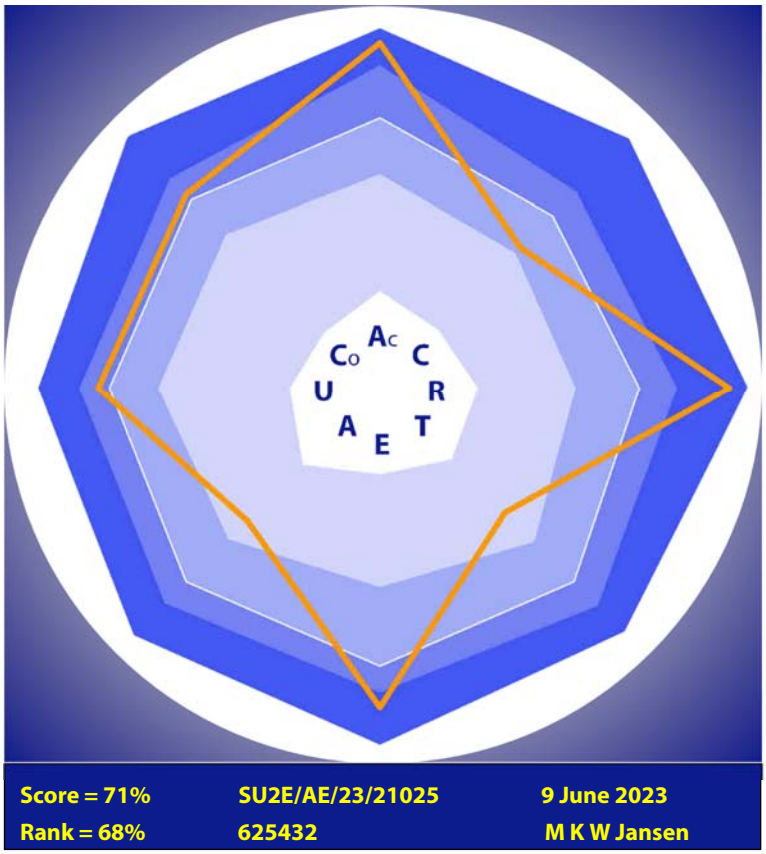
ISO/IEC 27001:2022	**Test of Understanding**	**Level 2 (Professional)**	
Name	**<first name> <last name>**		
Outcome	**<Pass>**	Unique Candidate Number	**< 625432>**
Overall score	**<71%>**	Overall rank	**<68%>**

Score summary by section

Section	No. of questions	Correct answers	Correct %
1. Principles & definitions, applicability	30	21	70%
2. Management system requirements	30	24	80%
3. Operational requirements	30	23	76%
4. Implementation	30	17	56%
Total =	120	85	71%

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%**



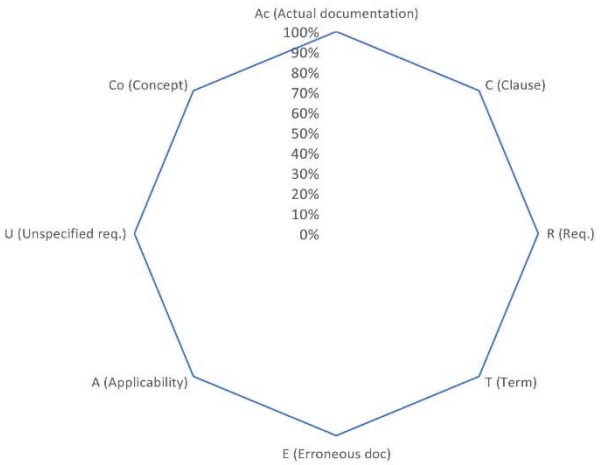
Each band represents 25% of candidate population score
White ring represents score of 50% of population

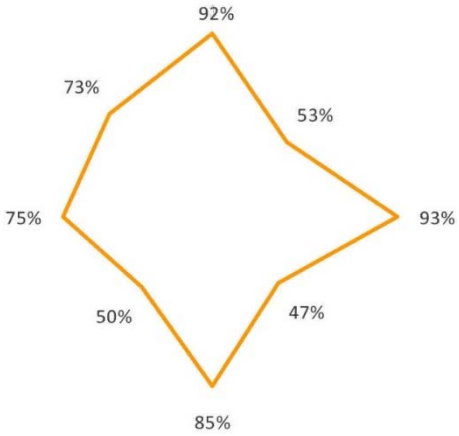
Test Panel
International Standardized Testing Organization
Report printed <12 June 2023>

J32/211221

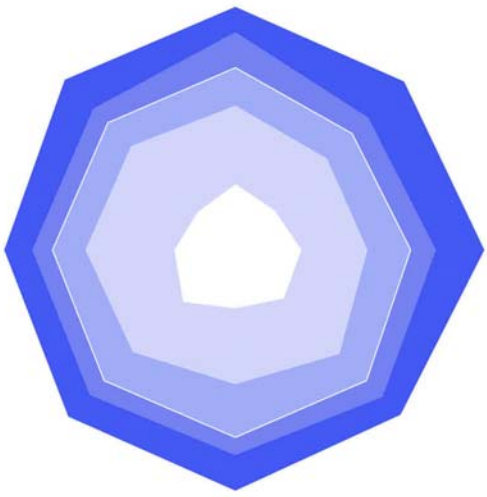
Star diagram explanatory notes

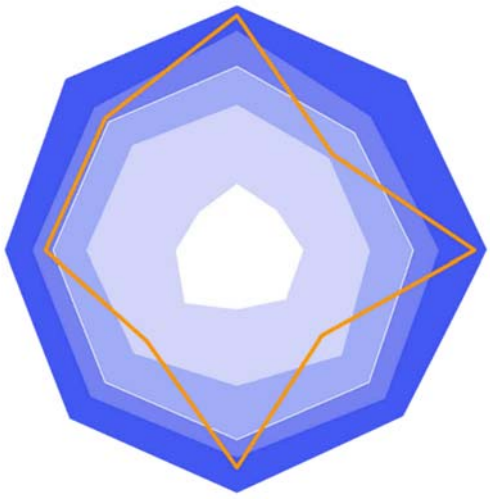
The Understanding Octagon	**The Candidate Score** (golden ring)
The axis radiating from the centre to one of its eight corners is the linear scale of the score in the level of understanding in that domain, from 0 to 100%.	Based on the scores achieved in each of the domain of understanding, the 'score octagon' of the candidate can be established.





The Population Score (4 bands)	**Overall Presentation** (ranking)
The four octagonal bands represent the lowest to the highest scores in 25 percent quartiles of the candidate population. The white octagon in between is the score of 50% of the population.	If the corners are in the outmost band, then the candidate ranks better scores than 75% of the population. If the corners are within the white octagon, then it ranks lower than 50% of the population.





Raw data of the above diagram (fictitious)

Score of candidate population =>	100%	75%	50%	25%	0%	Candidate
Ac (Actual documentation)	96%	86%	72%	57%	26%	92%
Co (Concept)	95%	79%	71%	58%	21%	73%
C (Clause)	94%	74%	65%	51%	22%	53%
U (Unspecified requirements)	91%	80%	72%	59%	24%	75%
R (Requirements)	98%	79%	69%	52%	26%	93%
A (Applicability)	93%	81%	73%	57%	29%	50%
T (Term)	92%	82%	73%	58%	27%	47%
E (Errorenous doc)	95%	81%	74%	53%	23%	85%