Towards a Process Assessment Model for Management System Standards

Stéphane Cortina, Nicolas Mayer, Alain Renault, Béatrix Barafort
Public Research Centre Henri Tudor, Luxembourg
{stephane.cortina; nicolas.mayer; alain.renault; beatrix.barafort}@tudor.lu

Abstract. Certification to management system standards is more and more attractive for organisations, and many companies are today certified according to several of them (e.g., ISO 9001, ISO 14001, ISO/IEC 27001, etc.). However, in this case, it is a remaining challenge to optimise the system in place by mutualising as much as possible the different processes required by the various management systems, and thus improving the integrated overall system. In order to fill this gap, this paper presents how a process assessment model for management system standards has been built. It is based on the High Level Structure proposed by ISO, which defines a set of common requirements for management system standards. This process assessment model will provide the core content and could be the basis of all the future process assessment models that will be developed to assess domain-specific management systems.

Keywords: process assessment, process assessment model, management system standard, management systems, integrated management system

1 Introduction

Every year, ISO (International Organization for Standardization) performs a survey [1] of certifications to Management System Standards (MSS). The 2012 results reveal that ISO 9001 (which gives the requirements for quality management systems) has generated more than 1.1 million of certificates in 184 countries since 1993. This survey also indicates an increase between 9 and 20% of the certificates related to emerging MSS such as ISO 14001 (Requirements for environmental management systems), ISO/IEC 27001 (Requirements for information security management systems), or ISO 22000 (Requirements for food safety management systems).

Regarding this growing interest about management systems and the penetration in the market of associated certifications, ISO has published in 2012 (and revised in 2014), as part of its Directives, an annex entitled "High-level structure, identical core text, common terms and core definitions" for MSS [2]. This High Level Structure (HLS) aims at ensuring consistency among future and revised MSS, and aims at making their integrated use easier. Indeed, many companies need to implement several management systems covering complementary domains (information security, service management, quality, etc...). The challenge is then to reduce the workload by sharing processes across the different management systems.

Implementing and assessing the capability of the processes composing such integrated management systems are both emerging challenges. In this paper, our focus

is on the process assessment activity and the purpose of this paper is to present how we have built a process assessment model for MSS (compliant with the requirement of the ISO/IEC 33000 series of standards for process assessment [3], [4], [5], [12]). This process assessment model will provide the core content and could be the basis of all the future process assessment models that will be developed to assess domain-specific management systems. The purpose of such a model is also to be used as a tool for assessing the capability of the processes that are common to any management system.

Section 2 presents the background of our research project and states its objectives. Section 3 describes our research method and the different steps followed to build the core content of a process assessment model for MSS. Then, in Section 4, the resulting core content is presented. Section 5 analyses our approach and its results by discussing the different strengths and weaknesses of the model and its building process. Finally, Section 6 concludes about the current state of the process assessment model for MSS and presents our future work.

2 Problem statement

On the one hand, management systems are implemented by companies under the form of a management system dedicated to a specific domain, or more and more often under the form of an integrated management system targeting several domains (such as business continuity, information security, and/or service management). This kind of integrated management system results in different processes that are common to and shared between several domains. It is indeed relevant to have for example only one management review process shared across these different domains. This enables taking optimal decisions during management review meetings based on the needs, the requirements and the priorities of the different management systems. Since 2012 and the first publication of the HLS, there is a robust description of the processes that are common to all management systems. First of all, the HLS is used to revise the existing MSS at the ISO level. All of the MSS shall now be compliant with the HLS structure. Furthermore, the HLS can be used by companies to establish their integrated management system. The HLS provides the description of what processes can easily be shared among the domain-specific MSS.

On the other hand, there is a growing community of consultants using process assessment methods to support the implementation, improvement, and integration of management systems. The ISO/IEC 33000 series is a well-established series of standards for describing processes and assessing process capabilities. It also introduces its own terminology such as "*process assessment model*", "*process reference model*", "*purpose*" or "*outcome"* that is not further developed in this paper. However, the reader can refer to ISO/IEC 33001 [3] for terms and definitions and more generally to the whole ISO/IEC 33000 series for an exhaustive explanation about the approach. A key element of the approach, explained in ISO/IEC 33002 [4], is that an assessment shall be performed based on compliant process assessment models, as defined in ISO/IEC 33004 [6].

Consequently, there is an emerging need for a process assessment model describing the common processes of MSS as described in the HLS, and meeting the requirements of ISO/IEC 33004 [5]. Such a process assessment model will be used to perform standardized assessments of the capability of processes now required for composing any integrated management system. The objective of this paper is to present a process assessment model for common processes of MSS, and the main focus of the paper is on how to build it according to a structured and reliable approach.

3 Method

This section describes how the authors have developed a process reference and then a process assessment model for MSS compliant with the HLS. The first step was the selection of a set of key criteria that were taken into account during the development process. These criteria are detailed in 3.1. Then, as explained in 3.2, the authors applied the transformation process described in [6] to the requirements contained in the HLS in order to build the process assessment model for MSS.

3.1 Key criteria

The following criteria have been used by the authors, all along the transformation process, to guide design choices. These criteria have been chosen on the basis of the experience of the authors in order to guarantee that the resulting process assessment model will be efficient whatever the domain assessed.

Assessability:
The main objective of a process assessment model is to be used to perform process assessments. For that each process has been described in a way that facilitates its future assessment. Particularly, the process model has been designed so that:
- each process has one single purpose
- the process outcomes are necessary and sufficient to achieve the process purpose
- each process outcome is defined as a measurable objective
- the base practices reflect the process purpose and outcomes

Interoperability:
The expected process assessment model needs to support interoperability between management systems. For that the produced model describes processes and work products in a way that fosters the exchanges between several management systems.

Integration:
The expected process assessment model needs to facilitate the integration of multiple management systems. For that the produced process assessment model only describes the common/generic part of any management system. Thus it focuses on the core content of an integrated management system covering several domains.

Completeness:
The expected process assessment model needs to address each requirement contained in the HLS. For that the traceability between the HLS and the process base practices (contained in the produced process assessment model) has been assured.

Adoption:
The produced process assessment model needs to describe the common processes of MSS in a way that encourages the adoption of these processes. For that the proposed processes have been designed in a way that reflects the processes that are usually implemented in most companies. Moreover, the proposed process descriptions were worded using terms, base practices and work products that can be easily understood and that are as close as possible to those used in MSS.

Applicability:
The proposed process assessment model needs to fit in with all companies, regardless of their type, size, or nature. It needs to be usable for various purposes such as: the rating of an individual process, the determination of the organizational maturity, the preparation for audit, or benchmarking. For that the produced process model has been designed in a way that ensures its compliance with all the requirements of ISO/IEC 33004 [5].

3.2 The transformation process

The transformation process described in [6] has been used by the authors of this paper to design and build a process assessment model for MSS compliant with the requirements of ISO/IEC 33004. Based on goal-driven requirements engineering techniques [7], this transformation process has already been used successfully to build process models in various domains [8], [9], [10].

Using this transformation process, the collection of requirements contained in the HLS are first transformed into requirements trees, then into goal trees, and finally into a process reference model and a process assessment model, as illustrated in Figure 1.

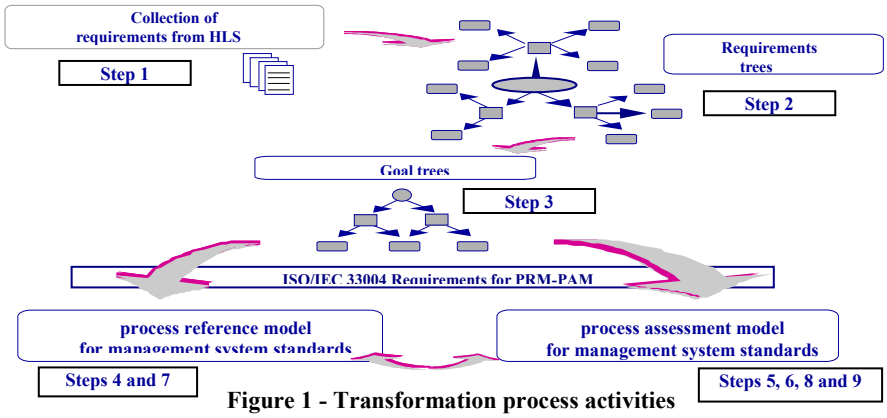

Figure 1 - Transformation process activities

The transformation process consists in 9 steps described in details in [6] and summarized below:

Step 1 – Identify elementary requirements in a collection of requirements

This step consists in identifying all of the requirements under the form of a collection of elementary requirements. In our case, the 'shall statements' (revealing requirements) contained in the proposed text of the HLS [2] were easily identified and split into elementary requirements. The final list was composed of more than one hundred elementary requirements made up of a subject, a verb and a complement, without coordination, conjunctions, or enumeration.

Step 2 – Organize, and structure the requirements

Then, the elementary requirements were organized and structured. For that, a 'mind map' helped to have a graphical view of the elementary requirements having the same object (or component). The requirements were then gathered around the objects they were relating to in order to build a requirements tree.

Step 3 – Identify common purposes upon those requirements and organize them

An internal task force composed of experts in process assessment and/or domain-specific management system (service management, quality management, information security management, and electronic records management) was then set up. The task force identified common purposes for the groups of requirements and organised them accordingly, taking the original meaning of the text proposed in the HLS into account. A goal tree was then built for each process (an example can be seen in Figure 2). On these goal trees, each low-level objective is linked to an elementary requirement of the HLS (and all requirements are linked to a low-level objective of a goal-tree). Thus, thanks to these goal trees, the task force carefully grouped inter-related activities, keeping in mind the key criteria (see Section 3.1), and particularly that the main objective was to create easily assessable processes. This semantic work enabled to outline the structure of the process reference model and particularly to identify its processes.

Step 4 – Identify and factorize outcomes from the common purposes and attach them to the related goals

The common purposes identified during step 3 of the transformation process can be considered as the observable results of something (i.e. the production of an artefact, or a significant change of state, or the meeting of specified constraints). These observable results are named 'outcomes' and are attached to the related purposes. Depending on the size of the goal tree, and in order to have from 3 to 7 outcomes per process, (as recommended by the ISO/IEC TR 24774 [11]) it was sometimes necessary to factorize and merge some of these outcomes.

Step 5 – Group activities together under a practice and attach it to the related outcomes

The original input of the transformation process (the requirements from the HLS) contains information describing activities that should be conducted for implementing the processes. According to the number and level of detail of these activities, they were grouped as practices. Each practice represents a functional activity of the process. When implemented, a practice contributes to the achievement of at least one outcome of the performed process. During this step, we linked these activities or practices to the related outcomes and we kept traceability between each practice and the initial set of elementary requirements. Indeed, it is possible that several elementary requirements are related to (or hidden behind) only one practice of a process. The goal trees enable to keep that in mind for further activities, in particular, when questionnaires are being developed for supporting process assessment.

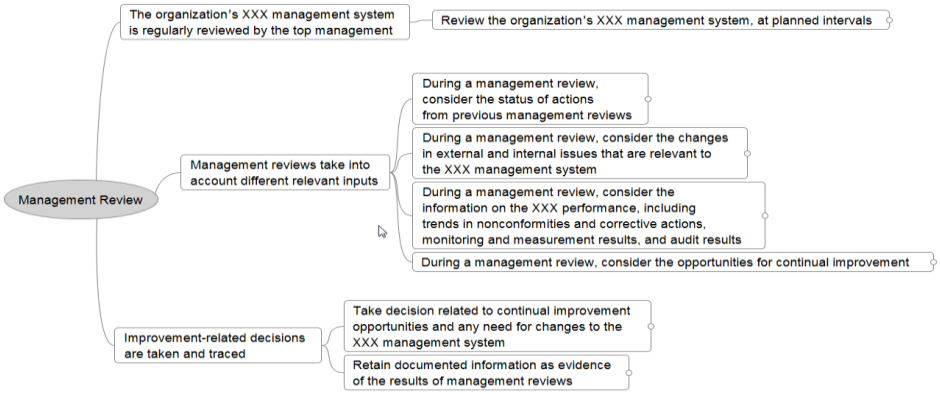

Figure 2 - Goal tree for the "Management Review" process

Step 6 – Allocate each practice to a specific capability level

During this step and for each process, we reviewed the practices and their linked outcomes in order to be sure that they contribute to the process performance attribute (capability level 1) of their associated process. New processes were added to gather HLS activities that were normally reflecting capability levels higher than 1. Thus, we ensured that our process descriptions are such that no aspects of the measurement framework beyond level 1 are contained or implied and thus, that the created process reference and process assessment models comply with ISO/IEC 33004 [5].

Step 7 – Phrase outcomes and process purpose

In order to create a process reference model that follows the guidelines of ISO/IEC TR 24774 [11], each outcome has been phrased as a declarative sentence using verbs at the present tense. Then, the purpose has been phrased to state a high-level goal for performing the process and provide measurable and tangible benefits to the stakeholders through the expected outcomes (process assessment concern). We also checked that the set of outcomes is necessary and sufficient to achieve the purpose of the process.

Step 8 – Phrase the Base Practices attached to Outcomes

Once the purpose and outcomes of a process have been phrased, the process reference model was considered stable enough to phrase the base practices. Base practices were phrased as actions, starting with a verb at the infinitive, according to the guidance provided by ISO/IEC TR 24774 [11]. During steps 8 and 9, we paid a particular attention to choose a wording that suits and that is commonly used in organizations in order to ensure a good adoption of the models.

Step 9 – Determine Work Products among the inputs and outputs of the practices

A work product is an artefact associated with the execution of a process. During the steps 1 and 5, many work products have been identified and listed as inputs or outputs. During this step, these work products were included as parts of indicators in order to finalize the process assessment model.

4 Results

The transformation process described in Section 3 resulted in the creation of the core content of a process capability assessment model for MSS. This model is composed of 10 processes, as listed in Figure 3. These processes, common to all management systems, are described in generic terms (as shown in Figure 4) and require to be contextualized before being used in an assessment.

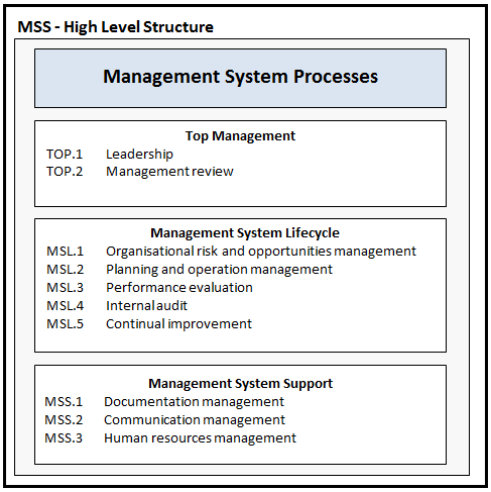

Figure 3 - Processes in the process assessment model for MSS

This list of processes and their associated descriptions have been compared with the results of one of our research project conducted at the same period in Labgroup (a digitization and archiving service provider in Luxembourg). This research project aimed at integrating requirements from various MSS such as ISO/IEC 27001 [13], ISO 31000 [15], and ISO 9001 [16] into a single integrated management system.

This experimentation permitted to consolidate and validate, through a bottom-up approach, the design choices made by the task force during the transformation process. It also helped to validate that the produced process assessment model has the required characteristics of assessability, interoperability, integration, completeness, adoption and applicability.

Process ID	**TOP.2**
Process Name	**Management review**
Process Context	This process, usually performed by the top management, consists in deciding the future improvements. This could be done only after having reviewed the management system and the policies and after having taken into account the actions from previous management reviews as well as the outputs from the "Performance evaluation", "Internal audit", and "Continual improvement" processes.
Process Purpose	The purpose of the Management review process is to decide the implementation of future improvements and changes that will enhance the XXX performance and the effectiveness of the XXX management.
Process Outcomes	As a result of successful implementation of the Management review process: 1. the organization's XXX management system is regularly reviewed by the top management; 2. management reviews include consideration of relevant and various inputs; 3. improvement-related decisions are taken and recorded.
Base Practices	**TOP.2.BP1: Review the organization's XXX management system at planned intervals** [Outcome 1] Organize reviews of the organization's XXX management system by the top management, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. *Annex SL - §5.1: Top management shall demonstrate leadership and commitment with respect to the XXX management system by ensuring that the XXX management system achieves its intended outcome(s)* *Annex SL - §9.3: Top management shall review the organization's XXX management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness*

Figure 4 - Extract of the "Management review" process description

5 Discussion

The discussions presented in this section took place during the third step of the transformation process and all occurred within the internal task force. Most of them (5.1 to 5.4) relate to the composition of the list of processes to be included in the process assessment model. The last two ones (5.5 to 5.6) relate to process assessment aspects.

5.1 Human resource management and resource management

The HLS contains some requirements related to human resources and some others related to other resources (financial, material, etc.) needed by the management system. But should these two aspects be included into one single process? Most of the companies have persons exclusively in charge of the management of human resources. Thus, it was decided to build a dedicated "Human resources management" process. Such a dedicated process contributes to a better assessability of this process

and a better adoption of the process model. The requirements related to the other resources needed by the management system were included into the "Planning and operation management" process. These resources are required whatever the domain(s) covered by the management system. Thus, the "Planning and operation management" process permits to reinforce the interoperability between and integration of multiple management systems.

5.2 Documentation management

The HLS contains two types of requirements dedicated to documentation. The HLS is first defining generic rules for managing documentation across the assessed organization. These requirements have been grouped into a "Documentation management" process. Such a dedicated "Documentation process" is applicable whatever the domain covered by the management system and even in case of an integrated management system. This also contributes to enhance the interoperability between, and the integration of, multiple management systems. The second type of requirements relates to the creation of documents specifically related to a process (as for example the record of the results of management reviews). In that case, each of these requirements specifying the content of these documents has been directly included into the related specific process (such as "Management review" in our example), enhancing the assessability of these specific processes.

5.3 Leadership vs management review

When analysing the requirements linked to the activities performed by Top Management (such as the leadership-related activities or the management review activities), the question of grouping all these requirements under the umbrella of one unique process emerged. The task force finally decided to split the requirements into two different processes: "Leadership" and "Management review". This choice has been done to ensure a better and easier assessability of these two processes. Indeed, on the one side the requirements from clause 5.1 of the HLS describe leadership-related activities (such as defining policy, assigning roles and responsibilities) that take place at the beginning of the implementation of a management system. On the other side the requirements related to the management review (such as those contained in clause 9.3) describe activities that usually take place at a different period of time (i.e. prior the improvement of the management system). Moreover, while the activities of the “Leadership” process are usually well performed and organized (as the beginning of something new), the management review activities can have less priority and thus be performed with lower assurance level. From an assessment standpoint, it is thus important to be able to make the difference between the capability levels of those two processes. Consequently, even if these two kinds of activities are performed by the top management, they should be seen as two different processes.

5.4 Communication management

To address the requirements from the HLS related to the management of the communication, the task force decided to create a dedicated "Communication management" process. Indeed, the internal and external communication activities are in most cases performed by a dedicated role, whatever the size of the company. Having a dedicated process better reflects the situation in place in the field. Thus, this contributes to a better adoption and applicability of the process assessment model. Moreover, the "Communication management" process defines communication and awareness practices that are applicable whatever the domain covered by the management system and even in case of an integrated management system. It permits to enhance the interoperability and the integration aspects of the core content of a process assessment model for MSS.

5.5 Non-auditable requirements

When analyzing the requirements from the HLS, we admitted that all of the elementary requirements were not equally defined or detailed. Indeed, some of these requirements were generic and not auditable as such. However, to ensure a strict traceability between the HLS and the produced process assessment model, the task force decided to include these non-auditable requirements into existing processes. For example, clause 4.4 stated that:

> *"The organization shall establish, implement, maintain and continually improve an XXX management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard."*

This generic requirement could be seen as a high-level requirement that covers all the elementary requirements described in the HLS. The task force first took the decision to split this requirement into four elementary requirements:

- *"The organization shall **establish** an XXX management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard. "*
- *"The organization shall **implement** an XXX management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard. "*
- *"The organization shall **maintain** an XXX management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard. "*
- *"The organization shall **continually improve** an XXX management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard. "*

Then, it was decided to associate the first three requirements to the "Planning and operation management" process whereas the fourth one was linked to the "Continual improvement" process.

5.6 Process completeness

At the end of the transformation process, we reviewed the complete process model to check the completeness of each process. Indeed, the fact that they are based on a set of elementary requirements coming from the HLS does not guarantee that the processes are complete, or in other words that the process outcomes are sufficient to achieve the process purpose. For example, in the HLS [2] the requirements related to risk and opportunity management does not include aspects such as the risk assessment, the selection of the risk treatment strategy, or the monitoring of the residual risk. All these aspects are missing but should be present in order to have a well-formed and complete risk management process. Thus, we decided to enrich our process model by adding the needed but missing outcomes and practices to each incomplete process. For filling the gaps of the HLS at the risk management level, we used the ISO 31000 standard [15], which provides requirements for risk management that are applicable to any domain. By doing so, we ensure a better assessability of each process and a better adoption of the created process models.

6 Conclusion

This paper describes the construction of the core content of a process assessment model for MSS. The resulting process model is covering the processes that are common to all MSS and thus reflecting an international consensus as defined by ISO standards. This paper also explains how the produced process model could support consistency and interoperability between domain-specific MSS.

With that core content made available, only the content specific to a particular domain still needs to be described when one wants to build a process assessment model to assess a management system for a specific domain. For this reason, the proposed process assessment model will permit to avoid the construction of new process assessment models from scratch. Experts from CRP Henri Tudor are currently using this core content to design a process assessment model for information security management system (based on [13]), as well as one for business continuity management system (based on [14]).

Another future work will consist in helping the digitization and archiving services providers in Luxembourg to comply with the technical regulation requirements described in [17]. For that, we will combine the core content of a process assessment model for MSS with requirements from international standards (ISO/IEC 27001:2005, ISO/IEC 27002:2005 and ISO/IEC 30301:2011) and national regulations [18]. This will lead to the design of an integrated management system for information lifecycle management.

Finally, in order to ensure that it reflects an international consensus, the process models described in this paper has been proposed as New Work Item at the ISO level. If accepted, the new Technical Specification can contribute to enhance the adoption of our research results, i.e. the core content of a process assessment model for MSS.

References

[1] ISO Survey (2012). http://www.iso.org/iso/home/standards/certification/iso-survey.htm
[2] ISO/IEC Directives, Part1. (2014). Annex SL.
[3] ISO/IEC 33001: Information technology -- Process assessment -- Concepts and terminology. (2014).
[4] ISO/IEC 33002: Information technology -- Process assessment -- Requirements for performing process assessment. (2014).
[5] ISO/IEC 33004: Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models. (2014).
[6] Barafort B., Renault A., Picard M., Cortina S. "A Transformation Process for Building PRMs and PAMs based on a Collection of Requirements – Example with ISO/IEC 20000". 8th international SPICE 2008 Conference, Nuremberg, 2008.
[7] Rifaut, A. (2005). Goal-Driven Requirements Engineering for supporting the ISO 15504 Assessment Process. European Conference for Software Process Improvement (EUROSPI) proceedings (pp. 151-162). Springer.
[8] Cortina, S., Picard, M., Valdes, O., & Renault, A. (2010). A Challenging Process Models Development: The ITIL v3 Lifecycle Processes. Proceedings of the 10th International SPICE Conference on Process Assessment and Improvement. Pisa.
[9] Public Research Center Henri Tudor. (2009). ITSM Process Assessment Supporting ITIL. Amersfoort: Van Haren Publishing.
[10] Togneri MacMahon, S., Mc Caffery, F., & Keenan, F. (2013). Transforming Requirements of IEC 80001-1 into an ISO/IEC 15504-2 compliant Process Reference Model and Process Assessment Model. Proceedings of the 20th EuroSPI² Conference. Dundalk.
[11] ISO, ISO/IEC TR 24774: Software and systems engineering -- Life cycle management -- Guidelines for process description. (2010).
[12] ISO/IEC 33020: Information technology -- Process assessment – Process measurement framework for assessment of process capability. (2014).
[13] ISO/IEC 27001: Information technology – Security techniques – Information security management systems -- Requirements. (2013).
[14] ISO 22301: Societal security – Business continuity management systems – Requirements. (2012).
[15] ISO 31000: Risk management – Principles and guidelines. (2009).
[16] ISO 9001: Quality management systems – Requirements (2008).
[17] Technical regulation requirements and measures for certifying Digitisation or Archiving Service Providers (PSDC) – Version 1.3 (2013)
[18] Circular CSSF 12/544: Optimisation of the supervision exercised on the "support PFS" by a risk-based approach (2012)