



**jtsec**

BEYOND IT SECURITY



Let's harmonize labs competence ISO  
19896

# Index

- ❑ 1. Introduction
- ❑ 2. ISO/IEC 19896 Structure
- ❑ 3. ISO/IEC 19896 Part 1
- ❑ 4. ISO/IEC 19896 Part 3
- ❑ 5. ISO/IEC 19896 Part 3 - Annexes
- ❑ 6. Conclusions



# Introduction

- ❑ One important factor in assuring comparability of the results of evaluations is to understand that the evaluation process includes the specification of both objective and subjective assurance measures.
- ❑ Hence the competence of the individual evaluators is important when the comparability and repeatability of evaluation results are the foundation for mutual recognition



# Introduction

- ❑ ISO/IEC 17025 defines some competence requirements:
- ❑ 6.2.2 The laboratory shall document the competence requirements for each function influencing the results of laboratory activities, including requirements for education, qualification, training, technical knowledge, skills and experience.
- ❑ 6.2.3 The laboratory shall ensure that the personnel have the competence to perform laboratory activities for which they are responsible and to evaluate the significance of deviations.
- ❑ 6.2.5 The laboratory shall have procedure(s) and retain records for:
  - ❑ a) determining the competence requirements;
  - ❑ ...
  - ❑ f) monitoring competence of personnel.



# Introduction

- ❑ ISO/IEC 23532 further refines these requirements:
- ❑ 6.2.5.1 The evaluation laboratory shall have procedure(s) and retain records for:
  - ❑ a) determining the competence requirements for personnel in **ISO/IEC 19896-3**;
  - ❑ ...
  - ❑ f) monitoring of competence of personnel.
- ❑ **NOTE The laboratory shall review annually the competence of each evaluator for each test method the evaluator is authorized to conduct.** The evaluator's immediate supervisor, or a designee appointed by the Laboratory Director, shall conduct annually an assessment and an observation of performance for each evaluator. A record of the annual review of each evaluator shall be dated and signed by the supervisor and the employee. A description of competency review programs shall be maintained in the management system.



# Introduction

- ❑ ISO/IEC 23532 further refines these requirements:
  - ❑ 6.2.6.1 Laboratory evaluator collectively shall have **knowledge or experience** for any specific **technologies** upon which an evaluation is conducted in **ISO/IEC 19896-3:2018**
  - ❑ 6.2.7 The evaluation laboratory shall maintain a competent administrative and technical personnel appropriate for ISO/IEC 15408-based IT security evaluations. The laboratory shall maintain **position descriptions, training records, and resumes** for responsible supervisory personnel and laboratory evaluators who influence the outcome of security evaluations.



# ISO/IEC 19896 Structure

ISO 19896 IT security techniques — Competence requirements for information security testers and evaluators —



Part 1 Introduction, concepts and general requirements



Part 2 Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers



Part 3 Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators





# ISO/IEC 19896 Structure

- ❑ Part 1 Introduction, concepts and general requirements
- ❑ Elements of competence
- ❑ Competency levels
- ❑ Measurement of elements of competence
- ❑ Annex A: Example structures for describing competence requirements
- ❑ Annex B: Example records of experience and competence



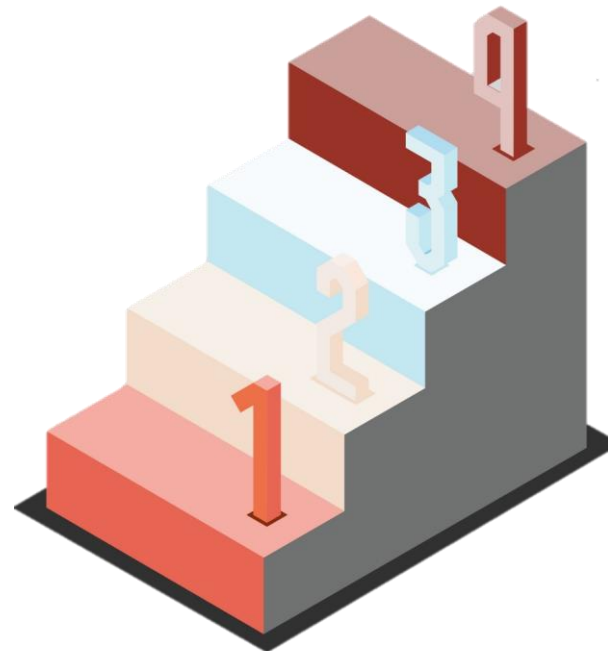
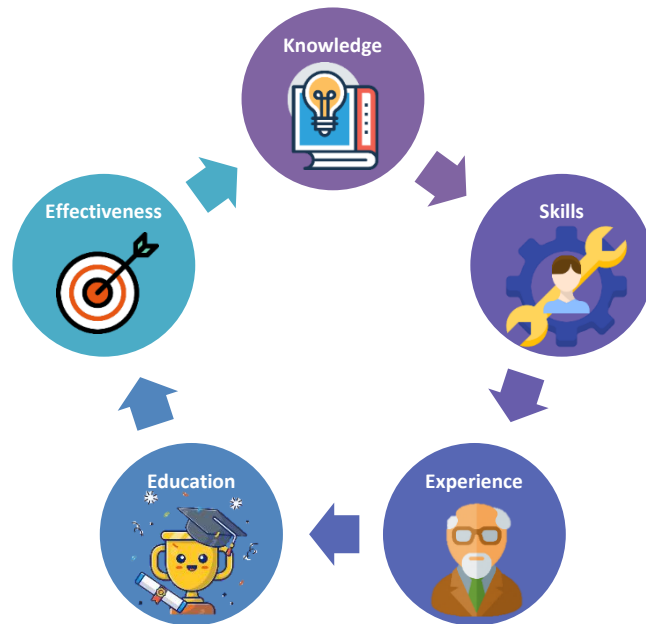
# ISO/IEC 19896 Structure

- ❑ **Part 3** Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
- ❑ Baseline for the minimum competence of ISO/IEC 15408 evaluators for each element of competence (knowledge, skills, experience,...)
- ❑ Annex A (informative) Technology types: knowledge and skills
- ❑ Annex B (informative) Examples of knowledge required for evaluating SARs
- ❑ Annex C (informative) Examples of knowledge required for evaluating SFRs



# ISO/IEC 19896 Part 1

- The standard defines 5 elements of competence and 4 competency levels



# ISO/IEC 19896 Part 1

## ❑ Elements of competence

- ❑ **Knowledge:** facts, information, truths, principles of understanding acquired through experience or education



- ❑ Of the standard
- ❑ Of the testing or evaluation methods
- ❑ Policies and procedures of relevant approval authorities
- ❑ Of IT product architecture and design in relevant technology areas



# ISO/IEC 19896 Part 1

## ❑ Elements of competence

- ❑ **Skills:** ability to perform a task or activity with a specific intended outcome acquired through education, training, experience or other means
- ❑ Understanding the boundaries, documentation analysis, selection of appropriate testing methods, calibrating and using tools, build a test environment, performing testing, interpreting results, write reports, ...



# ISO/IEC 19896 Part 1

## ❑ Elements of competence



- ❑ **Experience:** involvement at a practical level with projects related to the field of competence



- ❑ **Education:** process of receiving or giving systematic instruction, especially at a school or university



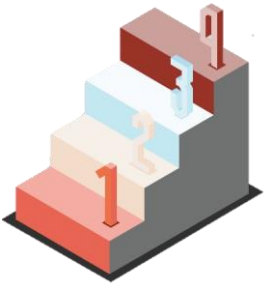
- ❑ **Effectiveness:** ability to apply knowledge and skills in a productive manner
  - ❑ Accuracy of test results, ability to repeat, ...



# ISO/IEC 19896 Part 1

## Competency levels

- ❑ Assigned for each competence area of 19896-3
  - ❑ Level 1 Associate: works under supervision
  - ❑ Level 2 Professional: requires supervision in just a few areas
  - ❑ Level 3 Manager: works unsupervised in most testing or evaluation areas, supervises level 1 and 2
  - ❑ Level 4 Principal: fully competent for at least one technology area, able to communicate with stakeholders, works unsupervised in all areas, supervise other levels.
- ❑ Overall level of competency may determine designation of professional capability: Technician/Evaluator/Senior Evaluator/Lead Evaluator



# ISO/IEC 19896 Part 1

## Measurements of elements of competence

Measuring is mandatory, how to do it is not mandatory

**Knowledge:** 19896-3 provides a measurable body of knowledge.

We may decide who will measure: The CAB-CB? The ITSEF?  
Third parties?

Training records and professional certifications

**Skills:**

Lab proficiency-testing programme (as required by 17025)

Feedback from other skilled personnel





# ISO/IEC 19896 Part 1

## Measurements of elements of competence

### Experience:

- Records of projects completed

### Education:

- Certificates issued by organizations recognized as legitimate by the approval authority

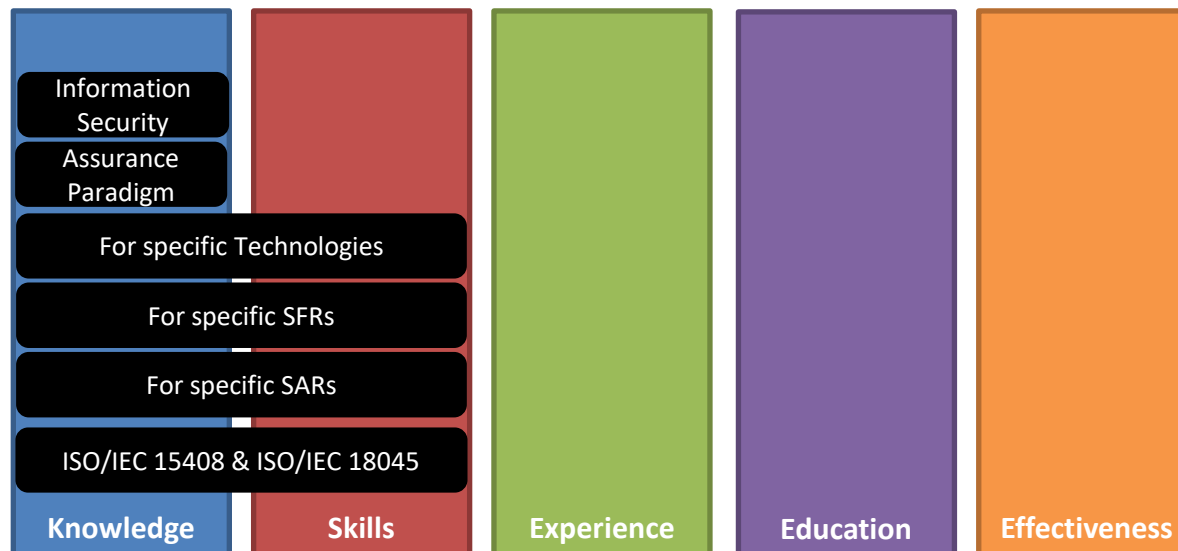
### Effectiveness:

- Time needed, nonconformities, adaptability , accuracy, ...



# ISO/IEC 19896 Part 3

- ❑ Provides baseline for the minimum competence of ISO/IEC 15408 evaluators for each element of competence (knowledge, skills, experience,...)



# ISO/IEC 19896 Part 3



- Knowledge:** what an evaluator knows and can describe
- ISO/IEC 15408 and ISO/IEC 18045
  - Terms and definitions
  - Protection profiles and packages
  - SFRs and SARs
  - The evaluation process
  - Method and activities
- The assurance paradigm
  - The evaluation authority: policies, recognition agreements, supporting documents, ...
  - The evaluation scheme: interpretations, guidance policies, ...
  - The lab and it's management system: policies, process and procedures; methods; competence requirements.



# ISO/IEC 19896 Part 3



- Knowledge:** what an evaluator knows and can describe
- The technology being evaluated
  - Common security architectures for each technology type. (See Informative Annex A Technology types: Knowledge and skills, based on classical CC categories).
- Protection Profiles, packages and supporting documents
- Since it is continually evolving, it is not possible to identify requirements for each technology, but can be obtained through experience. Experience can be developed by:
  - Education
  - Working as a trainee
  - Working as developer
  - Performing research



# ISO/IEC 19896 Part 3



- ❑ **Knowledge:** what an evaluator knows and can describe
- ❑ Each lab may define their technology types and requirements.
- ❑ Information Security: security principles, attacks, attack potential, SDLC, testing, vulnerabilities, ...
- ❑ Knowledge required for SARs (See Informative Annex B Examples of knowledge for SARs)
- ❑ Knowledge required for specific SFRs (See Informative Annex C Examples of knowledge for SFRs)



# ISO/IEC 19896 Part 3



- Skills:** what an evaluator is able to do
  - Basic evaluation skills
    - Evaluation methods: sampling, analysis, recording results, ...
    - Evaluation tools: report generation, specialized tools
  - Core evaluation skills given in ISO/IEC 15408-3 and ISO/IEC 18045
    - Evaluation principles: impartiality, objectivity, repeatability, reproducibility
    - Evaluation methods and activities (knowledge of the ISO 18045 verbs like check/confirm/demonstrate/....)
- Skills required when evaluation specific SARs
  - General: ability to write ORs
  - For each assurance component specific skills are required (mandatory)
    - E.g. VAN.3 Flaw hypothesis development



# ISO/IEC 19896 Part 3



- ❑ **Skills:** what an evaluator is able to do
  - ❑ Skills required when evaluation specific SFRs (mandatory)
    - ❑ General: ability to understand and test for conformance and search for vulnerabilities
    - ❑ E.g. FCS being able to determine if crypto algorithms and protocols are implemented correctly
  - ❑ Skills needed when evaluating specific technologies.
    - ❑ See Informative Annex A Technology types: Knowledge and skills, based on classical CC categories.
    - ❑ Like in Knowledge, skills can be obtained through experience.



# ISO/IEC 19896 Part 3

## Experience



- Experience is gained during the first and subsequent evaluations performed by an evaluator.
- Also during consultancy or product development

## Education



- At a minimum
  - Tertiary education with at least 3 years of IT studies
  - Experience which provided equivalent knowledge skills and effectiveness





# ISO/IEC 19896 Part 3

## ❑ Effectiveness

- ❑ Timely evaluations, e.g. time needed to develop or execute a test
- ❑ Accurate evaluations, e.g. comments received during validation
- ❑ Reports contain rationales and references with direct and focused language quickly understandable by the intended reader of the report.



# ISO/IEC 19896 Part 3

## ❑ Effectiveness

- ❑ Evaluator shall be able to apply knowledge and skills in a productive manner: aptitude, initiative, enthusiasm, willingness, ...
- ❑ Required evaluation principles: impartiality, objectivity, repeatability, reproducibility
- ❑ Scheme guidance and procedures are followed



# ISO/IEC 19896 Part 3 – Annexes

Annex A, technology types: knowledge and skills

Knowledge



- Knowledge required by evaluators working with specific technologies. List concepts that shall be known by evaluators for each classic CC technology category.
  - PPs related to technology type
  - Evaluation methods and activities related to the technology type
  - Technological standards related to the technology type
- The depth of knowledge depends on the assurance classes (e.g. Evaluators doing ALC may require less knowledge)



# ISO/IEC 19896 Part 3 – Annexes

Annex A, technology types: knowledge and skills

Knowledge



E.g. Databases

Concepts of data base management systems architecture

Access control methods



# ISO/IEC 19896 Part 3 – Annexes

Annex A, technology types: knowledge and skills

Skills



Mostly related to ATE

Skills required by evaluators working with specific technologies

Performance of evaluation methods and activities associated with the technology type

Being able to understand related technological standards

Lists the skills that shall be build upon evaluators for each classic CC technology category



# ISO/IEC 19896 Part 3 – Annexes

- ❑ Annex A, technology types: knowledge and skills

- ❑ Skills



- ❑ E.g. Databases

- ❑ Being able to correctly configure the database management system (DBMS) platforms

- ❑ Being able to use structure query language (SQL) or other database query languages.



# ISO/IEC 19896 Part 3 – Annexes

- Annex B, examples of knowledge for SARs
- Minimum knowledge required for each SAR class. E.g.
  - ADV\_ARC.1:
    - Self-protection property
    - Domain separation property
    - Non-bypassability property
    - Secure architecture and design concepts



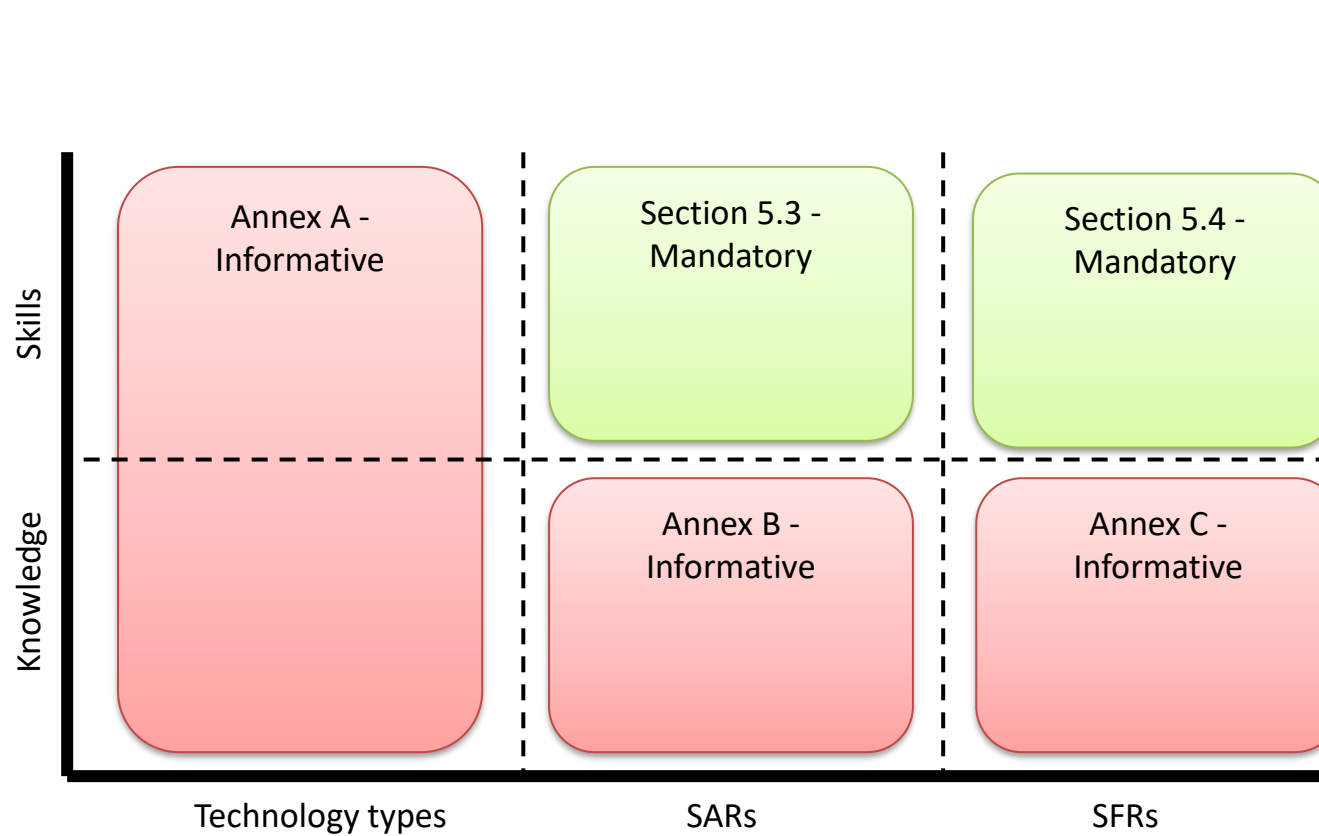
# ISO/IEC 19896 Part 3 – Annexes

- Annex C, examples of knowledge for SFRs
  - Minimum knowledge required for each SFR class. E.g.
    - FCO (Communication) Class
      - Proof origin
      - Non-repudiation of origin
      - Non-repudiation of receipt





# ISO/IEC 19896 Part 3 – Annexes



# How to implement in 6 easy steps?

- 1.- Define each job position for each evaluator level including the requirements in terms of competence
- 2.- Record the education and experience of each evaluator
  - Validate years of education or experience based on well-known person certifications?
- 3.- Track the knowledge you transmit to your team
- 4.- Assess the skills through questionnaires
- 5.- Evaluate the effectiveness through internal reviews and intercomparisons
- 6.- Put it all together!



# Conclusions

- ❑ The ISO 19896 framework for competency is a good framework but every lab shall define their technology types and knowledge (/skills) requirements because some are kind of ‘artificial’, specially Annex A.
- ❑ A competence management system can be used just to pass audits, not being really useful. Lab managers already know their evaluators, but this may not scale. Garbage in – Garbage out.
- ❑ It is difficult to reflect some intangible skills like the “killer instinct” or the skill to report. There is always some subjectivity.



# Contact

**jtsec Beyond IT Security**

Granada & Madrid – Spain

[hello@jtsec.es](mailto:hello@jtsec.es)

[www.jtsec.es](http://www.jtsec.es)



“Any fool can make something complicated. It takes a  
genius to make it simple.”  
Woody Guthrie