SWIPO Review of Approaches to Certification Schemes version 0.9

Introduction

Due to the Free Flow of Non-Personal Data Regulation (EU) 2018/1807 (further referred to as “the Regulation”), and specifically Article 6.1(c), the SWIPO Working Group has been asked to identify:

> “approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, *inter alia*, quality management, information security management, business continuity management and environmental management.”

SWIPO appointed a special Task Force to identify and describe such “approaches to certification”. The Task Force has decided to look at this matter from a high level due to the wording of the given section from the Regulation, the significant numbers and categories of standards that could apply to cloud services offerings, and the complexity of conformity assessment issues more generally.

This paper is not intended to promote, initiate, develop and/or maintain any certification scheme for switching and porting between cloud providers and their customers or adjacent certification activities. Among other things, this means that specific certification schemes generally will not be identified and the accuracy and completeness of the information provided is subject to this document’s disclaimer notice.

1. Certification Generally

As a preliminary matter, it is important to note that companies adopt many different types of "standards" addressing a broad range of issues in most of their products. Generally companies use these standards to address a range of business or customer needs without any related conformance assessment or certification.

There may be specific reasons for a company to undergo a conformance assessment for a product or service in whole or in part against a standard. An associated certification is normally done as a means of advertising or demonstrating the conformance to customers and the marketplace generally. Conformity assessment, and associated certification, generally can take one of three forms:

- First-party (also referred to as "self-declaration" or "self certification" where the company itself undertakes this assessment),[1]
- Second-party (where the conformance to a standard is assessed by a person or organization that has a user interest in the product or service) and
- Third-party (where assessment is performed by an independent third-party organization and which is described in greater detail below).

As noted above, there are different certification approaches that can be applied if there is a perceived need (usually customer sensitivity or widespread customer demand) in connection with a given standard. When this happens, industry players generally will offer a "first-party" supplier's self-declaration of conformance. This then becomes part of the supplier's "market offering" and generally creates certain related legal obligations. Depending on the customer's own risks and desired risk mitigation approach, the customer may seek a further enhancement (at additional costs) to the supplier's declaration, such as a type of contractually-based audit. A supplier's declaration generally is the overall preferred certification/conformity assessment approach because it is the most readily adaptable and lowest cost option minimizing the costs for all parties. In addition, it eliminates the risk of discrimination based on the geographic validity of the second or third party certification or the need to negotiate political agreements on the mutual recognition of certification results on a cross-border basis.

In order to minimize customer costs and maximize innovation, certification generally is most effective when it is customer-led and risk-based. Certification (and conformity assessment approaches more generally) is always based on a specified set of requirements. These requirements usually are set forth in a broadly recognized and deployed (voluntary) standard that was developed pursuant to a documented, open, fair and consensus-based governance

[1] While some people and organizations use the term "certification" in connection with self-declaration of conformance (*see, e.g.*, Privacy Shield Framework at https://www.privacyshield.gov/article?id=Self-Certification-Information, others believe that the term should only be used in connection with second-party or third-party certifications.

process. Such requirements act to transfer best practices and that generally is the primary value of the standard.

In some situations where there are common issues across the market and further certification can be justified based on the need to achieve market trust in a specific context (usually related to health, safety, environmental or security issues), certification may be conducted by third-party certification bodies. The EU Cybersecurity Act (effective on 27 June 2019), introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU may benefit from having to obtain certifications for their ICT products, processes and services - only once - and see their certificates recognised across the European Union. This new framework is anticipated to play a critical role in increasing trust and security in services that are crucial for the Digital Single Market. At the moment, a number of different security certification schemes exist in the EU.

This type of third-party certification generally is based on an external audit that is conducted by a qualified certification body that itself has been found to satisfy a prescribed set of internationally-established and detailed criteria for auditing competency, practices, independence, record-keeping, etc. There may be other considerations that must be addressed to have such formal certifications be accepted in different geographical regions. In addition, if third-party certification is taken up as a market requirement, then it becomes a cost barrier to market entry and possibly particularly burdensome for smaller players, niche or innovative market offerings.

Such formal third-party certification approaches typically are supported by an extensive framework of certifiers, accreditors of certifiers, and auditors that must each meet separate requirements in order to avoid conflicts of interest and other similar concerns. For example, ISO/IEC 17011:2004 (https://www.iso.org/standard/29332.html) specifies general requirements for accreditation bodies assessing and accrediting conformity assessment bodies (CABs), ISO/IEC 17065:2012 sets forth requirements for the competence, consistent operation and impartiality of product, process and service certification bodies, and ISO/IEC 17067:2013 describes the fundamentals of product certification and provides guidelines for understanding, developing, operating or maintaining certification schemes for products, processes and services.

This accreditation/certification/audit framework results in an additional layer of costs in order to ensure that such accreditors/certifiers/auditors are themselves trustworthy, and that the resulting certifications are “equivalent” and can provide a reasonable basis for comparison. There is yet another layer of cost in that the accreditors and certifiers often seek ways to work together to ensure comparable outcomes (such as through the International Accreditation Forum).

While third-party certification may be appropriate in the context of certain heath, environment or security-related issues, it also is important to remember that Europe has adopted the EU Single Market Strategy which is focused on leveraging the use of voluntary, “harmonized standards to demonstrate that products, services, or processes comply with relevant EU legislation.” Very often it is anticipated that providers can leverage tools such as the CE

mark which is a very good example of “first party certification”. A manufacturer can affix the mark to its products as a means of self-attesting that the product meets all related requirements.

The SWIPO Task Force, looking at “Approaches to Certification Schemes”, identified that there is a broad range of categories and a significant number of possible voluntary standards that may be implemented in connection with a cloud services commercial offering. Similarly, there are a variety of ways that conformance or compliance with any such standard can be assessed. Most often cloud service providers make their own assessments or determinations in this regard. As with the proposed SWIPO Codes of Conduct, such assessments may be accompanied by related public statements. As noted above, generally more formal frameworks are only used when there is a compelling public interest need and/or significant customer demand.

2. Voluntary Standards That May Apply to Cloud Services

The SWIPO Task Force looking at “Approaches to Certification Schemes” identified that there is a broad range and significant number of possible standards in diverse categories that may be implemented in connection with a cloud services commercial offering. Similarly, as noted further above, there are a variety of ways that conformance or compliance with any such standard can be assessed. Most often companies make their own assessments or determinations in this regard. As with the proposed SWIPO Codes of Conduct, such assessments may be accompanied by a related public statement to the effect that the provider complies with a specific standard or Code. Generally, and as noted above, any framework for assessing conformance to a standard is used when there is a compelling public interest need and/or significant customer demand.

While many accredited certification schemes are described and standardized by international standardization bodies such as ISO/IEC (as recognized developers of International Standards with diverse stakeholders participating through national body members), other schemes (such as commercial industry initiatives) can be considered as well.

Next to the above accepted international standards, self-certification and a number of other approaches can be considered like the ISAE 3402 standard. The ISAE (International Standard for Assurance Engagements) has issued ISAE 3402 called “Assurance Reports on Controls at a Service Organization” for voluntary use by public accountants and is risk-based. The official title of ISAE 3402 is "Assurance Reports on Controls at a Service Organization". The approach is always from a financial reporting perspective; for all other non-financial purposes one would use the guidelines contained in an ISAE 3000 standard for assurance. ISAE 3402 is a third party (mainly suppliers) assurance mechanism in the form of SOC (Service Organisation Controls) reports. Within the SOC reports there is a differentiation in two different approaches: The SOC1 report relates to assurance on controls that could impact financial statements, and the SOC2 report relates to assurance on IT controls.

The focus of the free flow of non-personal data Regulation is to facilitate the porting of non-personal data and support the ability for a customer to switch cloud service provider (CSP) and port such data from one CSP to another. In this context, it is important to note that cloud services offerings are software-based. As such, they are highly diverse and difficult to compare. A key aspect of any effort to compare cloud services is to have common terms, core concepts and architecture, and there are a range of ISO/IEC International Standards (*e.g.*, ISO/IEC 17788, 17789, 19941, 19944, 22123 and 22624) that can help enable portability and switching decision-making.

The Regulation further notes that there may be a number of other recognized standards and certification schemes that may help when comparing cloud services offerings. Such schemes may be available in the following general categories:

1. Management Systems Standards
2. Interoperability and Portability
3. Information Security Management
4. Quality Management
5. Risk Management
6. Environmental Management

3. Management Systems Standards

Any organization that voluntarily decides to implement a certain standard and undertake a related conformity assessment approach (either directly or through a third-party) will have to establish that the organization conforms to any mandatory elements within that management system standard. Different standards and related conformance/certification schemes may be based on a unified set of management system principles to facilitate both implementation and assessment. To the extent that a set of management systems standards are developed under the same umbrella (such as ISO/IEC), they tend to share common elements.

There are a number of current management systems standards and conformity assessment options that are available and may be relevant in the area of cloud services. These cover topics such as: information security management, quality management and environmental management.

4. Information Security Management and Cybersecurity Schemes

4.1 The European Cybersecurity Certification Framework under EU Cybersecurity Act

With the new Cybersecurity Act, the European Union is aiming at increasing trust and security in cloud services to ultimately increase the deployment of cloud computing in Europe. According to the European Commission, the high number of different cybersecurity certification schemes existing across Europe represents an obstacle for European businesses to move to the cloud. Against this backdrop, the Cybersecurity Act is trying to address the risk of fragmentation and barriers in the European Single Market by creating a common framework for EU cybersecurity certificates.

The Framework should help reduce such market-entry barriers for SMEs and new businesses because companies will have to undergo the certification process of their products or services only once and the corresponding certificate will be valid across the EU.

4.2 CSPCERT WG Recommendations for the Implementation of an European-wide CSP Certification Scheme

A self-regulatory working group (CSP CERT WG) together with the expert assistance of representatives of national cybersecurity certification authorities was tasked in 2017 by the European Commission to study and propose a new EU wide recognised cloud security certification framework to support the Digital Single Market strategy.

The CSP CERT WG used a taxonomy derived from studies by Tecnalia (commissioned by the European Commission)[2] to map and to merge controls from existing standards and certifications in a few consistent security domains. This includes SecNumCloud from ANSSI, C5 from BSI, and ISO/IEC 27001/2, 27017, and 27018.

A final proposal was presented to the Commission by the CSP CERT WG on 12 June 2019. The proposed recommendations is ISO-, Assurance- and Evidenced-based. The proposal is divided into three categories that map to the articles of the EUCA: CCAL (Cloud Computing Assurance Level); CSAR (Cybersecurity Act Requirements) and SGOV (Scheme Governance).

The CSPCERT report suggests that it is possible to establish a cloud certification scheme that can underpin equivalent security requirements throughout Europe. The report may be used among other inputs as a basis for ENISA to prepare a new EU cloud scheme under the Cybersecurity Act.

The Cybersecurity Act states that the new certification schemes will be voluntary and not mandatory.

4.3 ISO 27001 and ISO 27002

ISO/IEC 27001 and 27002 are voluntary standards that set forth requirements that are intended to help companies effectively manage their overall set of information security controls. For example, ISO/IEC 27001 sets forth parameters for companies' management to (a) systematically review and address the company's information security risks (looking at vulnerabilities, threats and related implications), (b) ensure that the companies' information security controls are clear and complete, (c) assess whether other risk avoidance

[2] https://op.europa.eu/en/publication-detail/-/publication/6a83608d-0fdb-11e9-81b4-01aa75ed71a1

mechanisms may be needed, and (d) ensure that the overall management process adequately provides for the information security controls to be updated on an ongoing basis. ISO/IEC 27002 sets forth guidelines for a company's information security standards and practices. This includes the selection, implementation and management of the company's controls. ISO/IEC 27017 further expands these guidelines for cloud services.

5. Quality Management

Quality Management in general focuses on ensuring the consistency of business practices while framing processes for (a) the ongoing improvement of the company's systems and (b) conformance to applicable statutory and regulatory requirements. All of this in turn can help enhance customer satisfaction stemming from the company's effective management of the consistency and quality of the company's processes. To ensure continual improvement, many organizations voluntarily define their goals with Key Performance Indicators (KPI's), monitor the results, and find ways to improve customer satisfaction, effectiveness and efficiency in the business processes used to deliver their services and/or products.

There are two basic elements that often are mentioned in connection with standards related to the consistency of business practices: Quality Management Systems (QMS) and Total Quality Management (TQM). As reflected in related, voluntary standards, both generally follow different paths and target different elements:

- Quality Management System (QMS) are the tools and processes that an organization defines in order to achieve consistency and therefore the consistent quality in their overall deliveries. This includes both quality assurance (reviews) activities and quality control (evaluation or testing) activities.

- Total Quality Management (TQM) is a set of steps that companies follow in order to help the company target the cause of defects and institute appropriate corrective measures.

Quality Management may be a type of a specific business process for a specific sector (such as maritime, agricultural and education), but generally such processes are all based on the voluntary International Standard that has been created and maintained by the International Organization for Standardization (ISO). See for reference material: https://www.iso.org/iso-9001-quality-management.html.

While not standards-based, the non-profit association "European Foundation for Quality Management" (EFQM) helps organizations and their stakeholders to "improve the performance of organizations and their ability to manage change and transformation". The EFQM developed a model that organizations may adopt to improve quality: https://www.efqm.org/

6. Business Continuity

ISO 22301 is a voluntary International Standard that sets forth requirements for a business continuity management system that also can be applied to all companies. It focuses on what companies may want to do to plan, establish, implement, operate, monitor, review, maintain and continually improve a management system that is focused on preparing for, responding to and protecting against “disruptive incidents” when they arise. Among other things, in this context it addresses leadership, planning, support, operation and performance evaluation.

Reference material: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en

7. Environmental management

Environmental management is a complex area in cloud service provision owing to the intended nature of cloud to separate user-based issues from basic ICT components. This is therefore normally addressed in a top down approach by the use of environmental management systems approaches, as most commonly expressed in the ISO 14000 series of standards supported by an extensive network of certification providers.

Overall this starts by setting an environmental policy, identifies accountability within the organisation, identifies the actual and potential environmental impacts and establishes objectives target and other programmes. This is then coordinated with compliance and reporting actions. One example is the Green House Gas Protocol Corporate Accounting and Reporting Standard. This then leads to a monitoring and measurement process combined with a review building into a complete continuous improvement process.

There are, however, a few key issues to note.

Although environmental management is part of and complementary to both quality management and risk management, its relationship to corporate accounting means it is complementary to standards that come from the world of corporate accounting and reporting (e.g., the GHG Protocol) and is an area covered by both regulations and regulatory bodies beyond the scope of this paper. There are also various voluntary and compulsory schemes reporting on energy consumption that differ around the world in their requirements. However corporate accounting and international reporting have largely harmonised the critical top level and allow a top-down approach.

Unlike other areas presented here, however, it is important to note that some of the primary issues may well lie with the usage profiles of the end customer. For example, minimising lag in a widespread organisation implies that multiple storage systems are continuously synchronised. On the other hand, a simple single data access requirement with periodic back-up would have a completely different consumption profile despite both being able to run on identical IaaS provisions. The impact of the main components of any cloud services -

- compute, storage and networking combined with supporting infrastructure - - would be fundamentally different in each case. Hence the prioritisation of a top-down management approach to avoid focusing on individual components or subcontracted services which can be deeply misleading and divert resources from those areas is what actually may make a difference.

It is further complicated by the range of potential models and dependencies. For example a SaaS provider may be operating purely as a virtual SaaS by utilising IaaS and network services. The impact of data transfers is again often complicated by routing dependencies and base loads of networking components.

Although many of these areas are supported by localised engineering tools and metrics, many of which are standardised themselves including, but not limited to energy management systems (ISO 50000 series), data centre metrics including Key Performance Indicators, Power Usage Effectiveness and Renewable Energy Factors (ISO/IEC 30000 series) as well as techniques such as life cycle assessment (ISO 14040 and its sector based variants). The networking elements are normally handled again and for similar reasons by their providers' own use of the ISO 14000 series.

Potentially relevant European standardisation and input into ISO/IEC is being coordinated through the CEN/CENELEC/ETSI Coordination Group Green Data Centres (CG GDC). International standardization activities in this area take place under ISO/IEC JTC 1/Standard Committee 39 and ITU-T Study Group 5. The EN 50600 and ETSI EN 305 series of standards have become the European reference for resource efficient design and operation of data centres.

ETSI identifies some key energy efficiency objectives inside the data center that include energy consumption, task efficiency, energy reuse and renewable energy which again may have , to varying degrees, potential impact on the performance of the overall system. The following specs - ETSI TS 105 174-2-2 V1.1.1 (2009-10), ETSI ES 205 200-2-1 V1.2.1 (2014-03) and ETSI GS OEU 012 V1.1.1 (2015-10) (operational efficiency), review the related considerations and key performance indicators (KPIs) such as - Energy Consumption (KPI_{EC}), Task efficiency (KPI_{TE}), Energy reuse (KPI_{REUSE}), Use of renewable energy (KPI_{REN}) to measure and monitor those energy efficiency objectives.
https://www.etsi.org/deliver/etsi_ts/105100_105199/1051740202/01.01.01_60/ts_1051740202v010101p.pdf
https://www.etsi.org/deliver/etsi_es/205200_205299/2052000201/01.02.01_60/es_2052000201v010201p.pdf
https://www.etsi.org/deliver/etsi_gs/OEU/001_099/012/01.01.01_60/gs_OEU012v010101p.pdf.

Additionally, there have been several documented best practices through documents such as 2018 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency (https://ec.europa.eu/jrc/en/publication/2018-best-practice-guidelines-eu-code-conduct-data-centre-energy-efficiency-version-910).

To summarise, CSPs offer complex services that must be optimised at the system level, which may be at the CSC level in some configurations and is covered by accounting standards as much as technical standards. Components, while important, form a varying part of the whole.

8. Privacy Management

Privacy relates to a person's right to determine and control the processing of their personal data. Personal data means any data that directly or indirectly identifies a natural person. In Europe, legitimate processing of personal data is principally governed by the GDPR. Privacy management is the set of controls that both data controllers and processors must put in place to adequately protect personal data and to manage the legitimate processing of personal data.

Article 40 of the GDPR encourages the development of codes of conduct which address the lawful processing of personal data under the GDPR. Codes of conduct that are approved by EU Member State Data Protection Authorities with or without consulting the European Data Protection Board (EDPB) have certain benefits for organizations that implement them – e.g. easier proof of compliance. They also can serve as a demonstration of appropriate technical and organisational measures under Art. 28.5 for data processors or as a factor for consideration e.g. when determining administrative fines by supervisory authorities or when performing a data protection impact assessment.

Currently, no code of conduct for cloud computing has been officially approved, though there are three voluntary industry driven codes in existence:

1. EU Cloud Code of Conduct
2. CSA Code of conduct for GDPR Compliance
3. CISPE Code of Conduct

The benefits of codes of conduct can also be obtained using certifications pursuant to Art. 42 of GDPR. No certification scheme has been approved so far.

There are international standards that provide controls and mechanisms that can be used as a basis for GDPR related technical and organizational measures, including security-related issues:

1. ISO/IEC 27018 "Information technology – Security techniques – Code of Practice for protection of personally identifiable information (PII) in public clouds acting as PII processors". The standard is a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for organizations for implementing commonly accepted PII protection controls.
2. ISO/IEC 27701 "Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management — Requirements and guidelines". This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS)

in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002.
A certification scheme against this standard is being developed.