ILNAS

THE ELECTRONIC ARCHIVING FRAMEWORK IN LUXEMBOURG

AN INTRODUCTION

Version 1.0 · June 2018

THE ELECTRONIC ARCHIVING FRAMEWORK IN LUXEMBOURG

AN INTRODUCTION

Version 1.0 · June 2018

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Contents

1 Introduction

Traditionally, the archiving of physical documents, such as paper documents, involves storing documents for a long period of time while ensuring their integrity during that time, i.e. archived documents should not be lost, damaged, or destroyed. Often it is also important to protect the confidentiality of the documents that were archived. As archiving can be costly, business organizations typically only archive documents that are valuable to them and essential to their business interests, or documents that have to be archived because of legal requirements. Documents that are archived may hence possess a legal value. For instance, an insurance company might archive insurance contracts signed by customers to keep physical and legal proof that customers have entered into a contractual relationship with the company.

The aim of electronic archiving is to transpose the concept of long-term document storage to the digital world. Digital documents can be ultimately seen as sequences of bits, i.e. sequences of the values 0 or 1, which can be easily duplicated. Moreover, unlike paper documents, the copies of digital documents are indistinguishable from the originals. In that way, digital documents can be easily protected against destruction by storing multiple copies of the documents at different locations, for instance. On the other side, paper documents can be copied as well, but typically only the original document is fully recognized in legal settings. The manipulation of digital documents can also present its own challenges: ensuring the long-term readability and confidentiality of digital documents may be harder to achieve than for paper documents. For example, in the world of information technology, formats used for storing data, or even the technologies used for physical data storage, may evolve very fast and they can become obsolete in a matter of years (e.g. floppy disks). One particular challenge is therefore to ensure that data stored in a specific format on some data storage device can still be read in ten or twenty years' time. Electronic archiving services therefore also have to incorporate solutions for guaranteeing the long-term readability and confidentiality of digital documents.

Despite these challenges, the lower storage & handling costs and physical space requirements of electronic archives, as well as the possibility of providing additional electronic processing, has increased the interest in electronic archiving solutions. One aspect that had still been missing for allowing electronic archiving to replace traditional archiving is the recognition of the legal value of digital archives. In the Law of 25 July 2015 on electronic archiving [26], the Grand Duchy of Luxembourg was one of the first countries to define the conditions under which the conformity of electronic archives with the original digital documents is legally recognized. However, the Law on electronic archiving does not stop there: it also introduces the legal conditions under which a digitized version of an analog document, e.g., a scan of a paper document, is considered to have the same probative value as the original document. The Law

on electronic archiving in the Grand Duchy of Luxembourg therefore establishes all the required components for replacing traditional archiving with its electronic counterpart. For instance, it even permits paper documents to be destroyed after digitization without losing the legal value that the paper documents offered.

However, for a digitized copy to benefit from the same probative value as the original analog document, or a digital archive w.r.t. the original digital document, it must have been created by an organization or service provider that has been given the legal status of *prestataire de services de dématérialisation ou de conservation* (PSDC), i.e. "provider of digitization or e-archiving services" in English.

The Luxembourg institute for standardization, accreditation, safety, and quality of goods and services (ILNAS), called "Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services" in French, is the sole government agency in the Grand Duchy of Luxembourg authorized to grant the status of PSDC. ILNAS is placed under the administrative supervision of the Minister of the Economy of the Grand Duchy of Luxembourg. To obtain the status of PSDC, organizations need to fulfill a certain number of conditions. For instance, they must be certified w.r.t. the Technical Regulation for a management system and security measures for digitization and e-archiving service providers [27]. The Technical Regulation is written as a sector-specific application of the international standards ISO/IEC 27001 and ISO/IEC 27002 concerning information security to digitization or e-archiving services.

The Digital Trust Department of ILNAS is Luxembourg's supervisory body for providers of digitization or electronic archiving services according to the Law of 25 July 2015 on electronic archiving that are established in Luxembourg. The legal missions of the Digital Trust Department of ILNAS are described in [25].

In the following chapters we provide an overview of the e-archiving framework that has been created in the Grand Duchy of Luxembourg with the aims of

(1) providing an introduction to the topic for readers who are unfamiliar with the legal context relating to e-archiving in Luxembourg, and

(2) giving guidance to organizations that plan to provide digitization or e-archiving services.

We also introduce the supervision procedure that is applied by the Digital Trust Department of ILNAS to organizations that have obtained the PSDC status.

2 The Electronic Archiving Framework in Luxembourg

The topic of electronic archiving in the legislation of the Grand Duchy of Luxembourg covers the following two aspects:

- digitization of analog documents, and
- archiving of digital documents.

A document is said to be "digital" if it consists of a sequence of bits and it can only be visualized or manipulated with the help of information processing equipment (e.g. laptops, desktop computers, servers, or smartphones). In the following, "electronic documents" is used as a synonym for "digital documents". On the other hand, "analog documents" are documents that are not digital, i.e. documents that are bound to physical objects such as paper, microfilm, photographic film, vinyl records, etc.

"Digitization of analog documents" refers to transforming analog documents into identical reproductions in the form of digital documents. Typically, paper documents are digitized with the help of scanners.

The aim of "archiving digital documents" is to preserve certain properties of digital documents, such as their integrity or confidentiality, over extended periods of time.

The *Law of 25 July 2015 on electronic archiving* [26] (in the following also simply referred to as "Law on electronic archiving") introduces the conditions under which digital documents benefit from a presumption of conformity w.r.t. the respective original documents, i.e. the conditions

(1) under which the digitized (digital) version of an analog document has the same probative value as its analog version, and

(2) under which the probative value of archived digital documents is maintained over time w.r.t. the digital document that was entered into the archiving process.

Informally, a document has probative value if it provides sufficient evidence to prove a disputed point in a trial.[1] Note that the process of archiving cannot modify the legal value of the document that was originally archived. For instance, if a digital document is a digital reproduction of a paper document that does not enjoy the same probative value as the original paper document, then the archiving of such a digital document only maintains the probative value w.r.t. the digital document that was archived and not w.r.t. the original paper document.

[1] See also, e.g., `https://www.law.cornell.edu/wex/probative_value`.

In the following we use the term "copy with probative value" to denote a copy that is assumed to have the same probative value as the original.

One can argue that the revolutionary aspect of the e-archiving framework in the Grand Duchy of Luxembourg concerns the digitization of analog documents as it opens up numerous possibilities for providing additional services that are difficult to implement for analog documents. Moreover, the digitization of analog documents may help to reduce operational costs. For instance, the digitization of documents can bring the following advantages.

- As digitized documents may benefit from the same probative value as the original analog documents, it becomes unnecessary to store the original analog documents. Consequently, large, physical archives for storing the analog documents and the associated manipulations of such archives are no longer needed.
- Using digital documents also mitigates several threats that affect analog documents. If only the original analog document has a certain legal value, then it becomes even more important to protect its integrity. Threats such as fire or theft may lead to grave consequences when the only document that possesses a legal value is no longer available. As digital documents can be easily duplicated, an organization can protect itself against the loss of important documents by storing them redundantly (in multiple locations).
- Another important advantage of digital documents is that they can be easily accessed and examined. Instead of having to search through a large physical archive, digital documents can be accessed instantaneously in databases or file stores, even from remote locations.
- The process of searching through documents can also be accelerated if the documents are in digital form. For instance, by indexing keywords in digital documents, it becomes possible to quickly find all the documents in which certain keywords appear. For analog documents that were digitized, one can first extract the keywords through an optical character recognition (OCR) process.

The Law of 25 July 2015 on electronic archiving introduces the main legal context regarding digitization and electronic archiving in the Grand Duchy of Luxembourg. The technical conditions that govern the provision of digitization and electronic archiving services are defined in a companion document, the *Technical Regulation for a management system and security measures for digitization and e-archiving service providers* [27] (in the following also referred to as "Technical Regulation for digitization and e-archiving service providers").

One aim of the legal context concerning digitization and electronic archiving in Luxembourg is to reverse the burden of proof. If an analog document has been digitized and archived according to the Law of 25 July 2015 on electronic archiving, then the digital document is presumed to have the same legal value as the original analog document by default. To contest the legal equivalence of the digital document, one would have to prove that some of the requirements of the Law of 25 July 2015 on electronic archiving were not followed during the digitization or archiving step.

We have to point out that the legal context concerning digitization does not apply to every type of analog document, but only to "private deeds" or to the types of documents referred to in Article 16 of the "Code de commerce" (see also Section 3). Regarding the archiving of digital documents, the Law of 25 July 2015 is applicable to any private deed in electronic form and to any document that was originally created in electronic form.

The Law of 25 July 2015 on electronic archiving introduces the legal status of

prestataire de services de dématérialisation ou de conservation,

or **PSDC**, i.e. "digitization or e-archiving service provider" in English. Although the Law on electronic archiving permits any legal person to obtain the PSDC status, we simply refer to "organizations" instead of "legal persons" in the following to simplify the presentation. Legal persons can be individuals, companies, government agencies, etc.

ILNAS is the sole government agency in the Grand Duchy of Luxembourg authorized to grant the status of PSDC to organizations. To that end, organizations need to fulfill a certain number of conditions. For instance, they must be certified w.r.t. the Technical Regulation for a management system and security measures for digitization and e-archiving service providers by a certification body that is accredited according to the international standards

- ISO/IEC 17021-1:2015 "Requirements for bodies providing audit and certification of management systems" [17],[2] and
- ISO/IEC 27006:2015 "Requirements for bodies providing audit and certification of information security management systems" [16].

Only documents that have been digitized or archived by PSDCs according to the policies, processes, and procedures that were certified in the electronic archiving context will be deemed to have the same probative value as the corresponding original documents.

In the following we describe the digitization and electronic archiving workflows that the Law of 25 July 2015 on electronic archiving considers (cf. [28]). Figure 2.1 illustrates the typical workflow for the digitization of analog documents.

- **Pickup or delivery of analog documents:** the first step consists in making the analog documents that should be digitized available to the organization that performs the digitization. To that end, the analog documents are either picked up by the organization itself or the client delivers them to the organization. Typically, after delivery or pickup the analog documents are stored in a temporary storage site that is under the organization's responsibility until the digitization of the analog documents can begin.

[2] All standards referenced in this document can be purchased from the ILNAS eShop, which can be accessed at `https://ilnas.services-publics.lu/ecnor/home.action`.

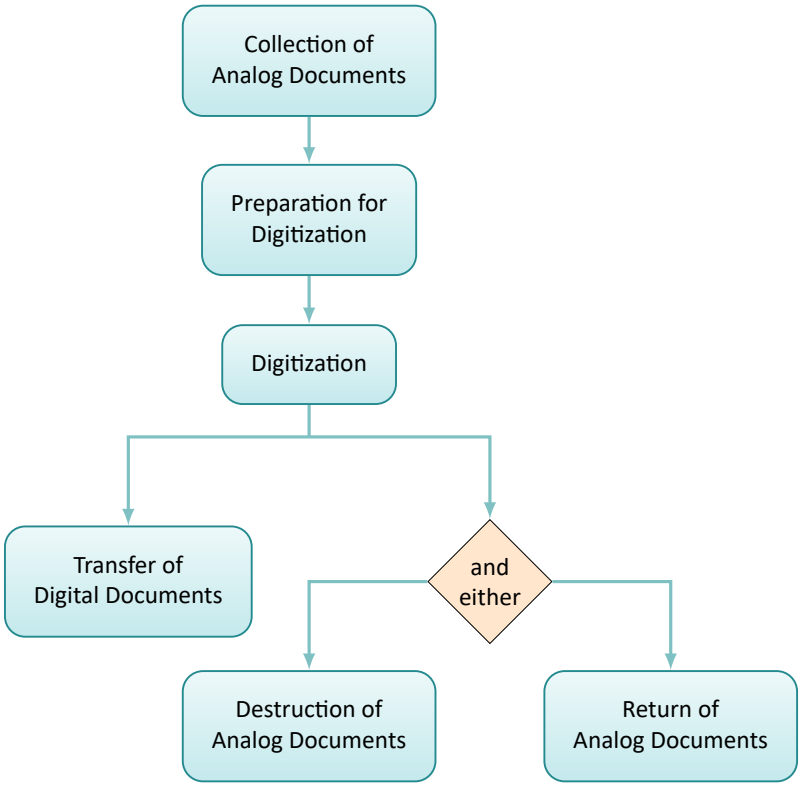

Figure 2.1: Typical workflow of digitization

- **Creation and temporary storage of digital documents:** in the next step, the analog documents are prepared for scanning (by aligning stacks of papers or by removing staples, for instance). Subsequently, the scanning takes place and digital documents are created out of the analog documents. Digitization metadata are associated with the digitized documents, and the digitized documents are temporarily stored in a secure file store. The metadata typically contain information about the scanner settings, such as the number of colors or the scanning resolution, but also information for protecting the integrity of documents, such as their cryptographic hash values.
- **Temporary storage of analog documents:** after the digitization, the analog documents are stored in a site that is under the organization's responsibility until either the analog documents can be returned to the client or they can be destroyed.
- **Transfer and return of documents:** the last step consists in transferring the

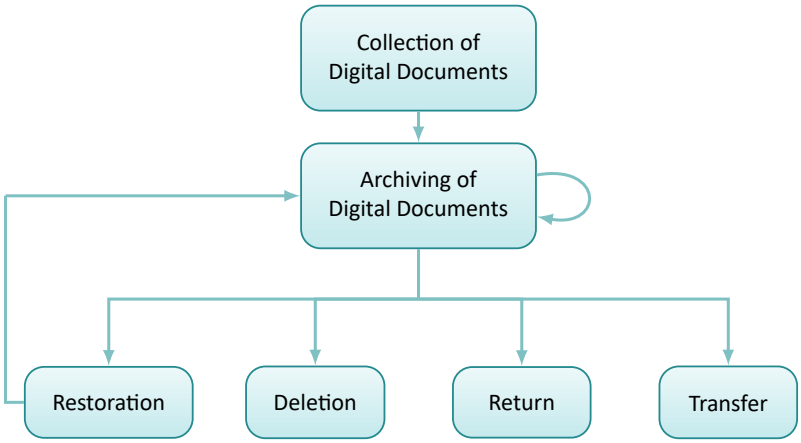

Figure 2.2: Typical workflow of electronic archiving

digital documents (with associated metadata) to the electronic archiving systems or to the client, which can be done in the form of an electronic file transfer or of a physical transport of storage media. Regarding the analog documents, there are two options:

- they can be returned to the client, either through a delivery set up by the organization, or through a pickup organized by the client; or
- the analog documents are destroyed by the organization.

In the last step, the organization deletes the digital documents and associated metadata, unless the organization also proceeds with archiving the digital documents.

Figure 2.2 depicts the typical workflow of electronic archiving.

- **Collection of digital documents:** the digital documents that should be archived are made available to the organization that carries out the electronic archiving, either through electronic file transfer or through physical transport (or pickup) of storage media,
- **Creation of digital archives:** the documents are prepared for archiving and they are then injected into the electronic archiving systems, where the digital documents are converted into digital archives and archival metadata is associated with the digital archives. The archival metadata may contain information necessary for ensuring the integrity of the digital archives such as cryptographic hash values. Additionally, the details of every manipulation that concerns a digital archive may be recorded in the archival metadata. The conversion into digital archives may be accompanied by a file format conversion. Once the correct submission of the digital documents into the electronic archiving systems has been

confirmed, the digital documents can be deleted. The digital archives need to be stored securely for as long as required.

- **Restoration, transfer, and deletion of digital archives:** Digital archives may be
  - restored: the client (or an authorized third-party) may request a copy of the digital archive from the organization, which can be transferred to the client either through electronic file transfer or through a physical transport of storage media. The digital archive itself is not modified. Note that the restoration request may be limited only to the metadata associated with the digital archive. Such metadata can be useful for proving or verifying that the archiving process has been executed correctly, for instance.
  - deleted: a maximum retention period may be assigned to digital archives. Once the maximum retention period has elapsed, the digital archive will be deleted from the archiving systems. Alternatively, the client herself may also request that a digital archive is deleted from the archiving systems.
  - returned: at the request of the client, a digital archive, together with its associated archiving metadata, may be returned to the client. For returning a digital archive, a copy of the digital archive is transferred to the client in the same way as for restoring a digital archive. Subsequently, the organization deletes the digital archive from the archiving systems.
  - transferred: at the request of the client or when the organization ceases to provide digitization or e-archiving services, a digital archive may be transferred to another digitization or e-archiving service provider. In that case the organization has to delete the digital archives that have been transferred away from its archiving systems.

The electronic archiving framework lends itself, for instance, to the commercial provision of digitization or e-archiving services.

External digitization or e-archiving service provider:

- A company that provides traditional archiving services of paper documents already may decide to additionally provide an electronic archiving service that is compliant with the Law of 25 July 2015 on electronic archiving.
- For reducing archiving costs, a company that needs to archive a great number of paper documents may decide to purchase digitization and e-archiving services provided by an established digitization or e-archiving service provider.

Another possibility that the Law of the 25 July 2015 allows is for organizations to provide digitization or e-archiving services internally or for subsidiaries only. Note that companies that provide such "internal" digitization or e-archiving services cannot immediately provide digitization or e-archiving services to external customers.

Internal digitization or e-archiving service provider: For instance, to avoid having to store large quantities of paper documents, a financial institution that maintains an archive of customer contracts consisting of paper documents and that does not want to purchase electronic archiving services for confidentiality reasons may decide to set up an internal digitization or e-archiving service.

The Law of 25 July 2015 on electronic archiving also introduces special types of digitization or e-archiving service providers for the financial sector.

Digitization or E-Archiving Service Providers for the Financial Sector

The Commission de Surveillance du Secteur Financier, CSSF,[3] is a public institution in the Grand Duchy of Luxembourg tasked with the supervision of the financial sector in Luxembourg. Besides supervision, regulation, and inspection, the CSSF also enforces laws relating to financial consumer protection and it aims at promoting transparency, simplicity, and fairness regarding financial products and services.

By law, every organization that wants to provide financial services in the Grand Duchy of Luxembourg is subject to regulation by the CSSF. For that purpose, the Law of the 5 April 1993 relating to the financial sector [24] introduces the legal status of "Professional of the Financial Sector" ("Professionels du Secteur Financier" in French), abbreviated with PSF. Moreover, the Law of the 5 April 1993 relating to the financial sector defines a sub-category of "support PSF" ("PSF de support" in French), which are organizations that do not carry out financial activities themselves but which are sub-contractors that provide operational services to proper PSF (which carry out financial activities themselves).

In particular, the Law of 5 April 1993 relating to the financial sector defines the following types of support PSF:

1. Art. 29-1: client communication agents,
2. Art. 29-2: administrative agents for the financial sector,
3. Art. 29-3: system operators of primary IT systems for the financial sector,
4. Art. 29-4: system operators of secondary IT systems and of communication networks for the financial sector,
5. Art. 29-5: digitization service provider for the financial sector, and
6. Art. 29-6: e-archiving service provider for the financial sector.

Note that an organization that wants to obtain the "digitization service provider for the financial sector" or the "e-archiving service provider for the financial sector" status needs to have been granted the PSDC status by ILNAS first.

In the following we will provide a short description of the Law of 25 July 2015 on electronic archiving, of the supervision scheme for PSDC applied by ILNAS, and of the Technical Regulation for a management system and security measures for digitization and e-archiving service providers.

[3] See also `http://www.cssf.lu`

3 The Law of 25 July 2015 on Electronic Archiving

In this chapter we briefly describe the most important articles of the Law of 25 July 2015 on electronic archiving [26].[1] Chapter 1 of the Law of 25 July 2015 on electronic archiving describes the following objectives of the law:

- to introduce the relevant notions and definitions for the digitization of original documents and for the archiving of digitized documents and of original documents in digital form;
- to determine the conditions under which digitized documents or original documents in digital form benefit from a presumption of conformity with the original documents;
- to define the rules that digitization and e-archiving service providers need to adhere to.

Note that in the Law on electronic archiving the term "original document" refers to a "private deed" or to the types of documents referred to in Article 16 of the "Code de commerce", i.e. certain documents relating to accounting and associated supporting documents. Similarly, an "original document in digital form" is defined as a "private deed in electronic form" or any document that was originally created in digital form (not limited to the types of documents referred to in Article 16 of the "Code de commerce").

Article 3 stipulates that additional requirements for the digitization and e-archiving of documents are specified in the Technical Regulation for Digitization and E-Archiving Service Providers [27].

The legal requirements under which digitization or e-archiving service providers have to operate are introduced in Chapter 2. Article 4 defines the supervision procedure of digitization and e-archiving service providers, and it determines ILNAS as the national supervisory body of such service providers. A more detailed description of the supervision procedure can be found in Section 4. Article 4 also introduces the concept of a List of digitization and e-archiving service providers, which is published on the website of ILNAS. Moreover, it is specified that only organizations which appear on that list can make use of the denomination "prestataire de services de dématérialisation ou de conservation" or "PSDC". More details regarding the List of PSDCs can be found in

[1] Note that our description can only be seen as an approximation or simplification of the contents of the law – the text of the law prevails.

Section 4. The last paragraph of Article 4 establishes that organizations that carry out digitization & e-archiving activities only for their own purposes or only for one or several companies that belong to the same group can also apply for the legal status of PSDC. In that case, the last paragraph of Article 4 states that fewer conditions apply on disclosure requirements, on ownership and guarantees regarding data storage equipment, and on the cessation of PSDC activities.

Article 5 defines the conditions under which the inscription of an organization into the List of PSDCs may be suspended or revoked. For instance, ILNAS may proceed with suspending or revoking the inscription of an organization into the List of PSDCs when it discovers an event or an incident that may violate, or that has already violated, one of the legal requirements of the Law on electronic archiving or the Technical Regulation for digitization and e-archiving service providers. Article 5 also forces digitization or e-archiving service providers to inform ILNAS without undue delay of any (suspected) violation of the Law on electronic archiving or the Technical Regulation for digitization and e-archiving service providers. After a suspension of revocation of its PSDC status, the organization must inform all interested parties that legally need to be in possession of an original document that has been digitized or archived by the organization. The affected parties then have the right to demand the return of every document, analog or digital, that is kept by the organization as well as the metadata relevant for e-archiving, without having to pay excessive fees.

Disclosure requirements that digitization or e-archiving service providers need to observe are specified in Article 6. Every time before a digitization or e-archiving service provider enters a new contractual relationship with a client, it has to inform the client, at least about,

- the procedure that is followed for digitization or electronic archiving;
- the procedure that is followed for restoring copies with probative value in a legible form while guaranteeing the faithfulness of the reproduction to the respective originals;
- the conditions for a possible outsourcing of data storage activities to subcontractors, including the storage location;
- the legal obligations that digitization or e-archiving service providers need to follow;
- the contractual conditions for providing digitization and e-archiving services, including the limits of the legal responsibilities of digitization or e-archiving service providers;
- the standards and the procedures that are being followed, as well as the essential technical characteristics of the technical installations used for providing digitization or e-archiving services.

Article 7 introduces the obligation for employees of a digitization or e-archiving service provider and for the personnel of ILNAS to observe professional secrecy regarding all information obtained (including the contents of the digitized or archived

documents) during their professional activities, except if permitted by the owner of the information. The obligation to observe professional secrecy does not apply if the disclosure of information is authorized or required by law, or during interactions with ILNAS in the context of supervisory activities.

Article 8 stipulates that every e-archiving service provider must ensure at all times that at least one data copy of the digital documents that have the same probative value as the originals or of original documents in digital form is stored on hardware that the service provider fully owns. Such storage hardware cannot be confiscated by law enforcement officers as long as the digital originals or the copies that have the same probative value as the original documents have not been returned to the respective owners.

The transfer and cessation of PSDC activities is addressed in Article 9. A digitization or e-archiving service provider may transfer a part or all of its activities to another digitization or e-archiving service provider under the following conditions:

- the digitization or e-archiving service provider has to inform the owner of the documents at least one month in advance of its intention to cease its PSDC activities and to transfer the copies with probative value and original documents in digital form that it keeps to another digitization or e-archiving service provider;
- at the same time, the ceasing digitization or e-archiving service provider needs to specify the identity of the digitization or e-archiving service provider to which the digital documents are being transferred;
- the owners of the documents also need to be informed that they may refuse the planned transfer of PSDC activities, in which case the ceasing digitization or e-archiving service provider must return all analog or digital documents (including relevant metadata) to their rightful owners (or to any other organization named by the owner of the documents);
- the document transfer has to take place on the date when the PSDC activities cease, at the latest.

Similarly, when a digitization or e-archiving service provider ceases its PSDC activities without transferring its activities to another digitization or e-archiving service provider, the ceasing service provider must return all analog or digital documents (including relevant metadata) to their rightful owners, or to any other organization named by the owner of the documents. Every digitization or e-archiving service provider that cannot or does not want to continue its PSDC activities must also inform ILNAS immediately. Moreover, within three months, the ceasing service provider has to ensure that its PSDC activities are taken over by another digitization or e-archiving service provider or that all analog and digital documents are returned to their rightful owners.

The only Article 10 in Chapter 3 refers to fines that can be imposed on organizations that make use of the denomination “prestataire de services de dématérialisation ou de conservation” (digitization or e-archiving service provider) or of the acronym “PSDC” without having been granted the PSDC status by ILNAS.

Modifications regarding the "Code civil" are introduced in Chapter 4. More precisely, Articles 11 and 12 modify the "Code civil" by declaring that, without proof to the contrary, digital copies that were made by a digitization or e-archiving service provider have the same probative value as the original document. It is also specified that a judge cannot reject a copy only because it is in electronic form (analogously to the eIDAS regulation) or because it has not been created by a digitization or e-archiving service provider.

Article 13 introduces two new types of organizations that will fall under the supervision of the CSSF: digitization or e-archiving service providers for the financial sector, which provide digitization or e-archiving services for certain types of financial organizations. The legal status of "digitization service provider for the financial sector" and of "e-archiving service provider for the financial sector" can only be granted to legal persons. Article 13 defines minimum requirements on share capital for these two types of service providers. Note that the status of "digitization service provider for the financial sector" or of "e-archiving service provider for the financial sector" can only be granted to an organization by the CSSF after that organization has already obtained the PSDC status from ILNAS.

4 ILNAS Supervision Scheme for PSDCs

As we have seen before, ILNAS is the sole government agency in the Grand Duchy of Luxembourg authorized to grant the status of PSDC to organizations. Moreover, the supervision of digitization or e-archiving service providers is carried out by ILNAS via its Digital Trust Department as well. In this chapter we describe the procedure that is applied by the Digital Trust Department in the context of the supervision of digitization or e-archiving service providers (which are applying for the PSDC status or which have been granted the PSDC status already). The detailed supervision procedure can be found in [9].

Figure 4.1 illustrates the supervision scheme that is applied by the Digital Trust Department. The scheme relies on the following actors:

- the national accreditation body, called "Office Luxembourgeois d'Accréditation et de Surveillance" (OLAS) in French, which accredits the competence of conformity assessment bodies according to the international standards ISO/IEC 17021-1:2015 [17] and ISO/IEC 27006:2015 [16];
- conformity assessment bodies (CABs), independent bodies of assessors, accredited by the national accreditation body on the basis of the standards ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, for assessing the conformity of organizations w.r.t. the Law of the 25 July 2015 on electronic archiving and the Technical Regulation for a management system and security measures for digitization and e-archiving service providers.
- the Digital Trust Department of ILNAS, the national supervisory body, which is responsible for the supervision of PSDCs under the Law on electronic archiving.

The purpose of an accreditation body, such as OLAS in the Grand Duchy of Luxembourg, is to act as a supervisory authority of conformity assessment bodies. According to ISO/IEC 17000:2004 [5.6], *accreditation* is defined as a "third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence to carry out specific conformity assessment tasks". Hence, the goal of accreditation bodies is to ensure the compliance of conformity assessment bodies w.r.t. certain standards. The evaluation process of conformity assessment bodies is called accreditation.

In accordance with the Law of the 25 July 2015 on electronic archiving, the Digital Trust Department maintains a list of all the organizations that have been granted the PSDC status, the so-called "List of PSDCs", which is published on the website of

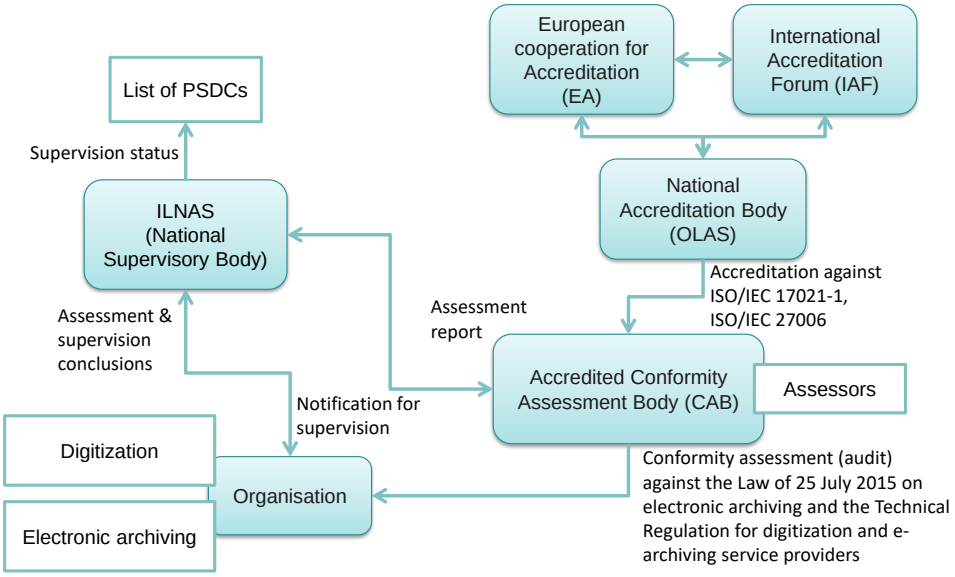

Figure 4.1: Supervision scheme for digitization and e-archiving service providers

ILNAS [7]. A simplified version of the List of PSDCs from 22 June 2018 is shown in Table 4.1. At the time of writing four organizations have obtained the PSDC status. Every organization that is included in the List of PSDCs falls under the supervision of the Digital Trust Department.

4.1 Initiation of the Supervision

To apply for the PSDC status, an organization needs to notify its intent by submitting the form "ILNAS/PSDC Form F001a – Notification for supervision" to the Digital Trust Department. The organization also has to specify the scope of its intended activities, i.e. whether it wants to provide digitization and/or e-archiving services. The submission of this form allows the PSDC to officially notify its intent of applying for the PSDC status and it constitutes the "triggering event" for the supervision process.

Together with form F001a (and some other documents), the applicant needs to include a certificate issued by the CAB that demonstrates the conformity of the organization with the Law of the 25 July 2015 on electronic archiving and the Technical Regulation for a management system and security measures for digitization and e-archiving service providers. The certificate is issued by the CAB after the organization has successfully passed an initial certification audit carried out by the CAB.

Initial certification audits are typically composed of two phases: the CAB reviews the

Organization	Supervision ID	PSDC Status Since	Scope
Lab Luxembourg S.A. 9, rue Henri Tudor L-5366 Münsbach	2016/9/001	1 February 2017	Digitization & E-archiving
Victor Buck Services S.A. 13-15, Parc d'activités L-8308 Capellen	2017/9/003	12 July 2017	Digitization & E-archiving
Numen Europe S.A. 15, rue des Scillas L-2529 Howald	2016/9/002	26 September 2017	Digitization & E-archiving
Syndicat Intercommunal de Gestion Informatique 6, rue de l'Étang L-5326 Contern	2017/9/005	26 February 2018	E-archiving

Table 4.1: Simplified List of PSDCs as of 22 June 2018

organization's documentation during the first phase and the second phase consists of a more detailed inspection taking place on the organization's premises, which includes members of staff being interviewed by auditors. The aims of the first phase are to determine the readiness of the organization for the second phase of the audit. The minimum duration of such audits is also fixed in the PSDC supervision procedure that is applied by the Digital Trust Department [9]. The audit duration depends on the audit type (initial vs. surveillance audit) and on the pre-existing certifications that the organization may own.

During the audit, *nonconformities* can be found, i.e. areas or aspects in which the organization is not compliant with the Law of the 25 July 2015 on electronic archiving or the Technical Regulation for a management system and security measures for digitization and e-archiving service providers. According to ISO/IEC 17021-1:2015, a nonconformity is defined as a non-achievement of a requirement. Typically, nonconformities are classified into two categories: minor and major. A *major nonconformity* is a nonconformity that affects the ability of a management system to reach the intended outcome. Dually, a *minor nonconformity* is a nonconformity that does not affect a management system's ability to attain a desired outcome. A major nonconformity is raised, for instance, if there is significant doubt that certain services fulfill the specified requirements. Also, several minor nonconformities that affect one requirement of a standard may give rise to a major nonconformity. A minor nonconformity may be raised, for example, if a problem has been detected that only affects one part of a requirement in a standard and that does not endanger the intended outcome of the management system.

All major nonconformities have to be resolved before the CAB can issue a conformity

assessment certificate. Minor nonconformities do not have to be fixed immediately, but it suffices to provide a corrective action plan for each minor nonconformity, which has to be accepted by the CAB. After an analysis of the corrective action plans, the CAB may issue a conformity assessment certificate to the organization.

We refer the reader to [9] for the complete list of documents that have to be submitted by an organization to the Digital Trust Department to apply for the PSDC status. Note that the Digital Trust Department may ask the applicant to provide additional documents that are not indicated in [9] before a decision about granting the PSDC status can be made.

Recall that the aim of the supervision by the Digital Trust Department is to ensure that PSDCs meet the applicable requirements laid down in the Law on electronic archiving and in the Technical Regulation for a management system and security measures for digitization and e-archiving service providers. During the review of the application for the PSDC status the following points (†) are analyzed in particular:

- validity and scope of the accreditation of the conformity assessment body;
- validity and scope of the conformity assessment of the applicant against the Law of 25 July 2015 on electronic archiving and the Technical Regulation for digitization and e-archiving service providers;
- knowledge of the Law of 25 July 2015 on electronic archiving and of the Technical Regulation for digitization and e-archiving service providers by the auditors who carried out the accreditation assessment of the CAB;
- knowledge of the Law of 25 July 2015 on electronic archiving and of the Technical Regulation for digitization and e-archiving service providers by the auditors who carried out the conformity assessment of the applicant;
- coverage of the Law of 25 July 2015 on electronic archiving and of the Technical Regulation for digitization and e-archiving service providers in the conformity assessment report;
- if applicable, the resolution of major nonconformities detected during the conformity assessment.

Note that, by the Law of 25 July 2015 on electronic archiving, an organization may only use the designation “PSDC” once it has appeared on the List of PSDCs.

4.2 During the Supervision

After an organization has been included into the List of PSDCs, it will be under the supervision of the Digital Trust Department of ILNAS.

During the supervision phase, the Digital Trust Department aims to organize a supervisory meeting with each PSDC at least every 6 months, which allows for a review of the PSDC’s recent activities. PSDCs are also obliged to inform the Digital

Trust Department of every major change in their organization. Major changes include significant changes to the structure of the organization or to the resources that are used for carrying out activities that fall under the supervision of the Digital Trust Department. PSDCs may apply for an extension of their PSDC status (e.g., if they additionally want to provide digitization services after only carrying out e-archiving activities so far) by notifying the Digital Trust Department using the same forms as for the initiation of the supervision.

PSDCs are obliged to annually demonstrate to the Digital Trust Department that they still fulfill all the conditions from the beginning of the supervision (see Section 4.1). To that end, the conformity assessment scheme applied by the CAB requires a conformity assessment every 12 months. These conformity assessments are organized in the form of a conformity assessment program that extends over three years. A full conformity assessment is carried out in the beginning, which is followed by yearly surveillance conformity assessments in the two following years. Three years after the initial conformity assessment, the assessment cycle starts anew with a full conformity assessment. PSDCs must submit conformity assessment reports issued after conformity assessments to the Digital Trust Department.

Note that the Digital Trust Department may request a conformity assessment of a PSDC at any time with the help of a CAB, at the sole discretion of the Digital Trust Department.

Also, PSDCs are obliged to inform the Digital Trust Department of any event, circumstance, or incident that may violate requirements of the Law of 25 July 2015 on electronic archiving or the Technical Regulation for digitization and e-archiving service providers.

4.3 Termination of the Supervision

Each PSDC may opt at any time for a reduction, a suspension, or a revocation of its PSDC status by notifying the Digital Trust Department. The List of PSDCs will then be updated accordingly and the changes will be communicated to the applicant.

A suspension of the PSDC status leads to the interdiction of using the designation "PSDC". Each voluntary suspension that lasts for longer than 18 months after the date of receiving the suspension notice by the Digital Trust Department will result in a withdrawal of the PSDC status.

5 Overview of the Technical Regulation for Digitization and E-Archiving Service Providers

In this chapter we will provide a more detailed overview of the Technical Regulation for a management system and security measures for digitization and e-archiving service providers [27], which introduces the technical conditions that must be observed for obtaining the status of PSDC. Recall that Article 3 of the Law of the 25 July 2015 on electronic archiving stipulates that the technical requirements for the digitization and e-archiving of documents will have to be specified in such a technical regulation.

The topics that are covered in this chapter include information security management systems and the ISO/IEC 2700x family of information security standards as the Technical Regulation for digitization and e-archiving service providers is formulated in the form of supplemental requirements to the ISO/IEC 27001 and ISO/IEC 27002 international standards.

We begin with an introduction to the ISO/IEC 27000 family of standards.

5.1 The ISO/IEC 27000 Family of Standards

In a nutshell, the goal of the ISO/IEC 27000 collection of standards is to ensure the security of information. The standards are generic in the sense that information assets that should be safeguarded can originate from an unlimited number of sources, such as financial data, health records, or personal details about employees. The ISO/IEC 27000 standards are therefore well-suited for guaranteeing the integrity and confidentiality of digitized documents and of electronic archives. All ISO/IEC 27000 standards are developed in a collaboration between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The notion of *Information Security Management System* (ISMS) is introduced in the ISO/IEC 27000 family of standards. According to ISO/IEC 27000:2018, an ISMS "consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets." An ISMS can be seen as a method for managing information in an organization in such a way that its security is ensured. For designing an ISMS, an organization needs to analyze all the risks that threaten information security and devise appropriate policies, procedures, and measures for reducing the likelihood of their occurrence or their impact on information security if they should materialize. Note that the deployment of an ISMS involves the implementation of security measures on IT equipment

as well as the participation of employees in the sense that specialized procedures have to be followed by them.

In the following we briefly present the following six members of the ISO/IEC 27000 family of standards, which are relevant in the context of electronic archiving:

- ISO/IEC 27000: "Information technology – Security techniques – Information security management systems – Overview and vocabulary" [23],
- ISO/IEC 27001: "Information technology – Security techniques – Information security management systems – Requirements" [14],
- ISO/IEC 27002: "Information technology – Security techniques – Code of practice for information security controls" [13],
- ISO/IEC 27003: "Information technology – Security techniques – Information security management system — Guidance" [22],
- ISO/IEC 27006: "Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems" [16], and
- ISO/IEC 27009: "Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements" [20].

We also refer the reader to [1] for additional information about the standards ISO/IEC 27000, 27001, and 27002.

5.2 ISO/IEC 27000

The standard ISO/IEC 27000:2018 introduces terms and definitions that are commonly used throughout the ISO/IEC 2700x standards and it gives an introduction to information security management systems. In particular, the principles & benefits of ISMS as well as the aspects of establishing, maintaining, and improving an ISMS are discussed. ISO/IEC 27000 concludes with an overview of the ISO/IEC 27000 collection of standards.

The latest version of the standard has been published in 2018, and it is available for download free of charge.[1]

5.3 ISO/IEC 27001

The goal of the ISO/IEC 27001:2013 standard is to provide guidelines that allow an organization to develop policies, processes, and procedures for preserving the confidentiality, integrity and availability of information. By following the ISO/IEC 27001 standard, an organization will be able to "establish, implement, maintain, and continually improve an information security management system" (ISMS) [14].

[1] Available from `http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html`

The standard mandates the use of the "Plan-Do-Check-Act" model for accomplishing information security goals.

"Plan:" The aim of the planning part is to design an ISMS that can achieve the information security goals. To that end, the organization is supposed to determine the intended scope of the ISMS and identify all internal and external issues that might affect the proper operation of the ISMS. The organization has to develop a risk assessment process that can identify all the risks that threaten the correct operation of the ISMS. For each identified risk one has (1) to assess the gravity of the consequences that will occur if the risk materializes and (2) to evaluate the likelihood of the occurrence of the risk. By combining these assessments, one can derive a "risk level" for each identified risk that expresses its harmfulness for the operation of the ISMS. At the same time, the organization has to define a risk acceptance level, which is a risk level that the organization deems acceptable. Risks that have a risk level that falls below the risk acceptance level do not require any further treatment. For risks that have been associated a risk level above the risk acceptance level, the organization will have to treat the risk, commonly by applying the measures that are described in Appendix A of ISO/IEC 27001, where they are called *controls*, to mitigate its consequences or the likelihood of its occurrence. Note that the organization is free to implement additional controls that are not contained in Appendix A. The choice of controls needs to be formalized in an information security risk treatment plan. For some risks, a viable alternative might be to purchase insurance to protect against their occurrence. The standard also mandates that the organization maintains a document called "Statement of Applicability", which lists all the controls that were implemented by the organization (i.e. controls from Annex A as well as supplemental controls not listed in Annex A) and the controls from Annex A that were excluded, together with justifications for doing so.

The standard also requires the management of the organization to provide sufficient resources to support the implementation and operation of the ISMS and to ensure that the employees have the necessary skills. Another requirement of ISO/IEC 27001 is that the organization adopts a document management system and that the organization maintains documented information on their processes, procedures, and the actions of employees.

"Do:" The implementation and the operation of the ISMS according to the planning phase are the focus of the "Do"-part. The standard mandates that all the processes and the risk treatment plan that were previously devised need to be implemented. Moreover, the organization needs to develop a procedure for handling (intentional or unintentional) changes to the ISMS. The assessment of information security risks needs to be reviewed at regular intervals, or whenever changes to the ISMS occur. As always, every action concerning the implementation of the ISMS and every review needs to be documented.

"Check:" The "Check"-part of the standard concerns the monitoring and the analysis of the operation of the ISMS, aiming at guaranteeing its adequacy & effectiveness. To that end, ISO/IEC 27001 mandates that the organization develops an internal audit program through which the organization itself assesses its conformity w.r.t. the

standard at regular intervals and monitors the performance of the ISMS w.r.t. internal performance criteria.[2] Another instrument that the standard requires is the management review. This review needs to be carried out by the top management at regular intervals with the aim of analyzing and endorsing all activities relating to the ISMS. For example, during the management review, updates to the assessment of risks or the results of internal audits need to be examined. Also, the top management is responsible for identifying opportunities for improvement and for taking decisions regarding modifications to the ISMS.

"Act:" Finally, the continual improvement of the ISMS for guaranteeing its future adequacy and effectiveness is addressed in the "Act"-part. One major aspect thereof is the reaction to nonconformities w.r.t. the standard. Whenever a nonconformity has been detected, the organization needs to analyze its root causes, identify the consequences and implement corrective actions. Also, the organization needs to make sure that such a nonconformity will not occur again.

5.4 ISO/IEC 27002

The ISO/IEC 27002:2013 standard aims to be a reference for organizations to choose controls when implementing an ISMS based on ISO/IEC 27001. Furthermore, the standard provides guidelines for implementing commonly used information security controls. In that way the standard can be helpful for organizations to develop their own strategies for information security management.

ISO/IEC 27002 considers 35 main security objectives that fall into 14 global categories (indicated as main clauses in the standard). For each security objective, several controls are listed that contribute to achieving the stated security objective. Overall, the standard describes 114 controls.

Security objectives that are covered in the standard range over human resource security, asset management, cryptography, communications security, supplier relationships, compliance, ...

The latest edition of the standard has been published in 2013.

5.5 ISO/IEC 27003

The standard ISO/IEC 27003:2017 intends to provide additional guidance on certain aspects of information security management systems as introduced in ISO/IEC 27001. The standard does not introduce any new requirements w.r.t. ISO/IEC 27001 or ISO/IEC 27002 and it aims at being suitable for organizations of all types and sizes. Organizations are also not obliged the follow the recommendations given in ISO/IEC 27003.

The aspects that are not covered in ISO/IEC 27003 relate to monitoring, measurement, analysis, and evaluation, as well as risk management, in the context of informa-

[2] Note that it is possible to mandate external auditors to carry out internal audits for the organization.

tion security. Detailed guidance concerning those aspects can be found in the standards ISO/IEC 27004 and ISO/IEC 27005.

The latest edition of ISO/IEC 27003 has been published in 2017.

5.6 ISO/IEC 27006

The standard ISO/IEC 27006:2015 can be seen as an extension of ISO/IEC 17021-1 to auditing and certifying ISMS based on ISO/IEC 27001.

ISO/IEC 17021-1 defines requirements for organizations that provide audits and certifications of management systems, e.g. conformity assessment bodies. ISO/IEC 27006 is intended to support the accreditation of organizations that provide certification services of ISMS according to ISO/IEC 27001.

For instance, ISO/IEC 27006 gives guidance regarding the avoidance of conflicts of interest to guarantee the impartiality of audits. Another aspect that ISO/IEC 27006 touches are skills & competences that auditors need to have, such as a familiarity with business management practices. Moreover, the standard imposes certain requirements regarding the documents that are issued after a successful audit for proving that an ISMS has been certified as compliant with ISO/IEC 27001.

The standard covers the whole certification life cycle from applying for a certification to planning and conducting audits. Requirements for the different audit stages (Stage 1 & 2) as well as for initial, surveillance, and recertification audits are also given in the standard. For instance, the standard mandates that organizations that are being audited need to give auditors access to all the documentation relating to the ISMS as otherwise the audit cannot be carried out. Moreover, Annex C of the standard details methods for determining the minimum duration of audits and Annex D aims at giving guidance for auditing the controls listed in Annex A of ISO/IEC 27001:2013.

Interestingly, ISO/IEC 27006 also recommends that certification bodies themselves operate an ISMS that is compliant with ISO/IEC 27001.

5.7 ISO/IEC 27009

The rather short standard ISO/IEC 27009:2016 gives guidelines for writing standards which are specializations of ISO/IEC 27001 or ISO/IEC 27002 that are applicable in specific areas. Examples of such standards include:

- ISO/IEC 27010:2015: Information security management for inter-sector and inter-organizational communications [18];
- ISO/IEC 27011:2016: Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations [21];
- ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services [19];

- ISO/IEC 27018:2014: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [15].

The standard ISO/IEC 27009 gives guidance on how to define requirements, guidelines, security objectives, or controls that complement the requirements and guidelines of ISO/IEC 27001 or the security objectives and controls of ISO/IEC 27002. In particular, ISO/IEC 27009 mandates that no such extension contradicts or weakens existing requirements, guidelines, or security controls from ISO/IEC 27001 and ISO/IEC 27002. The standard also contains a template for formulating such extensions of ISO/IEC 27001 and ISO/IEC 27002.

5.8 The Technical Regulation for Digitization or E-Archiving Service Providers

As we have seen above, the main legal context for e-archiving is defined in the Law of 25 July 2015 on electronic archiving [26]. The Technical Regulation for a management system and security measures for digitization and e-archiving service providers (in the following referred to as Technical Regulation) can be seen as a complement to the Law on electronic archiving in the sense that it defines the technical requirements that digitization or e-archiving service providers have to follow for obtaining the PSDC status. The Technical Regulation is published in an annex to a Grand-Ducal Regulation. At the time of writing, the latest edition of the Technical Regulation for PSDCs, version 3.1, has been published in the Annex II of the Grand-Ducal Regulation of 21 September 2017 [27].[3] The first edition appeared in the Grand-Ducal Regulation of 25 July 2015 [28]. In the following we only refer to version 3.1.

In line with ISO/IEC 27009:2016, the Technical Regulation is written as a sector-specific application of ISO/IEC 27001 and ISO/IEC 27002 to digitization or e-archiving services. Section 4 of the Technical Regulation lists additional requirements w.r.t. ISO/IEC 27001:2013 and Section 5 of the Technical Regulation describes supplementary controls, extending those of ISO/IEC 27002:2013.

Note that the Technical Regulation mandates that the trust services introduced in the eIDAS Regulation [2] are taken as a basis for establishing the security of information in the context of digitization and electronic archiving.[4]

One of the main goals of the Technical Regulation is to introduce the properties of **authenticity**, **trustworthiness**, and **operability** into the scope of the ISMS. Such an extended ISMS is then suitable for managing all the required properties of digitization or e-archiving services.

The Technical Regulation does not impose the implementation of a certain solution for digitization or electronic archiving. Instead, it introduces measures and it gives implementation guidelines that an organization needs to take into consideration for obtaining the PSDC status.

[3] Note that Annex II begins at page 88 in the PDF file available from `http://data.legilux.public.lu/eli/etat/leg/rgd/2017/09/21/a865/jo/fr/pdf`

[4] See, e.g., [8] for an introduction to the trust services defined by the eIDAS Regulation.

The Technical Regulation requires the use of cryptographic techniques to protect the integrity and trustworthiness of digitized documents and digital archives. In particular, the Technical Regulation recommends the deployment of qualified trust services as defined in the eIDAS Regulation.

The cryptographic techniques that the Technical Regulation advocates include:

- authentication based on cryptographic mechanisms,
- computation of cryptographic hashes of digitized documents and digital archives,
- validation and approval of internal documents (like activity reports) with the help of qualified digital signatures,
- qualified timestamping of log files,
- digital signing of documents that are sent to clients, and
- secure transfer of documents with the help of cryptographic techniques.

One important paradigm that the Technical Regulation advocates is the **traceability** of every action that affects the digitization or e-archiving systems. In particular, the Technical Regulation requires PSDCs to create, manage, and store a certain number of reports:

(1) reports concerning administration activities,

(2) reports concerning operational activities,

(3) security reports,

(4) activity reports concerning the users of the digitization or e-archiving systems,

(5) reports concerning software updates,

(6) reports concerning changes to the digitization or e-archiving systems,

(7) reports concerning events and incidents in connection with the digitization or e-archiving processes,

(8) reports concerning the review of event logs relating to the digitization or e-archiving systems,

(9) delivery receipts of analog documents that should be digitized,

(10) collection receipts of analog documents after digitization,

(11) conversion reports concerning the transformation of digital documents into digital archives,

(12) conversion reports for format conversions of digital archives.

In the following we will provide a detailed description of the different clauses contained in the Technical Regulation.

Section 3 of the Technical Regulation introduces the terms and definitions that will be used throughout the document.

Section 4 lists additional requirements w.r.t. ISO/IEC 27001:2013 that are specific to the digitization or e-archiving context. Note that the numbering of the subsections in Section 4 and in Section 5 is not linear as these subsections introduce additional requirements w.r.t. ISO/IEC 27001:2013 and ISO/IEC 27002:2013, respectively. Consequently, they have been assigned numbers that are not used in ISO/IEC 27001:2013 and in ISO/IEC 27002:2013.

Section 4.2.4.0 and 4.2.4.3 requires an organization to run a management system for the processes of digitization or of e-archiving that is integrated into an ISMS (or that follows the same requirements) to ensure

- the correct operation of the processes relating to digitization or e-archiving,
- the financial stability of the organization, and
- the ability of the organization to fulfill its contractual, legal, and regulatory responsibilities relating to the processes of digitization or e-archiving.

When determining the scope of the ISMS, the organization needs to take the digitization or e-archiving process itself, the type of documents, and the type of clients into account.

In addition to the basic security properties of confidentiality, integrity, and availability, Section 4.2.4.5 adds the properties of **authenticity**, **trustworthiness**, and **operability** into the scope of the ISMS.

The Technical Regulation defines the aforementioned properties as follows. For authenticity (often considered as a particular aspect of integrity), the organization needs to be able to prove that every activity carried out in the context of digitization or e-archiving is genuine, i.e.

- analog or digital documents have been transmitted by the person that is supposed to have transmitted them;
- digital documents resulting from digitization or digital archives have been created by a person or by the archiving system at the presumed moment;
- digital documents or archived documents are what they are supposed to be.

Regarding trustworthiness, the organization needs to be able to demonstrate that every activity carried out in the context of digitization or e-archiving is **trustworthy**. More precisely,

- every activity needs to be carried out according to the established policies and procedures;

- every digital document or archive that has been created or stored is an identical reproduction of the original and no unauthorized modification has been made to it.

To ensure operability, the organization needs to be able to demonstrate that the execution of the process of digitization or e-archiving only creates digital documents or digital archives that are, at any time, easy to find, readable, intelligible, fit for purpose in combination with the metadata that allows for tracing their origins, and available for as long as necessary.

Regarding further requirements on leadership, in Section 4.2.5.4 the Technical Regulation stipulates that the management of the organization needs to ensure that the responsibilities and tasks of the roles concerned by the digitization or e-archiving processes are fully assigned to staff members. The Technical Regulation lays particular emphasis on the roles for managing risks that affect the financial stability of the organization, the ability to fulfill its contractual, legal, and regulatory responsibilities relating to the processes of digitization or e-archiving, and the ability to continue executing the processes of digitization or e-archiving during a transition phase, when the organization ceases offering PSDC services.

Similarly, Section 4.2.5.5 refers to management actions in connection with the digitization or e-archiving processes. In particular, the management of the organization needs to provide proof of a stable financial situation to satisfy the expectations of all the parties concerned by PSDC activities. Furthermore, the management must provide a guarantee that it is possible to continue executing the digitization or e-archiving processes at least during a transition phase to ensure the complete transfer of PSDC activities whenever necessary (in particular, if the organization does not provide digitization or e-archiving services internally only).

Section 4.2.6 deals with the planning of the ISMS. The Technical Regulation adds the requirements to take the digitization or e-archiving processes into consideration during the risk analysis. The risks that may affect the financial stability of the organization or its ability to fulfill its contractual, legal, and regulatory responsibilities relating to these processes should be integrated into the risk analysis. Additionally, the Technical Regulation requires the organization to take the security objectives and measures introduced in Annex A of the Technical Regulation into consideration for the risk analysis (verify, in particular, that all the necessary measures have been included) and to make the Statement of Applicability available to clients and to ILNAS.

Section 4.2.7.4 extends the need for awareness and training of employees to include their responsibilities w.r.t. the digitization and e-archiving processes and the legal requirements regarding the Law on electronic archiving in the Grand Duchy of Luxembourg.

In Section 4.2.7.5.4 the Technical Regulation mandates that the organization sets up a record management system (which is protected from unauthorized modifications) to prove that it has respected the information security properties developed in Section 4.2.4.5 of the Technical Regulation. The term “record“ refers to all kinds of documents necessary for demonstrating that the ISMS is operating correctly.

Section 4.2.8.4 requires that the management of the organization must be involved in the risk analysis & treatment process. The involvement of the management needs to be documented in writing.

Section 4.2.9.1 stipulates that the organization must evaluate the performance of its management system for the digitization or e-archiving processes analogously to the performance evaluation of an ISMS. Similarly, Section 4.2.9.2 demands that the organization includes the digitization or e-archiving processes into the internal audit program.

Section 4.2.9.3 extends the necessity of management reviews to the management system of the digitization or e-archiving processes.

Finally, Section 4.2.10.2 extends the requirements for continually improving the appropriateness, adequacy, effectiveness of an ISMS to the management system of the digitization or e-archiving processes.

In the following we describe the security objectives, measures, and recommendations defined in Section 5.2 of the Technical Regulation. In line with ISO/IEC 27002, the Technical Regulation introduces new security objectives that are accompanied by measures for achieving the objectives. Recommendations for implementing the aforementioned measures may be given in the Technical Regulation as well.

5.9 Information Security Policies

Section 5.2 of the Technical Regulation introduces a new security objective aiming at ensuring management support for the digitization or e-archiving processes to follow best industry practices and all applicable legal requirements. The Technical Regulation introduces two security measures to support the aforementioned security objective.

A first measure recommends the introduction of a "digitization or e-archiving policy" that has to be approved by the management of the organization, applied throughout the organization, distributed and communicated to the employees and affected third parties. The digitization or e-archiving policy should contain a description of the processes that relate to digitization or e-archiving and their technical implementation. Other aspects that should be covered in the digitization or e-archiving policy include the roles and responsibilities in the organization connected to the digitization or e-archiving processes and the information security and documentation management principles that apply to those processes. A second measure recommends that the digitization or e-archiving policy is reviewed at regular intervals, and whenever major changes occur, to guarantee its appropriateness, adequacy, and effectiveness.

5.10 Organization of the Security of Information and of the Digitization or E-Archiving Processes

In Section 5.6 the Technical Regulation defines a new security objective concerning the introduction of an organizational framework for initiating and supervising the

correct operation of the digitization or e-archiving processes and the achievement of information security aims. A first security measure in the Technical Regulation recommends to define all responsibilities regarding information security, the execution of the digitization or e-archiving processes, and the supervision of the implementation of all applicable policies and procedures. These responsibilities should then be assigned to staff members. A second security measure concerns the segregation of duties. For instance, the Technical Regulation recommends that employees who have been tasked with roles and responsibilities concerning the operation of the digitization or e-archiving services do not review the effectiveness of the execution of these roles and responsibilities. The segregation of duties should also be extended to user accounts. For example, only operators should be allowed to modify the contents of digital archives. System administrators either must not be able to modify the digital archives at all, or all of their activities must be monitored. A third security measure recommends that the management procedures regarding the digitization or e-archiving systems have to be set out in writing and approved during the initiation phase of new digitization or e-archiving projects.

The Technical Regulation also defines a new security objective of establishing a management framework for guaranteeing that the specific legal requirements for the digitization & e-archiving processes are respected by the organization. For this objective, the Technical Regulation proposes four security measures. A first measure concerns the verification of digital documents after digitization. Such a verification can, for instance, be carried out by comparing the number of pages that were fed to the scanner with the number of pages contained in the scanned document, or by verifying whether the scanned document is indeed identical to the original paper document. Another security measure that is recommended by the Technical Regulation is the dual control principle regarding the manipulation of electronic archives. Every modification or deletion of documents that was not initially planned needs to be approved by two users that have the right to perform such actions. A third measure relates to the management of records. The organization should develop and apply a procedure for managing the records that relate to the correct operation of the digitization or e-archiving systems and to the activities of the employees. In particular, the organization should ensure that the integrity of the digitization or e-archiving systems and of the electronic archives is verified at regular intervals and whenever significant changes have occurred. A fourth measure that the Technical Regulation advocates concerns the communication with national authorities, in particular ILNAS. The organization should set up procedures to notify planned and significant changes to the competent authorities, in particular ILNAS: e.g., changes on the management level of the organization, modifications to the digitization or e-archiving systems, or changes to activities carried out by subcontractors that affect the digitization or e-archiving processes. Moreover, the organization needs to inform the competent authorities about every attempted, or successful, information security breach and every loss of integrity that could have a significant impact on the digitization or e-archiving services within 24 hours after having become aware of the incident.

Section 5.6.4 introduces a security objective which aims to clarify the responsibil-

ities between digitization or e-archiving service providers and their clients, and to ensure transparency concerning the security of information and the digitization and e-archiving processes.

A first measure concerns security aspects in contractual relationships with clients. The conditions that govern the execution of the digitization or e-archiving processes as well as the required security guarantees need to be defined in a written document that is approved by the PSDC and its client.

Such a document should contain detailed descriptions of

- the digitization or e-archiving project,
- the service level associated with the digitization or e-archiving services,
- the management of organizational and technical changes,
- the roles and responsibilities of the client and the organization,
- contact information of the client and of the organization, etc.

It is also recommended that the customer maintains a list of persons that are authorized

- to deliver and collect analog documents,
- to access the digital documents resulting from digitization or the digital archives,
- to use the digitization or e-archiving systems,
- to request the destruction of analog documents, digital documents resulting from digitization, or digital archives.

Another measure concerns the necessity of providing clients with a sufficient amount of information before entering any contractual relationship, in particular mandatory legal information for guaranteeing the transparency of the provided services. For instance, the Technical Regulation recommends that a PSDC provides the following pieces of information before entering into a contractual relationship with a client:

- the procedure that is followed for digitization or e-archiving,
- the procedure that is followed for producing digital copies with probative value in a readable form while guaranteeing their faithfulness to the originals,
- the terms and conditions governing subcontractors,
- the legal requirements that a PSDC needs to follow,
- the contractual obligations that govern the provision of services, including the limits of responsibilities,
- the standards and procedures, together with essential technical characteristics of the systems used for providing the services.

It is recommended to include the following aspects in the description of the operational procedure (as applicable):

- the collection of analog documents,
- the collection of digital documents,
- the temporary storage of digitized documents,
- the creation and storage of digital archives,
- the restoration, transfer, and deletion of digital archives.

If a maximum retention period has been defined for digital archives, the client should be informed before a scheduled deletion takes place. Otherwise, the client's authorization will be needed before a digital archive can be deleted.

A further measure concerns the classification of the client's assets. Clients should define the security classification level, the maximum retention period, and any other potential security requirements, like special access rights, for their documents.

A last measure advises that organizations should inform clients about incidents or about planned changes to any previously communicated information or to contractual obligations. In particular, clients need to be informed in the following cases without any undue delay:

- whenever an incident occurs that may affect the documents of a client, or the digitization or e-archiving services used by the client,
- whenever an attempt at accessing a client's documents using the client's credentials is detected outside of the usual connection times, e.g., outside of office hours.

Moreover, format conversions of digital archives should only be carried out after having received written approval by the concerned clients. Clients should also be informed about any potential consequences when the digitization or e-archiving service provider changes its appreciation of risks.

5.11 Security Aspects concerning Human Resources

Section 5.7 introduces a security measure that concerns security aspects in connection with human resources. The Technical Regulation advises that the staff members of the digitization or e-archiving service provider or of its subcontractors involved in the digitization or e-archiving services understand and agree in writing to respect the digitization or e-archiving policy. In particular, staff members need to be informed about their roles and responsibilities, and they should participate in training sessions concerning all relevant aspects of the digitization or e-archiving services.

5.12 Asset Management

The aim of Section 5.8 is to introduce additional implementation guidance and security measures for clarifying responsibilities relating to the organization's assets.

Regarding the inventory of assets, the Technical Regulation advises to take the different components of the digitization or e-archiving services into consideration. Concerning the ownership of assets, it is recommended that asset owners evaluate and approve the operational aspects of the digitization or e-archiving systems at least once per year and after significant changes have been made to them. Moreover, the asset owners should review the descriptions of the digitization or e-archiving systems at regular intervals (at least once per year) and after significant changes have been made.

The Technical Regulation introduces an additional security measure regarding the encapsulation of confidential or personal information. The digitization or e-archiving service provider should take care of encapsulating confidential or personal information to guarantee that such information can be deleted at the owner's request without interfering with the digital archives or the records & metadata relating to the digital archives.

Most importantly, to ensure compliance with the General Data Protection Regulation (GDPR) (EU) 2016/679 (i.e. the right to be forgotten), the digitization or e-archiving service provider must refrain from storing personal information in metadata that relate to the traceability of manipulations involving the digitization or e-archiving systems.

Regarding the classification of information, the Technical Regulation recommends that the requirements concerning authenticity, trustworthiness, and operability have to be taken into consideration for defining and assigning classification levels to assets. For instance, the criterion "trustworthiness" may imply that certain scanner settings (color vs. black & white, color encoding, resolution) are always applied during the digitization of analog documents. The criterion "integrity" may be used to include the requirements connected to authenticity, and the criterion "availability" may encompass the requirements related to operability.

The Technical Regulation gives additional guidance concerning the disposal of media. It is recommended that analog documents, data storage equipment, and client data are destroyed in a secure way. Moreover, the effectiveness of the destruction or deletion mechanisms should be evaluated by a third party.

5.13 Access Control

Section 5.9 provides further guidance on aspects of access control. An additional security measure recommends that three different persons are implicated in the management of access rights:

- one person needs to authorize that the requested access will be given to an applicant,

- a second person has to verify whether all the security requirements relating to the requested access have been respected, and
- a third person finally grants the requested access on the IT infrastructure.

5.14 Cryptography

Section 5.10 introduces implementation guidance and security measures relating to cryptography. The Technical Regulation advises to make use of the qualified trust services defined in the eIDAS Regulation [2] to ensure the security of digitized documents and of digital archives. The Technical Regulation also refers to ETSI TS 102 176-1 for a list of cryptographic algorithms and their recommended maximum usage periods.

Every person that can access the digitization or e-archiving systems should authenticate herself using cryptographic mechanisms, e.g., smart cards that contain digital certificates suitable for authentication or physical authentication devices. Two-factor authentication should also be used, which may be based on biometric authentication techniques. The components of the digitization or e-archiving systems should employ measures like IP address filtering or cryptographic techniques (for example, SSL certificates) to secure the communication links between them.

The Technical Regulation recommends to protect the integrity of digital documents with the help of appropriate cryptographic means. It is advisable that a cryptographic hash value is calculated of every digital document that is created by digitization. The hash values should also be transmitted to clients in a secure way. The integrity of the digitized documents that were received by the client can then be verified by first recalculating the hash values of the received documents and subsequently comparing them with the hash values that were transmitted to the client by the digitization or e-archiving service provider.

The integrity of internal documents relating to the digitization or e-archiving systems, in particular of event logs, should also be protected with the help of cryptographic techniques. The Technical Regulation suggests to implement a scheme for linking log entries among each other. For example, log entries can be grouped chronologically into blocks, and for each of these blocks, a hash value can be calculated over the log entries contained in the block and over the hash value for the previous block. By storing (some of) the hash values in a secure way, one can easily detect whether log entries were modified. Moreover, qualified timestamps should be applied on log files (e.g., once per day).

The Technical Regulation recommends that users of the digitization or e-archiving systems validate the internal documents used for proving that the digitization or e-archiving systems operate correctly with the help of qualified digital signatures (or mechanisms that offer similar guarantees).

Users of the e-archiving systems should electronically sign reports concerning activities relating to administration, information security, and the operation of the digitization or e-archiving systems with the help of qualified signature creation devices to

ensure the authenticity of the activities that were carried out. Similarly, digital documents that are to be sent to clients or authorities should also be signed with the help of qualified signature creation devices by a member of staff to ensure the authenticity of the transmitted documents.

The qualified signature creation device and the associated qualified certificate for electronic signatures should be compliant with the respective EU regulations, in particular the eIDAS Regulation. Digital signature formats like CAdES [5], XAdES [4], and PAdES [3] should be used to maintain the long-term validity of the signatures.

The transmission of information and of digital documents should be protected by appropriate cryptographic means. Secure transmission protocols like SFTP, TLS, PPP, L2TP, IPSEC, ...) should be used to protect the transmission of information internally and externally.

If the integrity of a digital document that is to be archived is based on a digital signature, it is recommended to archive the document along with proof that the validity of the digital signature has been verified at the moment of archiving, at the latest.

The integrity of a digital archive should be demonstrated by showing that

- at the time of archiving the qualified electronic signature & the associated qualified certificate for electronic signatures was valid, and the certificate was issued by a qualified trust service provider;
- the electronic archiving system maintains the integrity of the digital archives for as long as necessary.

Several techniques exist for proving that a qualified certificate for electronic signatures is valid. For instance, it is possible to

- use the online certificate status protocol (OCSP) of the certification authority that issued the qualified certificate, or
- timestamp activity reports and download the certificate revocation list published by the certification authority that issued the qualified certificate.

5.15 Physical and Environmental Security

Section 5.11 lists additional implementation guidance and security measures concerning physical and environmental security. The Technical Regulation recommends that visitors are accompanied at all times by at least one member of staff who is authorized to do so. Visitors should be prevented from having access to the confidential information of clients and they should not have access to areas reserved for digitization, especially if digitization activities take place. Similarly, third parties that are authorized to enter secured areas should be under supervision at all times whenever they access the digitization or e-archiving systems. Moreover, the technical assets of the digitization or e-archiving systems should be protected against unauthorized access if the areas in which such systems are located have to be evacuated or if the areas are used for other activities.

5.16 Security of Operations

In Section 5.12 the Technical Regulation introduces additional implementation guidance and security measures concerning the security of operations. It is recommended to devise and implement procedures that concern the administration and operation of the digitization or e-archiving processes and systems such that the properties of confidentiality, integrity, availability, authenticity, trustworthiness, and operability can be guaranteed. The procedures should cover all the relevant aspects relating to the digitization or e-archiving systems: access rights, system configurations, operating instructions, surveillance mechanisms, log management, cryptographic measures, malware detection, destruction mechanisms for documents, disposal of equipment, backup management, disaster recovery, change management, incident management, technical asset management (including technical support services provided by suppliers), third-party support, metadata management, and mechanisms for verifying the correctness of the digitization activities.

The Technical Regulation also recommends to log every event that occurs in connection with the digitization or e-archiving services, such as system events or errors related to the manipulation of analog or digital documents. Moreover, it is also advisable to log every user activity, in particular

- connection attempts outside of regular office hours,
- activities of users that were carried out quicker than usual, and
- duplications of user sessions.

Concerning clock synchronization, the Technical Regulation recommends that the clocks used in digitization or e-archiving systems are kept synchronized with a trusted source of time and that synchronization events are logged for as long as necessary. Additionally, the synchronization with a master clock needs to be carried out frequently to ensure that the clock drift remains below one second. Higher drifts need to be detected as soon as possible to allow corrective measures to be taken. Timestamps should also be created during the operation of the digitization or e-archiving systems to verify the accuracy of the clocks.

It is advisable to store log files in such a way that they are protected against all kinds of manipulations (including unauthorized deletions). Moreover, log files should be stored on long-term storage media.

Another security objective that is introduced by the Technical Regulation concerns the correct and secure handling of analog & digital documents as well as of digital archives. As an additional security measure, it is advisable that the organization demonstrates that the implemented security mechanisms correspond to the needs of the clients and that they allow to ensure the authenticity, trustworthiness, and operability of the documents created and managed by the digitization or e-archiving systems.

The Technical Regulation recommends to define and maintain an exhaustive description of the digitization or e-archiving systems that details the technical assets

as well as all relevant operational aspects and the dependencies between the system components. For instance, such a description should document the technical assets that are used for:

- the collection of analog or digital documents,
- the temporary storage of such documents,
- the digitization of analog documents or the creation of digital archives,
- the restoration, transfer, deletion of digital archives, as well as the destruction of analog documents.

Furthermore, the following operational aspects should be documented, for example:

- for the digitization systems
  - the minimum and maximum number of colors, and the gray scale resolution,
  - the minimum and maximum DPI settings for scanning,
  - the settings regarding single-sided or double-sided digitization,
  - permitted paper sizes (A3, A4, A5, ...),
  - image correction methods,
  - image compression methods,
  - the maximum number of documents that can be digitized within a given time period,
- for the e-archiving systems
  - the maximum number or the maximum size of digital documents that can be archived in one batch,
  - the data transmission rate,
  - response times,
  - the supported batch archiving or restoration frequency,
  - supported secure transmission protocols (like SFTP, TLS, L2TP, IPsec)

Finally, technical aspects such as the network architecture, the flow of data between assets, and the dependencies between assets should be documented in the form of diagrams.

The Technical Regulation recommends that the organization is able to prove that the digitization or e-archiving systems and the security mechanisms satisfy the needs of the clients and that they can guarantee the authenticity, the trustworthiness, and the operability of documents. To that end, the following security mechanisms should be set up:

- mechanisms for managing access rights: e.g., access rights need to be revocable immediately and every user action must be uniquely traceable to a single user,

- mechanisms for managing access privileges,
- surveillance mechanisms,
- cryptographic security techniques,
- mechanisms for the detection and deletion of malicious code contained in documents that are to be archived,
- secure deletion mechanisms for digital documents,
- format conversion mechanisms that can be applied to archived documents.

The Technical Regulation also recommends to continually supervise the operational aspects of the digitization or e-archiving systems, such as available disk space and the failure rate of redundant components.

It is also advisable to implement mechanisms for regularly checking the integrity of the digitization or e-archiving systems and of the information required for ensuring traceability. For example, one has to verify that

- the mode of operation of the digitization or e-archiving systems has not been modified due to maintenance work, system updates, or due to the replacement or the repair of (components of) assets, like scanners or storage media,
- configuration files have not been modified,
- the integrity of stored digitized documents, digital archives & associated metadata, or log files has not been compromised.

5.17 Acquisition, Development, and Maintenance of Information Systems

The Technical Regulation also recommends to ensure that mission-critical software and the digitization or e-archiving systems are developed following recognized methodologies for designing and writing secure software systems. In particular, it is recommended to set up a source code escrow agreement for every software system developed by a third party that is required for ensuring the integrity and availability of information stored in the digitization or e-archiving systems.

5.18 Relationships with Suppliers

Section 5.15 introduces an additional security measure concerning the relationships with suppliers. The Technical Regulation recommends to include conditions that guarantee the respect of the security policy and the digitization or e-archiving policies into the contracts established with suppliers that participate in the digitization or e-archiving services. For instance, such contracts should address the issues of

- ownership concerning the products and services provided by the supplier, such as, e.g., documents or software,
- business continuity, especially in the case of a disaster,
- respecting the digitization or e-archiving policy,
- establishing measures to ensure that
  - the organization is informed without any undue delay about changes made to assets owned by suppliers,
  - the confidentiality of information is respected, and
  - all changes planned to be made by suppliers that may affect the digitization or e-archiving services need to be approved first,
- receiving the support from suppliers in investigations concerning incidents that affect digitization or e-archiving services,
- having the right to audit suppliers,
- ensuring the conformity of the supplier (and of its suppliers) with all applicable laws and regulations, and
- specifying contact persons for each contract party.

5.19 Management of Information Security Incidents

Section 5.16 introduces implementation guidance concerning the handling of information security incidents: a procedure should be devised that defines when the incident management procedure should be activated, the restoring of data should be started, and clients & authorities should be informed about an incident that has taken place.

5.20 Information Security Aspects of Business Continuity Management

Section 5.17 defines a new security objective which aims at ensuring the continuity of the business operations concerning the digitization or e-archiving services.

A first security measure recommends to determine the requirements for guaranteeing the continuity of the digitization or e-archiving processes in an adverse situation, like a crisis or an accident. To that end, it is first advisable to identify the maximum Return Time on Objective (RTO) and the Recovery Point Objective (RPO) while taking the clients' requirements and the obligation to return the documents that were stored at the organization into account. The RTO is generally defined as the duration of time during which a service or process must be operational again after a disaster has occurred. The notion of RPO is linked to the prevention of unacceptable data loss

in the sense that it is defined as the time interval that might elapse after an incident before the loss of data exceeds a given limit (for more details, see e.g. [6]). For instance, if the RPO is set to twelve hours, then the loss of the data produced during the last twelve hours can be tolerated, at most. Data backups that are at most twelve hours old must be available at all times. The Technical Regulation also refers the reader to the standard ISO 22301:2014 [10] for additional guidance.

Additionally, the digitization or e-archiving service provider is advised to establish, document, implement, and maintain processes, procedures, and measures for ensuring the required level of business continuity during an adverse situation. A disaster recovery process that includes the digitization or e-archiving processes should be defined, taking the requirements of the clients, the legal obligations to return the documents of the clients, and high-risk scenarios that might affect the proper functioning of a business activity into account.

Finally, the Technical Regulation also advocates to regularly verify the measures relating to business continuity to ensure their ongoing validity. The key elements of the continuity and recovery plans should also be tested.

5.21 Compliance

Section 5.18 describes additional security measures and implementation guidance concerning information security reviews and the compliance of digitization or e-archiving service providers with legal and regulatory requirements.

It is recommended to store the records for proving that the activities carried out by members of staff were compliant with the digitization or e-archiving policies and procedures for as long as necessary on appropriate storage media. In particular, the following records should be kept:

- activity reports of the users of the digitization or e-archiving systems,
- update or change reports relating to the digitization or e-archiving systems,
- event and incident reports connected to the digitization or e-archiving processes,
- reports of event log reviews for the digitization or e-archiving systems,
- delivery receipts or collection receipts of analog documents for the digitization processes,
- conversion reports relating to the transformation of digital documents into digital archives, or conversion reports concerning format conversions of digital archives.

Furthermore, it is advisable that records of user activities contain the following pieces of information:

- the person that carried out an activity,
- the date & time when the activity took place,

- the location where the activity took place,
- assets used during the activity,
- assets targeted by the activity,
- a description of the activity,
- problems or errors encountered during the activity,
- affected clients.

It is recommended to conduct internal audits of the digitization or e-archiving systems and of the actions carried out by staff members to assess their conformity w.r.t. applicable laws, regulations, and the policies & procedures that govern security aspects and digitization or e-archiving activities. In particular, through sampling, such an evaluation should ensure that

- the collected analog documents have been correctly transformed into digital documents, and that they were subsequently destroyed or returned to the respective owners,
- the digitized documents have been correctly stored, returned, or entered into the electronic archiving process,
- the collected digital documents have been correctly transformed into digital archives and subsequently destroyed,
- the digital archives have been correctly created, stored, returned, transferred, or deleted, and
- the administrative procedures, operational procedures, and security procedures have been respected.

Moreover, internal audits should also verify that the technical assets of the digitization or e-archiving systems and the security mechanisms, e.g., the cryptographic instruments, have either been evaluated and certified by independent organizations specialized in such evaluations, or that they are compliant with recognized standards and that they are used according to recommended practices.

It is recommended in the Technical Regulation to conduct technical audits of the digitization or e-archiving systems to verify the correct operation of the security mechanisms indicated in the description of the digitization or e-archiving systems and to assess whether the digitization or e-archiving systems are protected at an appropriate level of security. Such technical audits should include penetration tests and privilege escalation tests carried out by auditors that are experienced in such tests.

The Technical Regulation also refers to the standard ISO/IEC 27007 [12] and to the technical report ISO/IEC 27008 [11] for additional guidance on auditing information security management systems.

6 Conclusion

In this document we provided an overview of the e-archiving framework that has been set up in the Grand Duchy of Luxembourg, aiming at

(1) providing an introduction to the topic for readers who are unfamiliar with the legal context relating to e-archiving in Luxembourg, and

(2) giving guidance to organizations that plan to provide digitization or e-archiving services.

In particular, we briefly described the most important articles of the Law of 25 July 2015 on electronic archiving, which introduces the legal status of *prestataire de services de dématérialisation ou de conservation* (PSDC), i.e. "digitization or e-archiving service provider" in English. As we saw before, ILNAS is the only government agency authorized to grant the status of PSDC to organizations. We also explained the procedure that is followed by the Digital Trust Department of ILNAS regarding the supervision of digitization or e-archiving service providers.

Subsequently, we presented a detailed overview of the Technical Regulation for a management system and security measures for digitization or e-archiving service providers, which introduces the technical conditions that must be observed for obtaining the PSDC status. To that end, we also introduced information security management systems and the ISO/IEC 2700x family of information security standards as the Technical Regulation can be seen as a supplement to the ISO/IEC 27001 and ISO/IEC 27002 standards.

Bibliography

[1] Georg Disterer. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4(2), 2013.

[2] European Parliament, Council of the European Union. Regulation EU No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. *OJ*, L 257:73–114, 2014. Available from `http://eur-lex.europa.eu/eli/reg/2014/910/oj`.

[3] European Telecommunications Standards Institute. *ETSI TS 102 778-1 V1.1.1 (2009-07) Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a Framework Document for PAdES*. France, 2009.

[4] European Telecommunications Standards Institute. *ETSI TS 101 903 V1.4.2 (2010-12) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)*. France, 2010.

[5] European Telecommunications Standards Institute. *ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*. France, 2013.

[6] Andrew Hiles. *The Definitive Handbook of Business Continuity Management*. John Wiley & Sons, Inc., New Jersey, USA, 2015.

[7] ILNAS. List of PSDCs. Available from `https://portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique/liste-psdc.html`.

[8] ILNAS. Trust Services under the eIDAS Regulation. Available from `https://portail-qualite.public.lu/fr/publications.html`.

[9] ILNAS – Digital Trust Department. ILNAS/PSDC/Pr001 – Supervision of Digitisation or E-Archiving Service Providers (PSDCs). Available from `https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/confiance-numerique/surveillance-psc/procedures/ilnas-pscq-pr001-supervision-en/ilnas-pscq-pr001-supervision-en.pdf`.

[10] ISO. *ISO 22301:2012: Societal Security – Business Continuity Management Systems — Requirements*. International Organization for Standardization, Geneva, Switzerland, 2012.

[11] ISO/IEC. *ISO/IEC 27008:2011: Information Technology – Security Techniques – Guidelines for Auditors on Information Security Controls*. International Organization for Standardization, Geneva, Switzerland, 2011.

[12] ISO/IEC. *ISO/IEC 27007:2017: Information Technology – Security Techniques – Guidelines for Information Security Management Systems Auditing*. International Organization for Standardization, Geneva, Switzerland, 2017.

[13] ISO/IEC. *ISO/IEC 27002:2013 — Information Technology — Security Techniques — Code of Practice for Information Security Controls*. International Organization for Standardization, Geneva, Switzerland, 2013.

[14] ISO/IEC. *ISO/IEC 27001:2013: Information Technology — Security Techniques — Information Security Management Systems — Requirements*. International Organization for Standardization, Geneva, Switzerland, 2013.

[15] ISO/IEC. *ISO/IEC 27018:2014: Information Technology — Security Techniques — Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds acting as PII Processors*. International Organization for Standardization, Geneva, Switzerland, 2014.

[16] ISO/IEC. *ISO/IEC 27006:2015 — Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*. International Organization for Standardization, Geneva, Switzerland, 2015.

[17] ISO/IEC. *ISO/IEC 17021-1:2015: Conformity Assessment — Requirements for Bodies Providing Audit and Certification of Management Systems — Part 1: Requirements*. International Organization for Standardization, Geneva, Switzerland, 2015.

[18] ISO/IEC. *ISO/IEC 27010:2015: Information Technology — Security Techniques — Information Security Management for Inter-sector and Inter-organizational Communications*. International Organization for Standardization, Geneva, Switzerland, 2015.

[19] ISO/IEC. *ISO/IEC 27017:2015: Information Technology — Security Techniques — Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services*. International Organization for Standardization, Geneva, Switzerland, 2015.

[20] ISO/IEC. *ISO/IEC 27009:2016: Information Technology — Security Techniques — Sector-Specific Application of ISO/IEC 27001 — Requirements*. International Organization for Standardization, Geneva, Switzerland, 2016.

[21] ISO/IEC. *ISO/IEC 27011:2016: Information Technology — Security Techniques — Code of Practice for Information Security Controls based on ISO/IEC 27002 for Telecommunications Organizations*. International Organization for Standardization, Geneva, Switzerland, 2016.

[22] ISO/IEC. *ISO/IEC 27003:2017 — Information Technology — Security Techniques — Information Security Management System — Guidance*. International Organization for Standardization, Geneva, Switzerland, 2017.

[23] ISO/IEC. *ISO/IEC 27000:2018: Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*. International Organization for Standardization, Geneva, Switzerland, 2018.

[24] Legilux. Loi du 5 avril 1993 relative au secteur financier, April 1993. Available from `http://data.legilux.public.lu/eli/etat/leg/loi/1993/04/05/n1/jo`.

[25] Legilux. Loi du 4 juillet 2014 portant réorganisation de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services et portant organisation du cadre général pour la surveillance du marché dans le contexte de la commercialisation des produits, July 2014. Available from `http://legilux.public.lu/eli/etat/leg/loi/2014/07/04/n2/jo`.

[26] Legilux. Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification: 1. de l'article 1334 du code civil; 2. de l'article 16 du code de commerce; 3. de la loi modifiée du 5 avril 1993 relative au secteur financier, August 2015. Available from `http://legilux.public.lu/eli/etat/leg/loi/2015/07/25/n1/jo`.

[27] Legilux. Règlement grand-ducal du 21 septembre 2017 modifiant le règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique, August 2015. Available from `http://legilux.public.lu/eli/etat/leg/rgd/2017/09/21/a865/jo`.

[28] Legilux. Règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er de la loi du 25 juillet 2015 relative à l'archivage électronique, July 2015. Available from `http://legilux.public.lu/eli/etat/leg/rgd/2015/07/25/n1/jo`.

Index

June 2018 · The Electronic Archiving Framework in Luxembourg · V1.0 · © ILNAS

ILNAS
Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -50 · Fax : (+352) 24 79 43 -50 · E-mail : confiance-numerique@ilnas.etat.lu

www.portail-qualite.lu