QTICS GROUP

PROFESSIONAL.INTELLIGENT.HUMAN

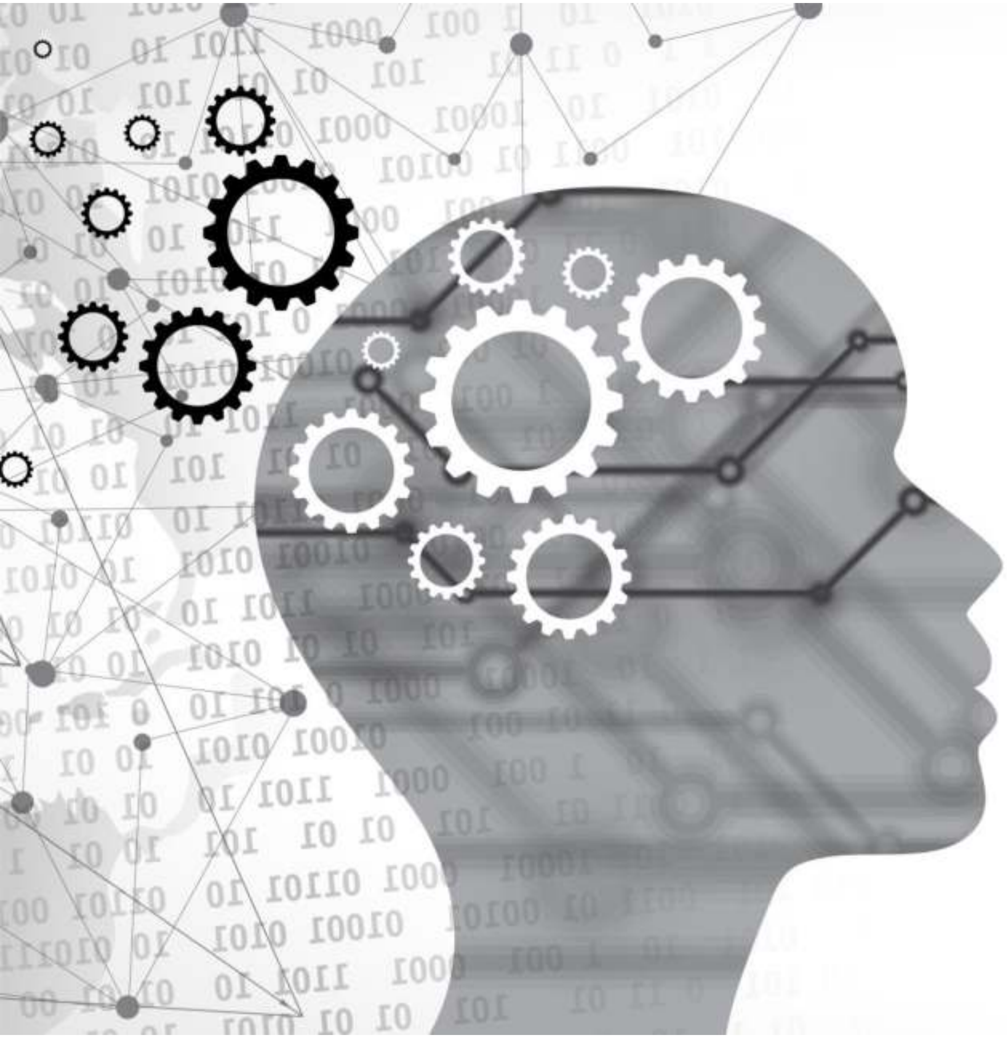
IMPLICATIONS OF CONFORMITY ASSESSMENT <-> **AI** ACT

Human-Centered Regulation of AI Conference

@ Technical University of Budapest, 2023 06 28, 11h50-12h15

by Zoltán Karászi

TABLE OF CONTENTS:



1. Opening Quote: ASIMOV - 1
2. Definition of TRUST and RISK. What is their relation? Why TIC?
3. Trustworthy? Who says that? Based on what??
4. Let us apply all these, to see „assessability of conformity” of AI in EU!
5. Further key elements of the AI ACT relevant for compliance
6. What does the AI ACT prescribe as of now (EP version) for high-risk AI systems?
7. How is it from a given TOE’s point of view? → e.g.: AI driven Medical Devices
8. Best practices so far - 1 – Fraunhofer IAIS
9. Best practices so far - 2 – TÜV-IT / TÜV NORD
10. Best practices so far - 3 – AICERT
11. What is next? Estimated time-line for AI-Certification „as usual”
12. Closing quote: ASIMOV – 2

Agenda of conference: https://hcaim.bme.hu/en/hcrai/

“After all, all devices have their dangers.

The discovery of speech introduced communication—and lies.

The discovery of fire introduced cooking—and arson. The discovery of the compass improved navigation—and destroyed civilizations in Mexico and Peru. The automobile is marvelously useful—and kills Americans by the tens of thousands each year. Medical advances have saved lives by the millions—and intensified the population explosion.”

— *Isaac Asimov, Robot Visions*

Definition of TRUST and RISK. What is their relation? Why TIC?

- **TRUST** is 'a psychological state comprising the intention to accept vulnerability based upon the positive expectations of the intentions or behavior of another'
  — Rousseau, Sitkin, Burt, & Camerer, 1998, p. 395

- **RISK** : the probability or likelihood that a negative event will occur

- **CONFORMITY ASSESSMENT**: The process of conformity assessment demonstrates whether a product, service, process, claim, system or person meets the relevant requirements.
  - **T**esting: determination of one or more characteristics of an object of conformity assessment, according to a procedure.
  - **I**nspection: examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements.
  - **C**ertification: third-party attestation related to products, processes, systems or persons.

— Wikipedia

A PROFESSIONAL THIRD PARTY CONFORMITY ASSESSMENT WILL REDUCE RISKS, SO INCREASING THE TRUST!

Trustworthy? Who says that? Based on what??

Trustworthy? Who says that? Based on what??

Zoltán KARÁSZI

founder and chairman of the board of QTICS Group

- ❖ Electrical engineer and economist
- ❖ 13 years in the Testing, Inspection and Certification sector
- ❖ Successful architecture of **10+ EU Notified Body domains** under QTICS Group
- ❖ (NoBo 2102 & NoBo 2806)

…„innovatio necesse est, vivere non est necesse”…

https://www.qtics.group/

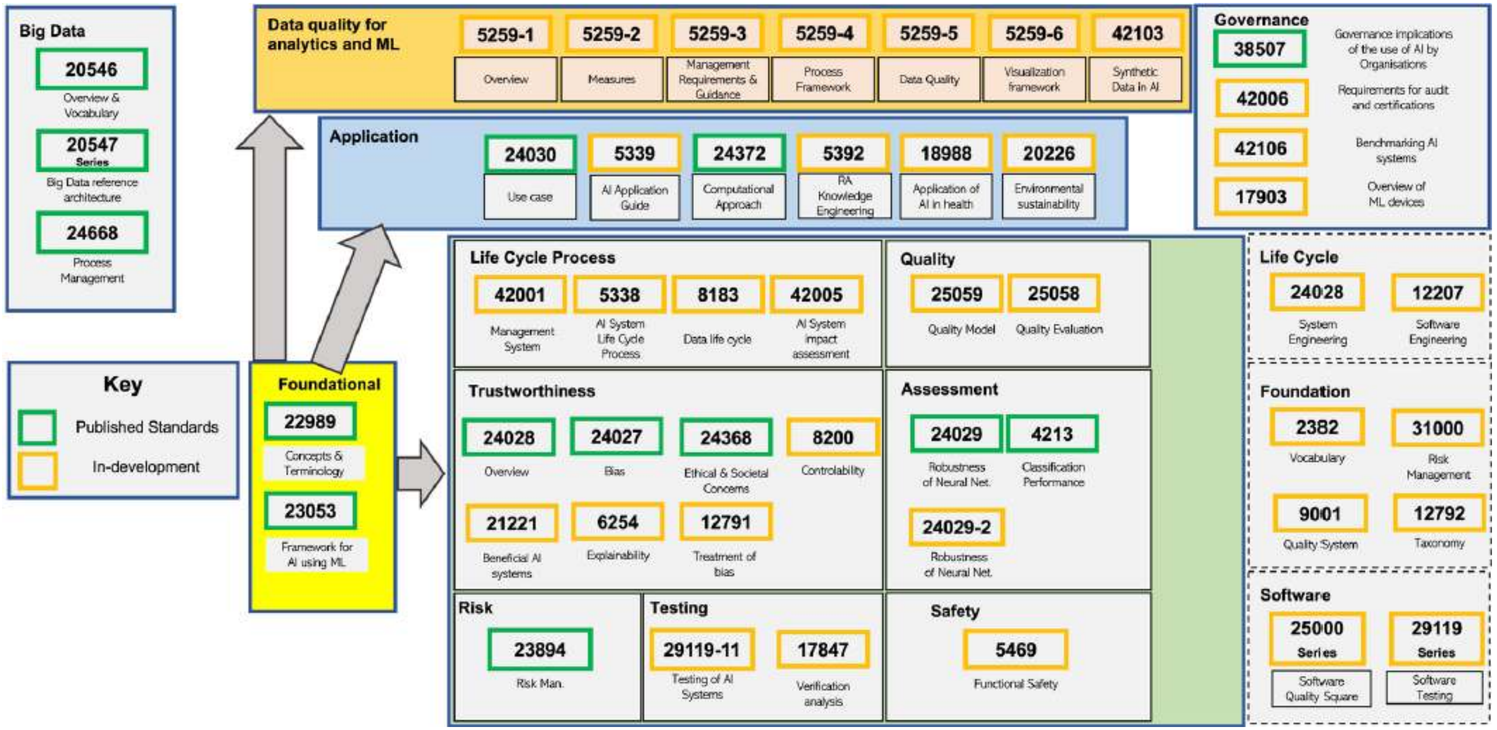
WE BELIEVE IN KNOW-HOW SHARING, HUMAN COLLABORATION & INTELLIGENT NETWORKS

ACCREDITATION is the independent, third-party evaluation of a conformity assessment body (such as a certification body, inspection body or laboratory) against **RECOGNIZED STANDARDS**, conveying formal demonstration of its impartiality and competence to carry out specific conformity assessment tasks

DESIGNATION is an authorization to carry out conformity assessment activities.

A NOTIFIED BODY is a conformity assessment body which has been published by the European Commission on a dedicated website, indicating the products and conformity assessment procedures covered by the designated conformity assessment area and the identification number of the body.

ONLY A THRUTSWORTHY ORGANISATION CAN ACT CREDIBLY IN REDUCTION OF RISK & INCREASE TRUST !



Big Data
20546 Overview & Vocabulary
20547 Series Big Data reference architecture
24668 Process Management

Data quality for analytics and ML
5259-1 Overview
5259-2 Measures
5259-3 Management Requirements & Guidance
5259-4 Process Framework
5259-5 Data Quality
5259-6 Visualization framework
42103 Synthetic Data In AI

Governance
38507 Governance implications of the use of AI by Organisations
42006 Requirements for audit and certifications
42106 Benchmarking AI systems
17903 Overview of ML devices

Application
24030 Use case
5339 AI Application Guide
24372 Computational Approach
5392 RA Knowledge Engineering
18988 Application of AI in health
20226 Environmental sustainability

Life Cycle Process
42001 Management System
5338 AI System Life Cycle Process
8183 Data life cycle
42005 AI System impact assessment

Quality
25059 Quality Model
25058 Quality Evaluation

Life Cycle
24028 System Engineering
12207 Software Engineering

Key
🟩 Published Standards
🟨 In-development

Foundational
22989 Concepts & Terminology
23053 Framework for AI using ML

Trustworthiness
24028 Overview
24027 Bias
24368 Ethical & Societal Concerns
8200 Controlability
21221 Beneficial AI systems
6254 Explainability
12791 Treatment of bias

Assessment
24029 Robustness of Neural Net.
4213 Classification Performance
24029-2 Robustness of Neural Net.

Foundation
2382 Vocabulary
31000 Risk Management
9001 Quality System
12792 Taxonomy

Risk
23894 Risk Man.

Testing
29119-11 Testing of AI Systems
17847 Verification analysis

Safety
5469 Functional Safety

Software
25000 Series Software Quality Square
29119 Series Software Testing

Let us apply all these, to see „assessability of conformity” of AI in EU?

AI ACT: EU leads they way in defining regulations for AI Trustworthiness

Target of Evaluation – subject to Certification:
A Group of AI solutions – **high-risk category** – is considered to be assessed by Third Party CAB

The Conformity Assessment Body (CAB) shall be accredited by National Accreditation Body, then the CAB shall be designated by a „National Competent Authority”, finally approved by the EU Commission as Notified Body (and listed on the NANDO) → *(see AI ACT Chapter 4, Article 33)*

- „High-risk” AI Solutions to be tested against **recognized standards**!
- The test results shall be the basis for certification!
- Probably the certified items have to be registered in a unique publicly accessible database, so that Citizens can verify certified status
- Validity of Certification has to be maintained by **changes in TOE**!
- Market Surveillance Activity by dedicated EU/National Authorities?

FRAMEWORK → CERTIFICATION FRAMEWORK → ACCREDITATION → CONFORMITY ASSESSMENT → TRUST

Further key elements of the AI ACT relevant for compliance

A few key elements of the AI ACT relevant for compliance

Risk based categories

(4 → prohibited, high-risk, limited & minimal risk)

Accuracy, robustness and cybersecurity

(Chapter 2, article 15)

Human oversight

Authorized representative

What does the AI ACT prescribe as of now (EP version by 14th June 2023) for high-risk AI systems?

Article 16

Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;

(b) have a quality management system in place which complies with Article 17;

(c) draw-up the technical documentation of the high-risk AI system;

(d) when under their control, keep the logs automatically generated by their high-risk AI systems;

(e) **ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;**

(f) comply with the registration obligations referred to in Article 51;

(g) take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;

(h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;

(i) to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;

(j) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

How is it from a given TOE's point of view? → e.g.: AI driven Medical Devices

Horizontal regulation AND vertical regulation

- Horizontal: AI-ACT, but CSA & CRA, GDPR, etc..
- Vertical: Medical Device Regulation (MDR)

Example:

There are 4 risk categories defined in the EU AI act, and by **MDR** Class III 3 'high-risk' devices include most medical AI devices. (That's because most AI as a Medical Device performs clinical decision support or diagnosis.)

Above that are the Class IV 'unacceptable risk' devices such as emotion detection and biometric categorization which are banned under the new **AI-ACT**! Hm??

Active Medical Devices fall under the high-risk category of the **Cybersecurity Act..**

THE COMING AI ACT AS HORIZONTAL REGULATION STILL HAS TO BE HARMONISED WITH SECTORAL REGULATIONS!

Non-Accredited / Private Scheme

Fraunhofer

IAIS

SCIENCE's approach to AI Certification – I.

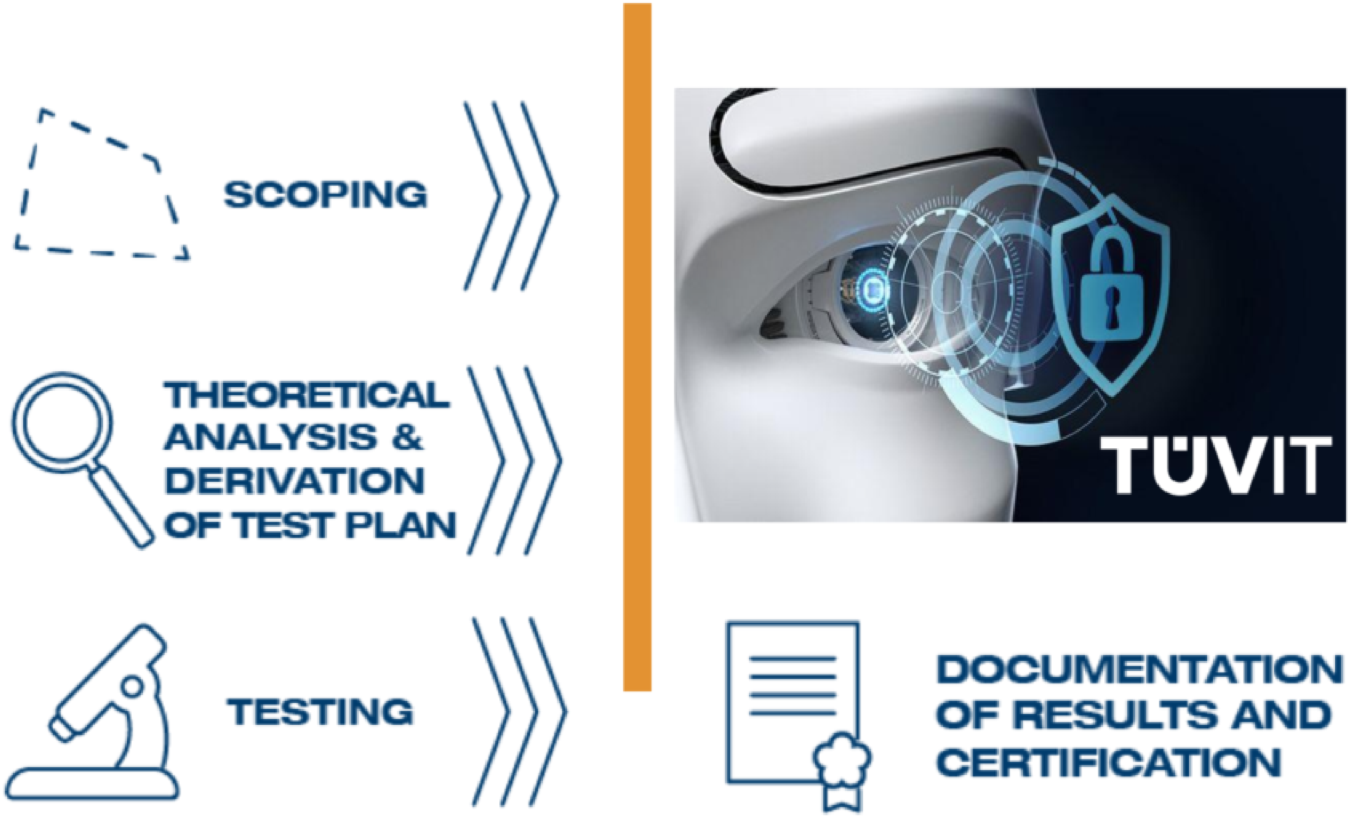
(research) →FRAUNHOFER IAIS

Intelligent Analysis and Information Systems

Publikationen | ZERTIFIZIERTE KI (zertifizierte-ki.de)

- 100% owned by **German State**, a leading scientific research organization
- **Scientific research** champion!
- Cooperation with Industrial Players

Non-Accredited / Private Scheme



SCOPING

THEORETICAL ANALYSIS & DERIVATION OF TEST PLAN

TESTING

DOCUMENTATION OF RESULTS AND CERTIFICATION

TEST Profi’s approach to AI Certification – II.

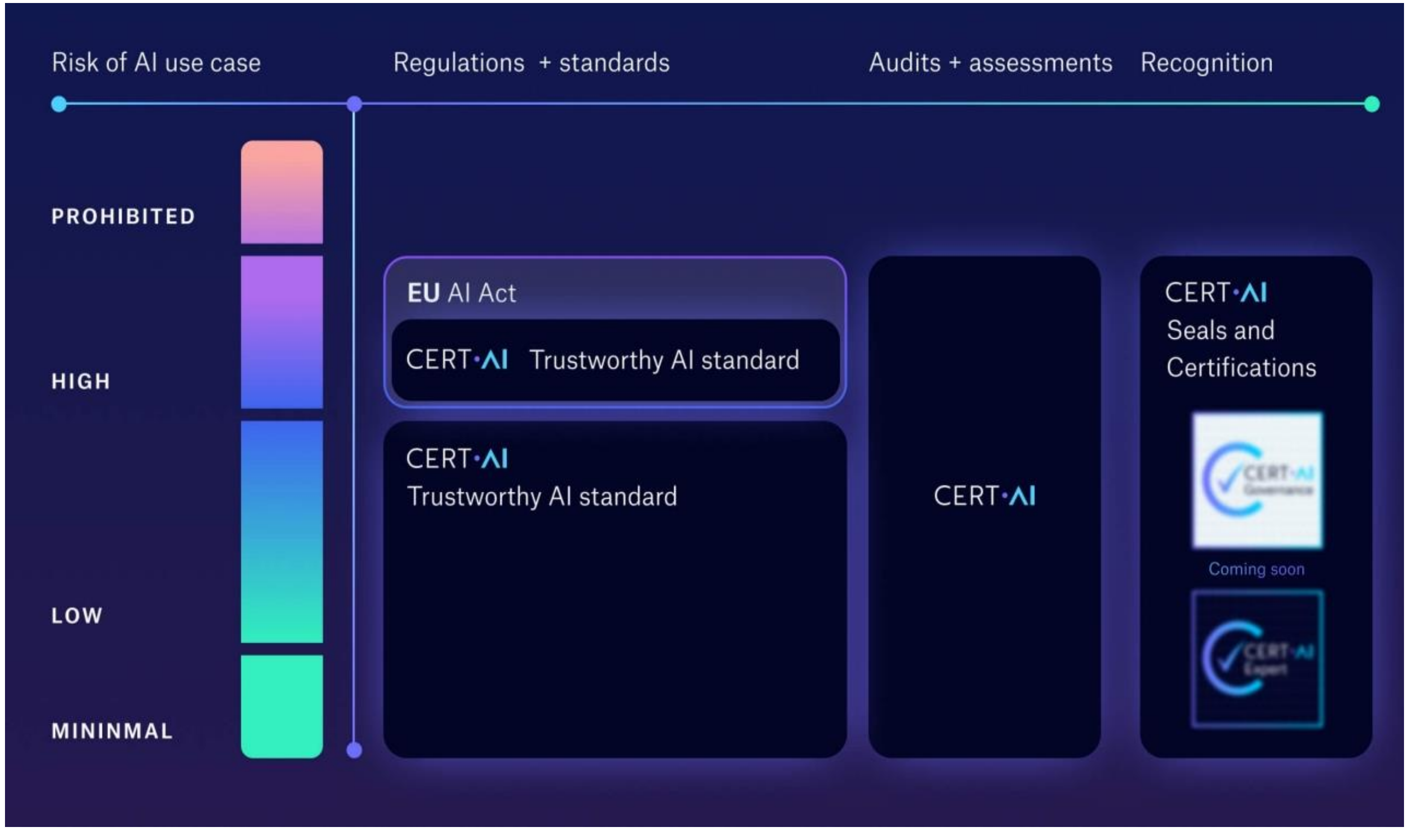
(pioneers) →TUV-IT ([Testing & Certification AI Security | Artificial Intelligence | TÜVIT (tuvit.de)](tuvit.de))

- 100% owned by **TÜV Nord**, a leading global Testing, Inspection & Certification company
- TÜV-IT is a **cybersecurity** specialist!
- Common Criteria evaluation up to **EAL7**
- **„No test – no fun!”**
- The test methodology has been continuously developed since 2018
- Cooperation with BSI (Bundesanstalt für..)

Insurer’s approach to AI Certification – III.

(no surprise..) →CertAI (Home | CertAI)

Non-Accredited / Private Scheme



- ❖ 100% owned by **Munich Re**, a leading global re-insurance company
- ❖ We combined Munich Re’s expertise in risk assessment with the leading AI knowledge of scientists at **Fraunhofer IAIS** to develop own Trustworthy AI standard → 6 dimensional control + **secret souce!!**
- ❖ CertX has a background in functional safety, cyber security and artificial intelligence, and being the Swiss national chair of INB 149 / NK 42 – Artificial Intelligence, CertX aims to build the first accredited AI certification scheme

What is next? Estimated time-line for AI-CErtification „as usual”?

THE FOUNDATION & SYSTEMATIC BUILDING OF THE EUROPEAN AI CONFORMITY ASSESSMENT TAKE 5+ YEARS!

❖ AI-ACT: next step is the TRILOG

the time need is estimated to be 24-36 month
The European Commission, The European Council &
the European Parliament must agree on final version

❖ STANDARDISATION

The time need is 36-48 month, or more..:

CREATION OF CERTIFICATION SYSTEM (rules, actors, procedures..

The time need is +24-36 month, or more..:
the certification scheme, the requirements for accreditation,
the preparation of the national accreditation bodies,
so that they are in a position to start with accreditation audits..

❖ ACCREDITATION AND NOTIFICATION (assessment of CABs, LABs)

The time need is +8-12 month:
The Applicant Conformity Assessment Bodies must apply officially
to the National Accreditation Bodies, then by the National Competent
Authority for the notification, then the usual process…

"**The religion** - which the Foundation has fostered and encouraged, mind you - is built on strictly authoritarian lines.

The priesthood has sole control of the instruments of science we have given Anacreon, but they've learned to handle these tools only empirically. **They believe in this religion entirely, and in the ... uh ... spiritual value of the power they handle.**

— *Isaac Asimov, Foundation*