HSbooster.eu
TRAINING ACADEMY

Intermediate 1

Course 5

STANDARDISATION TRAINING ACADEMY

Topic:

CONFORMITY ASSESSMENT SCHEMES AND SYSTEMS

November 23

Author:
Lucio González Jiménez | **Biljana Tošić**
SGS
University of Belgrade

Funded by the European Union

Module Objectives

After completing this module, you should be able to:

1. understand who can develop a certification scheme;
2. understand why should R&D projects learn how to develop a certification scheme;
3. understand what are the main motives for developing a certification scheme;
4. understand what are the main benefits of developing a certification scheme;
5. understand what are the main challenges of developing a certification scheme;
6. understand the process (step-by-step) of developing a certification scheme;
7. understand how certification schemes and systems evolve in the future;
8. understand the impact developing a certification scheme can have on European actors; and
9. understand the impact developing a certification scheme can have on international actors, as well.

Key Terms (Glossary)

conformity assessment scheme, conformity assessment system

About The Authors

Lucio Gonzalez Jimenez

SGS BrightSight in Spain

Business and strategy professional with more than 30 years of experience. He has worked for national and multinational high-tech technology sectors such as telecommunications, IT, Security, high technology projects management, IT Products (HW & SW) or Services commercialisation, design and deployment at national and international scales. Also, he has managed Research & Development and Innovation public-private entities (Cluster and R&D Centre) devoted to ICT Security and Defence technologies and has been an expert and evaluator of the European Commission in Security and Defence, as well as in dual-use technological companies. He has taken part in the high-level groups for the preparation of the Commission's paper "Report on the dual-use Potential of Key Enabling Technologies: identification of Strategic Areas for EU Civilian and Defence Markets" whose objective was to identify areas in which Europe should invest in innovation to fully benefit from technologies that have dual use in the civil and defence markets, especially involving SMEs. He also participated in the strategy to strengthen the defence and security sector focused on defence technology-based SMEs in Europe (Towards a more competitive and efficient defence and security sector) and was a speaker at the High-level Conference on the European Defence sector (Setting the Agenda for the European Defence Industry), a prelude to the preparatory action for the research in Defence. He specialises in market analysis, leadership and management of multidisciplinary and multicultural teams, both technical and commercial. He has developed his career in companies such as Ericsson, Mobiltron, Microelectrónica Española, Maxdata or Realsec/Utimaco, now Cybersecurity Lab Director in Madrid and Business Development Manager for Space and Defence at SGS Brightsight. He is currently Vice Chairman of ECSO and AEI of Cybersecurity of Leon, and coordinator of the EDIH of Cybersecurity of Leon. He is a member of the board of directors of the Circle Foundation of the Technologies for Defence and Security, and the SGS Brightsight CyberLab manager in Madrid.

Biljana Tosic

University of Belgrade in Serbia

Biljana Tošić is a Teaching Assistant and a Research Assistant at the Faculty of Organisational Sciences, University of Belgrade. She earned a B.Sc. and M.Sc. in Quality Management and Standardisation and another M.Sc. in Human Resources Management at the same Faculty. She is currently a Ph.D. Candidate, working on a doctoral dissertation titled "The significance of the expertise in standardisation for the internationalisation of SMEs". To date, she has been engaged in teaching several courses at the Faculty: Fundamentals of Quality, Standardisation 1, Metrology with the Fundamentals of Engineering, Normative Regulation of Quality, and Accreditation and Certification. She has been a member of the organisational

board of the World Standards Cooperation Academic Day 2019 and the International Cooperation for Education about Standardisation (ICES) WorkShop 2019. She has been a member of the technical board of the International Symposium SymOrg 2020 titled ''Business and Artificial Intelligence'' and the SymOrg 2022 titled ''Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the post-COVID Era''. She has been engaged in project III 47003 ''Infrastructure for technology-enhanced learning in Serbia'', supported by the Ministry of Education, Science, and Technological Development of the Republic of Serbia (2017-2020). She has been Editor in Chief of the Quality Media Station, the first media centre for quality established within the TEMPUS project titled ''Enhancement of Quality Infrastructure in Western Balkan Countries (EQIWBC)'' (2015-2017). She is currently a member of the National Mirror Committee Conformity Assessment & Quality Management KS CASCO at the Institute for Standardisation of Serbia (National Technical Committee related to ISO/CASCO, ISO/TC 176, ISO/TC 176/SC 1, ISO/TC 176/SC 2, ISO/TC 176/SC 3, ISO/TC 283, CEN/SS F20, CEN/TC 279, CEN/TC 379, CEN/TC 381, CEN/TC 389, CEN/CLC/JTC 1, and CEN/CLC/JTC 4).

Table of Contents

1 INTRODUCTION

While each conformity assessment activity should be treated differently, there are several proven advantages of using a systemic approach and the concepts of conformity assessment schemes and systems. [1] While **a conformity assessment scheme** usually describes ''a particular group of objects having sufficiently similar characteristics that the same set of rules and procedures can be carried out under the same management for assessing conformity with the same set of specified requirements''**, a conformity assessment system** ''uses a common set of rules, procedures or management for several conformity assessment schemes''. [2] Although ''rules and procedures may need to be detailed in different ways for different schemes'', there are several proven advantages in terms of ''efficiency and consistency to working within a common framework''. [3]

The **ISO/IEC 17000, Conformity Assessment – Vocabulary and General Principles** gives the definitions of these terms. According to the ISO/IEC 17000 **– a conformity assessment scheme** (which is sometimes referred to as a conformity assessment programme) is defined as ''a set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment'' whereas **a conformity assessment system** is defined as ''a set of rules and procedures for the management of similar or related conformity assessment schemes''. [4]

While a conformity assessment scheme can be managed within a conformity assessment system, both schemes and systems can be operated at an international, regional, national, sub-national, or industry level. [5] Which type of scheme or system would be the most appropriate under the given circumstances depends on several factors, such as the codes of conduct of the certification body, the complexity of the industry or the sector, etc. [6] Although some certificates may last for a limited period (e.g., 1 to 3 years), most of them have no time limit. [7] As long as the certified organisation regularly pays the annual fees and surveillance audits do not reveal major non-conformities that are not dealt with promptly, all the issued certificate remains valid. [8]

---

[1] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox.
Accessed on October 12, 2023. Retrieved from:
https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 81.
[2] Ibid.
[3] Ibid.
[4] ISO/IEC. (2020). ISO/IEC 17000, Conformity assessment – Vocabulary and general principles.
Accessed on October 12, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en.
[5] Ibid.
[6] Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit).
Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf, pp. 118.
[7] Ibid.
[8] Ibid.

Several types of conformity assessment schemes currently exist: [9]

- certification schemes,
- testing schemes,
- inspection schemes,
- verification schemes,
- validation schemes,
- accreditation schemes, etc.

Schemes can be set up as: [10]

- voluntary self-regulation or commercial marketing purposes or
- regulatory purposes to ensure compliance with legal requirements.

Schemes can be developed by: [11]

- professional and industrial associations,
- purchasers,
- regulators,
- non-governmental groups,
- Conformity Assessment Bodies (CABs),
- National Standardisation Bodies (NSBs), etc.

According to the **ISO/IEC 17011, Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies – accreditation scheme** may be defined as ''rules and processes relating to the accreditation of conformity assessment bodies to which the same requirements apply''. [12] Accordingly, accreditation scheme requirements may include (but are not limited to): ISO/IEC 17020, ISO/IEC 17021, ISO/IEC 17024, ISO/IEC 17025, ISO 17034, ISO/IEC 17043, ISO/IEC 17065, ISO 15189, and ISO 14065. [13]

Accreditation schemes are not addressed in this document.

[9] ISO. (2019). How to develop scheme documents: Guidance for ISO technical committees. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100439.pdf, p. 4.
[10] Ibid.
[11] Ibid.
[12] ISO/IEC. (2017). ISO/IEC 17011, Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:17011:ed-2:v1:en.
[13] Ibid.

1.1 WHAT IS A SCHEME OWNER?

Each conformity assessment scheme has an owner which means that: [14]

- a manufacturing company could develop a scheme for its products alone, including testing, inspection and auditing, leading to the issuing of declarations of conformity;
- a certification body could develop a scheme for its clients in which case the certification body takes on ''full responsibility for the design, application, management, and maintenance of the scheme'';
- a regulatory body or a trade association could develop a scheme and collaborate with one or more certification bodies to operate it in which case the regulatory body or a trade association takes on full responsibility usually by signing a contract or a formal agreement with the certification body;
- a group of certification bodies (from different countries) could also develop a certification scheme jointly in which case bodies (as joint owners of the scheme) must create a management structure which will enable the scheme to be operated effectively by all participating (certification) bodies.

If several schemes are using the same rules and procedures, the scheme owner(s) should set up a system under which all these schemes could effectively operate. [15] In this case, ''the scheme owner would become the system owner and be responsible for the management of the system and the schemes operating within it''. [16]

Additionally, within some sectors, it has been reported to be useful to operate a single system that supports a single scheme whereby one single set of standardised operating rules and procedures is developed which are then applied by all conformity assessment bodies that have been approved by the system to participate. [17]

The roles and responsibilities of scheme owners can include: [18]

- validating the scheme before it is implemented;
- establishing and changing the scheme, when necessary;
- ensuring that the scheme continues to meet market needs;
- adopting a continuous improvement approach, to ensure the scheme remains relevant; and
- informing the NSBs/CABs of any relevant information and developments relating to the scheme.

[14] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 83.
[15] Ibid.
[16] Ibid.
[17] Ibid.
[18] ISO. (2019). How to develop scheme documents: Guidance for ISO technical committees. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100439.pdf, pp. 14.

1.2 THE NEED FOR A SCHEME

A key step when setting up a conformity assessment scheme is determining the need(s) for such a scheme (and conformity assessment in accordance with such a scheme). [19] This means addressing different demands and/or requirements to demonstrate that an object of conformity assessment fulfils specified requirements. [20]

If the need exists, several additional issues must be considered: [21]

- issues of implementing the scheme in emerging, transition or developed economies;
- the objectives of the scheme;
- any existing schemes that could fulfil these needs or could serve as a model for a new scheme;
- International Standards developed by ISO and IEC that may form the basis for a range of schemes;
- the balance between the potential advantages and disadvantages;
- the impact of the proposed scheme on affected parties;
- external and internal issues relevant to the scheme and affected parties; and
- obtaining input from affected parties when developing or setting up a scheme.

1.3 THE SCHEME DESIGN BASED ON THE RISK OF NON-CONFORMITY

A key decision when setting up a conformity assessment scheme is who should carry out the conformity assessment. [22] This decision should be based on the risk assessment and the analysis of not only the likelihood of non-conformity but also the consequences which can arise from the non-conformity of products/services. [23] Sometimes, the consequences could be of a commercial nature (e.g., market reputation and sales volume) and sometimes, the consequences could be hazards to health and safety or even damage to the environment. [24] Consequently, the amount of time and money being spent on developing a conformity assessment scheme must be balanced against these consequences. [25] As the risks (and related consequences) become higher, conformity assessment activities become more extensive (involving expensive test equipment/procedures), so it may seem reasonable to contract out conformity assessment activities to a third (independent) party to

[19] ISO. (2019). How to develop scheme documents: Guidance for ISO technical committees. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100439.pdf, p. 9.
[20] Ibid.
[21] Ibid.
[22] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 84.
[23] Ibid.
[24] Ibid.
[25] Ibid.

carry out some activities or at least review the evidence of conformity and issue an attestation (a certificate). [26]

1.4 CREATING A SCHEME

All schemes should be designed and developed by competent individuals. [27] Their competence should cover both the technical field of expertise and the adopted conformity assessment procedure which will be used. [28] When creating a scheme, scheme developers should consider **ISO/IEC 17007, Conformity Assessment – Guidance for drafting normative documents**. [29] While International Standards are incorporated into many conformity assessment schemes around the world, such schemes cannot replace International Standards. [30] Rather, schemes may list additional requirements, besides those already given in International Standards. [31] Accordingly, if a scheme gives additional requirements on CABs, these cannot contradict or exclude any of the requirements given in the ISO/IEC 17000 standards series and if a scheme gives additional requirements on national accreditation bodies (NABs), these cannot contradict or exclude any of the requirements given in ISO/IEC 17011. [32] Additionally, scheme developers may also find useful the good standardisation practices given in the ISO/IEC Directives (which specify the requirements for ISO and IEC normative documents) and the World Trade Organisation's Agreement on Technical Barriers to Trade (WTO TBT Agreement), Annex 3, Code of Good Practice for the Preparation, Adoption and Application of Standards. [33] The ISO/IEC Directives, Part 2, 2004, 6.7, also covers aspects relevant when creating conformity assessment schemes and systems. [34]

When creating a scheme, the developers should follow the functional approach to conformity assessment described in the **ISO/IEC 17000, Conformity Assessment – Vocabulary and General Principles (Annex A).** [35]

[26] Ibid.
[27] ISO. (2019). How to develop scheme documents: Guidance for ISO technical committees. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100439.pdf, p. 13.
[28] Ibid.
[29] ISO/IEC. (2009). ISO/IEC 17007, Conformity Assessment – Guidance for drafting normative documents. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/standard/42635.html.
[30] ISO. (2019). How to develop scheme documents: Guidance for ISO technical committees. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100439.pdf, pp. 13.
[31] Ibid.
[32] Ibid.
[33] ISO/IEC. (2009). ISO/IEC 17007, Conformity Assessment – Guidance for drafting normative documents. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/standard/42635.html.
[34] Ibid.
[35] ISO/IEC. (2020). ISO/IEC 17000, Conformity assessment – Vocabulary and general principles. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en.

1.5 PRODUCT CERTIFICATION SCHEMES

Product certification is the mechanism whereby a certification body ''attests that products – either a batch or the continuous production thereof – have been inspected and tested by it and that the products collectively comply with specified requirements, usually contained in a standard''. [36] The attestation by the certification body is issued in the form of a certificate which is supported by a product certification mark – that the manufacturer is entitled to affix on a product after showing compliance with specified requirements. [37]

Product certification schemes are developed by certification bodies ''in both the public and private sectors, at both national and international levels, offering services in both the regulated and nonregulated domains''. [38] Within emerging economies, the NSB is usually the only organisation which offers product certification at the national level, while within more developed economies, product certification is offered by private sector certification bodies (eventually leading to the total withdrawal of the NSB and the state in many instances). [39] Since national product certification marks (usually the ones issued by the NSB) face serious obstacles in being recognised across national borders, various product certification marks have been developed recently, some of which are: [40]

- The British Standards Institution (BSI) Kitemark for general products, United Kingdom,
- The Geprüfte Sicherheit (GS, for “tested safety”) mark for product safety, Germany,
- The Underwriters Laboratories (UL) mark for product safety, United States,
- The American Society of Mechanical Engineers (ASME) mark for pressure vessels, United States,
- The Canadian Standards Association (CSA) mark for general products, Canada, etc.

* Note: The CE mark is not a product certification mark but a regulatory device of the European Union (EU).

The **ISO/IEC 17067, Conformity Assessment — Fundamentals of product certification and guidelines for product certification schemes** [41] describes seven types of product certification schemes suggesting that the elements in these seven existing schemes can be combined in other ways to create additional scheme types. [42]

[36] Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit). Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf, pp. 117.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] ISO/IEC. (2013). ISO/IEC 17067. Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17067:ed-1:v1:en:term:3.2.
[42] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 86.

1.6 MANAGEMENT SYSTEM CERTIFICATION SCHEMES

While product certification is all about the supplier-consumer relationship (as it determines product quality), **management system certification** is all about building confidence in the supplier's ability to continuously provide products and services that fulfil specified requirements. [43] The attestation by the certification body is usually issued in the form of a certificate which is supported by a wide range of materials and documents – that the organisation which is being certified can use for the purposes of marketing and/or public relations. [44]

Compared to product certification which is usually supported with a product certification mark that the manufacturer is entitled to affix on a product after demonstrating compliance with specified requirements – the management system certification does not assess or make any claims about the product quality (per se). [45] Rather, the management system certification denotes only the capability of the supplier to continuously provide products and services complying with contractual obligations which is why the management system certification emblem should not be affixed to the product – because it does not denote product compliance. [46]

The well-known management system certification schemes are based on **ISO 9001** for which over 1 million certificates have been issued around the globe since its development in the 1980s. [47] Additionally, various International Standards (e.g., **ISO 14001, ISO 27001**, and **ISO 50001)** a growing number of private standards (e.g., **IATF 16949**, **FSSC 22000,** and **FSC)** are also used for management system certification around the globe. [48]

1.7 PERSON CERTIFICATION SCHEMES

Person certification schemes set out ''the competence and other requirements related to specific occupational or skilled categories of persons''. [49] People who fulfil these requirements might end up being recognised as Certified Auditors, Certified Welders, and Certified Information Technology Security Specialists. [50]

---

[43] Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit). Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf, pp. 122.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 93.
[50] Ibid.

The **ISO/IEC 17024, Conformity Assessment — Fundamentals of product certification and guidelines for product certification schemes** [51] and **ISO/IEC TS 17027:2014 Conformity assessment — Vocabulary related to competence of persons used for certification of persons** [52] set out requirements and vocabulary for bodies operating certification of persons. [53] Clause 8 of ISO/IEC 17024 sets out specific requirements for the development and administration of certification schemes for persons, covering the following six areas: (1) certification scheme categories, (2) elements of a certification scheme, (3) process requirements, (4) development of the certification scheme, (5) continual review and validation of the scheme for persons, and (6) obligations of the scheme owner. [54] The ISO has published guidance to Clause 8 of ISO/IEC 17024:2012 entitled ''How to develop schemes for the certification of persons'' which can be assessed freely via the link. [55]

1.8 INTERNATIONAL CERTIFICATION SCHEMES

Over the years, several large CABs have established themselves by providing conformity assessment services in many countries. [56] They are recognised as multinational organisations in the area of conformity assessment (although these organisations are sometimes touted as international organisations – which they are not). [57] However, there are a few international organisations that manage international certification schemes, such as **the International Electrotechnical Commission (IEC)**, **the International Organisation of Legal Metrology (OIML)**, and **the UNECE World Forum for Harmonisation of Vehicle Regulations (Working Party 29 – WP.29)**. [58]

The **QI Diagnostics and Reforms Toolkit (Module 6 – Conformity Assessment)** which was jointly developed by the World Bank Group and the National Metrology Institute of Germany, explores in detail these organisations and the international certification schemes they manage and may be accessed freely via the link.

[51] ISO/IEC. (2012). ISO/IEC 17024:2012 Conformity assessment — General requirements for bodies operating certification of persons. Accessed on June 05, 2023. Retrieved from https://www.iso.org/standard/52993.html.
[52] ISO/IEC. (2014). ISO/IEC TS 17027:2014 Conformity assessment — Vocabulary related to competence of persons used for certification of persons. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/standard/62024.html.
[53] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 93.
[54] Ibid.
[55] Ibid.
[56] Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit). Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf, pp. 132.
[57] Ibid.
[58] Ibid., pp. 133-135.

1.9 CERTIFICATION SCHEME SELECTION

Several questions must be considered when choosing the type of certification scheme: [59]

- should it be a product certification scheme or a management system certification scheme?
- if the choice is a product certification scheme, is one already developed by a certification body or ''would a national one be more appropriate to serve the purpose in the short and long terms''?
- is a more general certification scheme required or would a sector-specific scheme be appropriate?
- if the choice is a general management system certification scheme, would it be focusing on quality, the environment, information security, food security, energy efficiency, etc., or their combination?
- if the choice is a sector-specific scheme, would it be focusing on automotive parts or medical devices?
- is the cost of developing a certification scheme worthwhile (compared to the potential benefits)?

Several questions must be considered when choosing the certification body: [60]

- is the certification body accredited for a standard to which certification is required;
- is the accreditation body (by which the certification body is accredited) a signatory to a multilateral recognition agreement (MRA) covering the scope you are interested in, such as those operated by the IAF for public standards or (in the case of private standards), the relevant multinational one?
- does the accreditation of the certification body cover the scope of the certification scheme?

Another criterion is whether the certification body is recognised in the marketplace, e.g. Does it have a list of well-known names among its certified clients and is this list of clients publicly available on the website? [61] A recognised certification body will not object to providing evidence and feedback from its certified clients.

The certification needs of a company may be manifold which is why some certification bodies can provide an integrated service – e.g., a system that integrates quality management and environmental management certification, and/or occupational health and safety and risk management, and/or even product certification. [62] If this seems like a more appropriate solution for the company, such an integrated certification service may be an obvious choice and may be more cost-effective than obtaining stand-alone certification for each area. [63]

[59] Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit). Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf, pp. 136.
[60] Ibid., pp. 138.
[61] Ibid., pp. 139.
[62] Ibid., pp. 139.
[63] Ibid., pp. 139.

2 INTERVIEW

Conducting an interview with:

Lucio Gonzalez Jimenez

SGS Brightsight

General Manager CyberLab Madrid

Can you tell us something about the work you do at SGS Brightsight?

With over 35 years of experience in evaluating IT products in different industries, SGS Brightsight supports manufacturers to get their products certified through independent third-party evaluations or audits, demonstrating (with impartiality) that their products comply with the security regulations and requirements. We evaluate these products against requirements set both by public and private certification schemes. These schemes use our evaluation reports to issue product certificates stating that evaluated products comply with their requirements. Thereby, a product certificate gives you access to the market you would like to serve. With our extensive list of schemes recognition, we also support industries all over the world and try to deliver meaningful and sustainable value to society.

2.1 WHO CAN DEVELOP A CERTIFICATION SCHEME?

Who can develop a certification scheme?

In my experience and I've been on different sides of the table, I've been on the manufacturers' side, I've been on the public and private side and right now I'm on the evaluation and certification side, I might say that both public and private organisations can develop certification schemes. The intention is to demonstrate (either to the market or to customers) the commitment they may have to sector-specific requirements, standards, etc. For public organisations, it's more related to compliance with regulatory requirements. This seems to suggest that the public sector will act as a regulatory profile because these organisations need (for example, food regulations, oil regulations, electricity regulations, etc.) standards that need to be fulfilled for the benefit of society and the industry. As such, private organisations usually get together themselves to reach a common agreement and promote some sector-specific certification schemes because they want to promote these requirements and demonstrate (on their own or through a third party) the compliance level of their products or services. Also, it could be seen as a set of requirements in a procurement process, as a part of the supply chain.

2.2 WHY BOTHER?

Why should R&D projects learn how to develop a certification scheme?

At the very beginning, when the consortium drafts or writes a proposal, R&D projects usually do not have a certification scheme in their minds or even their strategies, as an outcome of the project. What they have and it is relevant and linked to a certification scheme is a set of standards they have to apply. The main goal of most R&D projects is to provide a validated outcome and/or to uptake the market with new development, under a technological perspective. It could be a new technology project, or an innovation project and, depending on the technology readiness level (TRL), these outcomes will be closer to the market. Drawing upon the last ten years, the EU-funded projects have been following a trend to get closer to the market because Europe needs to improve the competitiveness of different industries. Speaking about cybersecurity or security and defence, we have a very strong feeling that we need to push innovation to the market. I might even say that R&D projects might not only need to know about the existing certification schemes but also know how to participate or mobilise a whole ecosystem. A certification scheme development needs the involvement of different stakeholders, so maybe they are more interested in attracting these stakeholders or maybe they need to be aware of existing certification schemes and how to fit into these certification schemes or how to improve them (given the project lifetime). If they find out that there is nothing in the market (which is very unusual), they can create a de facto standard which may eventually lead to developing a certification scheme(s).

What are the main motives for developing a certification scheme?

If we reel back to the first question, I drafted two scenarios, public and private. So, if we follow these two parallel scenarios, from the public sector's perspective, the motive is to regulate. For example, we need to fulfil quality standards or technical standards, as a set of requirements to reach a higher level of quality, safety, etc. Another motive is to support society and industries (consumers/end-users). When the project gets to an end and when a consortium sees a possibility to get to a market, to uptake a market opportunity, if we have a strong standards landscape or consolidated certification schemes – what we have is a lower volume of market entry barriers because the rules are clear – these are the requirements, and you must demonstrate your compliance with these requirements. Such compliance can be demonstrated through independent third-party evaluations or audits demonstrating (with total impartiality) that your products or services fulfil the standards and that you are qualified or competent in such contexts. From the private sector's perspective, the motive is to support industries to be more competitive and to enable customers or end-users access to better products and services. Speaking about the private sector, the industry has the motive to raise competitive sectors and bring new requirements, more demanding or more technologically advanced.

What are the main benefits of developing a certification scheme?

From the public sector's perspective, e.g., products in the cybersecurity domain, construction domain, and health and safety domain must fulfil a minimum of quality, health, and safety (and technological) requirements. When the public sector invests in new technology (e.g., health or telecommunications), it feels more reliable to acquire certified products instead of those that are not fulfilling (or there is no evidence of

fulfilling) relevant standards. The public sector relies on certified products. On the other hand, in the case of non-certified products, we rely on the goodwill of manufacturers. There is no doubt that there is always the goodwill to market the best of your products and services. The different story is when a third party checks if you are doing a good job because maybe you are doing a good job in your mind but, for example, in software development, forget to document all steps in the design process, or forget to document how you developed this software or how you fixed that bug. These things are usually described and are part of a set of requirements in a given standard.

For example, we have the GDPR, but we also have data protection technology solutions or products. These are different angles, but in the end, the main goal is to protect data or the identity of citizens. So, we can see different beneficiaries. For example, the public sector can rely on this new technology, manufacturers can be part of the market because of the fulfilment of relevant certification schemes, and society is aware of the government investment in reliable technology so customers and end-users can trust this new solution, this antivirus, or electronic signature device in their mobile phones to not compromise their bank account credentials because their mobile operator is very demanding with security, data protection, etc. So, from different perspectives, the trustworthiness of the products and services is the main benefit. For example, I could be a software provider, but I need to communicate with my customers, so I can benefit from the relationship with other vendors/other service providers. In the end, trustworthiness seems to be the main benefit.

What are the main challenges of developing a certification scheme?

From the private perspective, when addressing the need to develop a certification scheme, it is usually a matter of getting together and reaching a common agreement between private organisations, and to reach a common agreement (e.g., on quality or safety) means addressing both technical and business aspects. To be able to do so, the main challenge is determining who you can rely on. Who is who? What do we have to do? What do they have to do? Who is in charge of this? Who is in charge of that? Another challenge is ensuring communication and collaboration among different stakeholders, such as national accreditation bodies, certification bodies, and the industry (SMEs and large enterprises). Finally, there is a cultural aspect that must also be addressed. For example, if you are accredited as the certification body for products, services, and processes (in accordance with the ISO 17065 standard), you must continuously demonstrate your impartiality to a third party (e.g., national accreditation body) which will eventually get in touch with you aiming to obtain the objective evidence of such impartiality. In business, impartiality is hard (not to say impossible) to obtain. There are some very good examples, but eventually, it depends on the needs of the industry. If they need to get to the market, and they are delayed, they are out of the market. Certification is not a matter of speeding up, it's a constant activity. So, there is a cultural gap between the public and the private sector, which is diluting continuously, but not at the speed we would like. Accordingly, public organisations are a bit more aware of these matters, (e.g., impartiality, independence, or codes of conduct) that are needed to issue accredited certificates. With certification, you are providing differentiation value and that is the value of certification.

All of us are audited. For example, I must be able to provide objective evidence of the status of the product (e.g., or anything else the manufacturer wants to test). To be able to perform these tests (in the most

professional and qualified way), I have to be audited so my customer can rely on my professional capacity (of me and my company). This is probably the reason why certification bodies need to communicate more. For example, and this could be also interesting, everybody knows about the ISO 9001 quality management system standard, but 20 (or 30) years ago, quality was absolutely unknown. So, it takes time, but in the end, it's important to close this cultural gap.

2.3 HOW TO DEVELOP A CERTIFICATION SCHEME?

How would you describe the process (step-by-step) of developing a certification scheme?

To date, we have been part of both public and private certification schemes and I must say each one of them has its own way of understanding what they want to test, evaluate, and eventually try to certify. So, I might say that there is no specific methodology to develop a unique certification scheme. Instead of "How to develop a certification scheme", the question could be "What is needed to develop a certification scheme and who could participate in this initiative?". What is our interest in developing a certification scheme? Who has the competence to drive it? As mentioned above, developing certification schemes need to engage a whole ecosystem, a complex environment comprising different stakeholders, such as national accreditation bodies, certification bodies, test labs, and the industry. When it comes to private sector schemes, these can include academia, universities, research centres, and maybe even a public entity, and when it comes to public sector schemes, the ecosystem becomes wider including academic and legal entities, technical companies, and organisations (even SMEs).

As a certification scheme, you just put a set of requirements to the market and you said – here are the questions to the exam, it is up to you to answer them. For example, many certification schemes include the IT security or safety evaluation methodology, but we also have a common criteria evaluation methodology for functional security in SW/HW-SW-based products that was established by ISO and has been globally recognized. As a result, different governments agreed to accept the certificates based on a common methodology. Governments know very well what they want to protect. Let's say we want to protect IT products and services. As we want to protect society, we want to engage the industry. Three steps seem to be crucial. First, we must determine IT security requirements. Second, we must establish a methodology to evaluate the fulfilment of these requirements. Third, we must establish a threshold or a few thresholds (depending on the security demand level we want to apply). So, these steps differ significantly when it comes to quality, health, safety, food industry, oil, and gas, and agriculture industries. What do we want to certify? What is the technological context or the process that we want to evaluate and what are the requirements?

It's different from the private sector's perspective, as private organisations are more oriented towards the market and the business. If they want to create a private certification scheme, private organisations must be aware that it has to be consistent. Otherwise, customers and end-users will not buy products because everything goes public in the end. Lately, there is a trend (at least in the cybersecurity domain) – we are witnessing new private certification schemes directly addressing ISO 17025 or ISO 17065, as a minimum set of requirements to fulfil. Drawing upon the last five years, private schemes are acting as public schemes. These schemes are engaging a whole ecosystem, following the same path as the government, because they

opt to provide reliable, trustworthy, and quality products. Our feeling is that they aim to convince customers rather than seduce them. This is an important improvement, especially in cybersecurity where we are more sensitive to security, trust, and all those big words because the opposite meaning of these big words might be quite scary.

Finally, both private and public certification schemes follow the same path. They are gathering around both academic and legal entities, technical companies, and organisations (even SMEs). Large organisations must engage with SMEs, trying to understand how to collaborate more effectively, and in a more coordinated way. When I say that private certification schemes are following the same path as public certification schemes, maybe we will witness some kind of standardised methodology to develop a certification scheme because as long as they are converging to the same way to do things, we can only hope that someone will eventually say – maybe we need to standardise these a bit more. For the time being, the unique methodology of developing a certification scheme just does not exist.

2.4 PRIOR EXPERIENCE & LESSONS LEARNED

How would you describe your experience with developing a certification scheme?

If we are still talking about these two parallel scenarios with people from public and private domains – I can say that the most difficult part when developing a certification scheme was to manage their (often conflicted) interests (because they come from two different worlds), coordinate them, align them, and reach a common agreement. To reach a common agreement – all personal interests, industrial interests, and social interests must be aligned.

Can you list up to 3 lessons learned from developing a certification scheme?

For instance, at the European level, we have the GDRP, a regulation implemented by Member States. At the very beginning, there were some discrepancies about implementing the GDPR because most Member States already had something else implemented. The question was if the GDPR was needed, but even at that moment, Member States needed to get together with the Commission and reach an agreement, because there was still a clear need to agree on (at least) a minimum set of requirements. So, **the first lesson learned** might be that if there is not a clear need for developing a (public or private) certification scheme, it will take some time to develop a certification scheme. You need a clear need to engage a whole ecosystem, motivate different stakeholders to get the support you need and eventually succeed at developing a certification scheme.

Another lesson learned might be related to the lack of knowledge about the environment (ecosystem). Manufacturers do not know what it means to be an accreditation body, a certification body, or even a test laboratory – what are these entities supposed to do, in which order and under which conditions? For instance, they do not understand that a laboratory must work together with a certification body, and they must follow some guidelines, some requirements, or else they may face serious obstacles. Also, in reverse,

accreditation bodies, certification bodies, and test laboratories do not understand the environmental and societal conditions of private and public organisations. For example, they do not understand the reasons why, suddenly, a small company wants to have its products certified. It is usually because they are required to do so. So, **the second lesson learned** might be the magnitude or sensitivity to understanding that a company could cease to exist if they do not reach a certain market or, understand that as a testing laboratory, we cannot issue a certificate, since we are not a certification body. These things that look very simple are sometimes crucial when enabling access to the market. We, as a lab, are not asking you to fulfil these requirements because we want you to waste your time. We are asking you to fulfil these requirements because we are required to do so. Sometimes, despite this lack of understanding or lack of empathy, the process runs well, but sometimes, something that normally takes up to five months could last over two years.

We are currently developing a certification scheme with the public entity and let's say we can support 300 manufacturers (a total of 120 hours providing the service). So, what are we going to do with them? If we launch a certification scheme, it will take a lot of effort by them to align with new requirements. How can we get them on board? So, this is **the third lesson learned**. We must think not only about the fulfilment of the requirements but also about state-of-the-art. We must gain momentum because although we are convinced that with certification, we are providing strong differentiation value if we don't manage it properly, it could be a waste of time and companies and organisations will not benefit from certification as much as they could.

Do you have any other advice for R&D projects that want to develop a certification scheme?

Vendors need to understand that they have to set priorities and develop a strategy when addressing the need to certify a product. If they choose not to do so, they would achieve merely a mid-term visibility of that product because they were feeling obligated to eventually get that product certified. New regulations on health, safety, gas, oil, electricity, or cybersecurity are constantly being developed, so they will eventually have to get that product certified. What can happen is that a single company may have to acquire two or three certificates. When it comes to R&D projects, as well, they must acquire this mindset, this approach to standardisation as part of the roadmap. They must include it in the roadmap, not only as the acquisition of the technology or the consultancy. They must acknowledge that somewhere down the path, they will have to address this topic.

It might be said that about 90% of today's products are managed (at least to some extent) with ICTs. We mentioned the GDPR, but what nobody understands is that all products with a technology base will manage and store data. For instance, I could be a software developer and to be able to certify my products, I must include some data protection features or functionalities in them. The sooner I do that, the sooner I will understand that, as a manufacturer, I need the software. So, if I'm not responsible for this software, I will have to demand my software suppliers to provide me with certified software, because it's not a matter of making my life easier, it's a matter of providing my customer with a reliable, consistent, and competitive product, otherwise, we are all offering (more or less) the same products (services), and this is very important part.

A part of a typical R&D project is to take into consideration, even at a draft proposal stage, the state of the art. If you are going to bring a research outcome, you need to start somewhere, and the state of the art is

this starting point. In this stage, they must at least consider standardisation. So, once they are aware of the current standardisation level, they can decide whether to push more or maybe it's not sufficient so they may have to decide to not go ahead with the product development. If they are certain that they are bringing something new, something relevant and something valuable – they may have to add standardisation considerations to product marketing assessment or address them within their current technology roadmaps, sales strategies, or even business models. So, I am not saying that this is not a moment to think about the possibility of developing a certification scheme, but maybe it is too early to do so. Instead, they must at least become aware of these aspects – the state of the art, technology, standards, whether there is an existing certification scheme or not, and if it could affect technology roadmaps, sales strategies, business models, etc. These are the aspects they could consider from the very beginning because if there is an existing certification scheme, it may help them access the market. Otherwise, they will come to address these aspects once they have developed a product.

2.5 FUTURE EXPECTATIONS & IMPACT ASSESSMENT

What are your expectations? How would certification schemes and systems evolve in the future?

I strongly believe in certification progress. I already mentioned that certification is a strong value in itself. Actually, standardisation, certification, and accreditation – these are the three pillars of quality. Nowadays, more and more companies are starting to see the benefits of their products being certified. All relevant players are already working (for quite some time now) on developing certification schemes. For example, each time you open your laptop, you must know that it has been certified. Although, what comes to your laptop usually is not (but companies are also trying to prevent these casualties). Additionally, a couple of years ago, the Commission put in place the Cybersecurity Act which covers a range of certification schemes for different sectors. Speaking about the ICTs and the software industry, we have the EU Cloud Act for cloud computing services and systems, we also have schemes for 5G, IoT, etc. Also, a new scheme for Artificial Intelligence (AI) has recently been discussed, and the GDPR (which is somewhere in between) has also been strengthened with another one – the Cyber Resilience Act which provides strong recommendations on how to include security features in the design stage and provide more reliable products. I believe that in the future, we will witness more vertical certification schemes, such as cybersecurity which applies to different sectors, complementing other schemes more related to these sectors (e.g., cybersecurity in the healthcare, automotive, space industry, etc.). So, it's only a matter of time to see how European actors will benefit from these certification schemes.

Can you describe the impact developing a certification scheme can have on European actors or maybe internationally?

Normally, certification schemes are dedicated to establishing technical and even organisational sets of requirements that we have been discussing. These requirements must be fulfilled by the industry and also

must be assessed by a third independent party. So, the main impact would be on society, thus enabling customers to access trustworthy products and services. There is an old saying ''made in Germany'', meaning that e.g., cars and domestic devices made in Germany are fully reliable because they are based on high-quality standards. This must also be expanded to the digital world because most of the things we know today are created with digital design. So, we must be aware of all these aspects to speak about the impact, and speaking about European actors, the impact is twofold. First, Europe needs to enhance the competitiveness of its industry (and different sectors). Although we are quite competitive when it comes to providing quality products, we also depend on other parts of the world to complement our products (e.g., semiconductors). So, we need to boost this strong side. We need more competitive industries and certification schemes can contribute significantly to making our industries more competitive, not only at the European or regional but also at the international level(s). Second, and the second one is the consequence of the first one, we need to strengthen our skills and capabilities to be able to compete and collaborate, not only with European actors but also globally. We are currently competing and collaborating with the USA, Canada, and Central and South America, as well as, Eastern countries, such as South Korea, Taiwan, Malaysia, and even China, and certification schemes can contribute significantly to strengthening our roles and responsibilities in these markets.

SUMMARY

While each conformity assessment activity should be treated differently, there are several proven advantages of using a systemic approach and the concepts of conformity assessment schemes and systems. [64] While **a conformity assessment scheme** usually describes ''a particular group of objects having sufficiently similar characteristics that the same set of rules and procedures can be carried out under the same management for assessing conformity with the same set of specified requirements''**, a conformity assessment system** ''uses a common set of rules, procedures or management for several conformity assessment schemes''. [65] Although ''rules and procedures may need to be detailed in different ways for different schemes'', there are several proven advantages in terms of ''efficiency and consistency to working within a common framework''. [66]

The **ISO/IEC 17000, Conformity Assessment – Vocabulary and General Principles** gives the definitions of these terms. According to the ISO/IEC 17000 **– a conformity assessment scheme** (which is sometimes referred to as a conformity assessment programme) is defined as ''a set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment'' whereas **a conformity assessment system** is defined as ''a set of rules and procedures for the management of similar or related conformity assessment schemes''. [67]

While a conformity assessment scheme can be managed within a conformity assessment system, both schemes and systems can be operated at an international, regional, national, sub-national, or industry level. [68] Which type of scheme or system would be the most appropriate under the given circumstances depends on several factors, such as the codes of conduct of the certification body, the complexity of the industry or the sector, etc. [69] Although some certificates may last for a limited period (e.g., 1 to 3 years), most of them have no time limit. [70] As long as the certified organisation regularly pays the annual fees and surveillance audits do not reveal major non-conformities that are not dealt with promptly, all the issued certificate remains valid. [71]

---

[64] ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf, pp. 81.
[65] Ibid.
[66] Ibid.
[67] ISO/IEC. (2020). ISO/IEC 17000, Conformity assessment – Vocabulary and general principles. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en.
[68] Ibid.
[69] Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit). Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf, pp. 118.
[70] Ibid.
[71] Ibid.

GLOSSARY

conformity assessment scheme

''a set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment'' [72]

conformity assessment system

''a set of rules and procedures for the management of similar or related conformity assessment schemes''. [73]

[72] ISO/IEC. (2020). ISO/IEC 17000, Conformity assessment – Vocabulary and general principles. Accessed on October 12, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en.
[73] Ibid.

BIBLIOGRAPHY

ISO. (2019). How to develop scheme documents: Guidance for ISO technical committees. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100439.pdf

ISO/IEC. (2020). ISO/IEC 17000, Conformity assessment – Vocabulary and general principles. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en

ISO/IEC. (2009). ISO/IEC 17007, Conformity Assessment – Guidance for drafting normative documents. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/standard/42635.html

ISO/IEC. (2017). ISO/IEC 17011, Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies. Retrieved from: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:17011:ed-2:v1:en

ISO/IEC. (2012). ISO/IEC 17024:2012 Conformity assessment — General requirements for bodies operating certification of persons. Retrieved from https://www.iso.org/standard/52993.html.

ISO/IEC. (2014). ISO/IEC TS 17027:2014 Conformity assessment — Vocabulary related to competence of persons used for certification of persons. Retrieved from: https://www.iso.org/standard/62024.html.

ISO/IEC. (2013). ISO/IEC 17067. Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes. Accessed on June 05, 2023. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17067:ed-1:v1:en:term:3.2

ISO/UNIDO. (2022). Building trust. The Conformity Assessment Toolbox. Accessed on October 27, 2022. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf

Kellerman, M. (2019). Ensuring Quality to Gain Access to Global Markets (A Reform Toolkit). Accessed on October 27, 2022. Retrieved from: https://thedocs.worldbank.org/en/doc/249621553265195570-0090022019/original/FullQIToolkitReport.pdf

HSbooster.eu
Horizon Standardisation Booster

Follow us

Website
hsbooster.eu

Twitter
@HSboosterEU

LinkedIn
HSbooster.eu

YouTube
HSboosterEU

Funded by
the European Union