This consolidated text was drawn up by the CSSF for information purposes only. In case of discrepancies between the French and the English consolidated texts, the texts published in the Journal officiel du Grand-Duché de Luxembourg are the sole authoritative and universally valid versions.

Grand-ducal Regulation of 25 July 2015 implementing Article 4(1) of the Law of 25 July 2015 on e-archiving.

(Mém. A 2015, No 150)

as amended by:

- the Grand-ducal Regulation of 22 May 2017 amending the Grand-ducal Regulation of 25 July 2015 implementing Article 4(1) of the Law of 25 July 2015 on e-archiving;
  (Mém. A 2017, No 563)
- the Grand-ducal Regulation of 21 September 2017 amending the Grand-ducal Regulation of 25 July 2015 implementing Article 4(1) of the Law of 25 July 2015 on e-archiving;
  (Mém. A 2017, No 865)
- the Grand-ducal Regulation of 7 August 2023 amending the Grand-ducal Regulation of 25 July 2015 implementing Article 4(1) of the Law of 25 July 2015 on e-archiving.
  (Mém. A 2023, No 500)

We Henri, Grand Duke of Luxembourg, Duke of Nassau,
Having regard to the Law of 25 July 2015 on e-archiving and particularly Article 4(1) thereof;
Having regard to the opinions of the Chamber of Commerce and the Chamber of Skilled Trades and Crafts;
Having heard our State Council;
Upon the report of Our Minister of Economy and after deliberation of the Government in Council:

Decide:

“Article 1. The certification of dematerialisation or conservation service providers provided for in Article 4(1) of the Law of 25 July 2015 on e-archiving shall intervenes, at their choice, until 19 June 2018, according to the conditions and arrangements of Annex I or according to the conditions and arrangements of Annex II.

As from the above-mentioned date, the certification of dematerialisation or conservation service providers laid down in Article 4(1) of the Law of 25 July 2015 on e-archiving shall intervene according to the conditions and arrangements of Annex II.”[1]

“Article 2. As from 1 March 2023, the certification of dematerialisation or conservation service providers provided for in Article 4(1) of the Law of 25 July 2015 on e-archiving is carried out according to the Luxembourg standard ILNAS 106:2022 – E-archiving – Requirement framework for the certification of dematerialisation or conservation service providers (PSDC) (*Archivage électronique - Référentiel d’exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC)*).

The certification of dematerialisation or conservation service providers provided for in Article 4(1) of the Law of 25 July 2015 on e-archiving is carried out, at their choice, until 1 June 2024, either according to the conditions and terms of Annex II, or according to the conditions and terms of the above-mentioned Luxembourg standard ILNAS 106:2022.

For any future update of the above-mentioned Luxembourg standard ILNAS 106:2022, an eighteen-month transitional period is set as from the publication date of the application of the standard in the Journal officiel du Grand-Duché de Luxembourg. During the transition period, the certification of dematerialisation or conservation service providers provided for in Article 4(1) of the Law of 25 July 2015 on e-archiving is carried out, at their choice, until the end of the transition period, either according to the conditions and terms of the updated version of the above-mentioned Luxembourg standard ILNAS 106:2022, or according to the conditions and terms of the version preceding the updated version of the above-mentioned Luxembourg standard ILNAS 106:2022.”[2]

Article 3. Our Minister of Economy shall be in charge of the execution of this regulation which will be published in the Mémorial.

[1] Grand-ducal Regulation of 21 September 2017
[2] Grand-ducal Regulation of 7 August 2023

(Grand-ducal Regulation of 21 September 2017)

ANNEX I

(repealed by the Grand-ducal Regulation of 7 August 2023)

Annex II

Technical regulation establishing a management system and security measures for Dematerialisation or Conservation Service Providers (Version 3.1)

Table of contents

0 Introduction

0.1 Context

This Technical Regulation (hereinafter "Technical Regulation") defines the requirements and measures enabling an organisation to set up an information security management system and an operational management system specifically for dematerialisation or conservation processes.

From the information security management point of view, the Technical Regulation is based on the international standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013, so as to allow an organisation to be able to define, implement, maintain and improve:

a) an Information Security Management System (hereinafter "ISMS") based on the international standard ISO/IEC 27001:2013, incorporating the dematerialisation or conservation processes.

b) the information security objectives and measures based on the international standard ISO/IEC 27002:2013, specific to dematerialisation or conservation processes.

The Technical Regulation was drawn up in accordance with the requirements of ISO/IEC 27009:2016.

The Technical Regulation shall be used for compliance evaluation audits of organisations performing dematerialisation or conservation processes.

These evaluation audits must not only cover security requirements and measures, but also implementation recommendations. Any deviation from these recommendations which is not duly reasoned, documented or evident may give rise to minor non-compliance. Any deviation from the measures, unless the exclusion of the measure is duly justified by the risk treatment process, as well as any deviation from the requirements must give risk to minor or major non-compliance as defined in ISO/IEC 17021-1:2015.

The Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (hereinafter "ILNAS") shall be the only Luxembourg national authority empowered to grant an organisation a status of "dematerialisation or conservation service provider" (hereinafter "PSDC status") if this organisation has been certified as compliant with the Technical Regulation by a certification body accredited for this activity in accordance with the requirements of the international standard ISO/IEC 17021-1:2015 "Conformity assessment - Requirements for bodies providing audit and certification of management systems" as well as the additional requirements of ISO/IEC 27006:2015 "Requirements for bodies providing audit and certification of information security management systems". These standards define the requirements to carry out internationally recognised certifications of management systems according to ISO/IEC 27001:2013 and the Technical Regulation.

The Technical Regulation does not replace the regulations, laws or standards applicable to organisations performing dematerialisation or conservation processes. In particular, Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (also called "eIDAS Regulation") must be considered as the foundation for the establishment of security properties laid down therein, notably with respect to confidentiality, integrity, availability, authenticity, reliability and usability.

0.2 Structure of the document

This document is structured as follows:

- Chapter 1 specifies the scope of the Technical Regulation.
- Chapter 2 lists the references of standards, i.e. the standards the organisations implementing the Technical Regulation must comply with.
- Chapter 3 defines the terminology used in this text.
- Chapter 4 lays down the specific requirements for the management system of dematerialisation or conservation service providers. This chapter shall be read as a supplement to ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements", which explains the non-linear numbering of the requirements: a supplement to an existing section of the original standard keeps the same number, the unchanged sections are not included in this document and the new sections have numbers which are not used in ISO/IEC 27001:2013.
- Chapter 5 defines specific guidance, in particular objectives, security measures, implementation recommendations and additional information. This chapter shall be read as a supplement to ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls", which explains the non-linear numbering of the requirements.
- Annex A summarises the specific objectives and the specific security measures referred to in Chapter 5 while making their review compulsory when treating risks.

The transitions required by ISO/IEC 27009:2016 are indicated in *italics*.

1 Scope

The Law of 25 July 2015 on e-archiving lays down that a person may, if in possession of a certification in accordance with the requirements and measures defined in the Technical Regulation for a management system and security measures for Dematerialisation or Conservation Service Provider (hereinafter "PSDC") certification in view of the performance of its dematerialisation or conservation processes, notify ILNAS in order to obtain the PSDC status.

If the verification criteria established by the Law on e-archiving and by the ad hoc quality system of the Digital Trust Department of ILNAS are validated, ILNAS shall register the person concerned on the list of PSDCs (specifying the processes relating to the certification), thus establishing the "PSDC" status. Any significant event or incident identified and any major change to the scope of certification must be notified to ILNAS. Any withdrawal, suspension or non-renewal of the certification shall de facto result in the withdrawal of the PSDC status.

The PSDC status remains voluntary, except where regulatory or sectoral provisions require it.

The effective certification of any person according to the Technical Regulation for a management system and security measures for PSDC certification allows the application for the dematerialisation or conservation service provider status issued by the Digital Trust Department of ILNAS. ILNAS formally recognises the person concerned as PSDC via this status.

The certified person must be able to guarantee the results of the execution of the dematerialisation or conservation processes for which it obtained the certification. The certification guarantees that the digital documents generated by scanning analogue documents and the digital archives will be recognised as compliant with the specific requirements associated with the dematerialisation respectively conservation activity, as established in this document.

Thus, a copy shall be presumed to be true to the original documents when it is produced via the ad hoc process of a PSDC. Similarly, a digital archive shall be deemed as equivalent to digital originals when it is conserved via the ad hoc process of a PSDC.

Irrespective of its type, size, its processes or its activities, for their internal requirements or as part of the services provided to its clients, the Technical Regulation for a management system and security measures for PSDCs shall apply to any public or private organisation.

The Technical Regulation was defined based on the international standards published and maintained by the International Organization for Standardization (hereinafter "ISO").

The Technical Regulation must therefore be considered as a supplement to ISO/IEC 27001:2013 and ISO/IEC 27002:2013 by amending and supplementing their content specifically to the dematerialisation or conservation processes.

2 Standard references

The following reference documents are essential to the application of the Technical Regulation.

For dated references, only the mentioned editions shall apply. For undated references, the last edition of the reference document shall apply (including possible amendments).

ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

3 Terms and definitions

For the purposes of the Technical Regulation, the following abbreviations shall apply:

SoA	Statement of Applicability (declaration relating to the applicability of the security objectives and measures)
eIDAS	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
L2TP	Layer 2 Tunneling Protocol
IPSec	Internet Protocol Security
PPP	Point to Point Protocol
PSDC	Dematerialistion or Conservation Service Provider
SDC	Dematerialisation or Conservation System
SFTP	SSH File Transfer Protocol
ISMS	Information Security Management Systems
SSH	Secure SHell
TLS	Transport Layer Security
UTC	Coordinated Universal Time

For the purposes of the Technical Regulation, the terms and definitions provided for in ISO/IEC 27000:2016 as well as the following additional definitions shall apply.

3.1 asset

anything that has value to the organisation

Note 1: There are several types of assets, including:

a) information;

b) documents;

c) archives;

d) technical assets, such as scanner, server or hard drives;

e) intangible technical assets, such as virtual storage units;

f) staff of an organisation;

g) intangible assets, such as reputation and image;

h) processes and services.

Note 2: Definition adapted from ISO/IEC 30300:2011, definition 3.1.2.

3.2 analogue

non-digital

Note: An analogue storage medium is a non-digital storage medium, for example, paper, silver halide film or vinyl record.

3.3 archive

document maintained unchanged for continuing use

Note: Definition adapted from ISO/IEC 30300:2011, definition 3.1.1.

3.4 digital archive

archive in the form of digital document

3.5 authenticity

property that an entity is what it claims to be

[ISO/IEC 27000:2016]

3.6 confidentiality

property that information is not made available or disclosed to unauthorised individuals, entities or processes

[ISO/IEC 27000:2016]

3.7 conservation (electronic)

the activity which consists in conserving a digital original or a copy with probative value in the conditions that ensure reliable guarantees as to the integrity of the conserved document

[Law of 25 July 2015, Article 2(b)]

Note: Throughout the rest of this document, the term “conservation” shall be a synonym for “electronic conservation”, unless otherwise specified.

3.8 dematerialisation

the activity consisting in creating a copy with probative value of an original in analogue form in conditions that ensure reliable guarantees as to the compliance of the copy made from the original

[Law of 25 July 2015, Article 2(d)]

3.9 availability

property of being accessible and usable upon demand by an authorised entity

[ISO/IEC 27000:2016]

3.10 document

recorded information or object which can be treated as a unit

[ISO 15489 -1:2001]

3.11 reliability

property of consistent intended behaviour and results

[ISO/IEC 27000:2016]

3.12 management

definition, implementation or application, operation, control, revision, maintenance and improvement

Note: Similarly, “manage” shall be synonym for “define, implement or apply, operate, control, review, maintain and improve”.

3.13 indexing

establishing access points to facilitate document retrieval

Note 1: The generation of metadata associated with digital documents and digital archives is generally used to facilitate their retrieval.

Note 2: Definition adapted from ISO/IEC 15489-1:2001, definition 3.11.

3.14 integrity

property of accuracy and completeness

[ISO/IEC 27000:2016]

3.15 metadata

data describing the context, content or structure of documents and their management over time

Note: Definition adapted from ISO/IEC 30300:2011, definition 3.1.6.

3.16 non-repudiation

ability to prove the occurrence of a claimed event or action and its originating entities

[ISO/IEC 27000:2016]

3.17 organisation

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1: The concept of organisation includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[ISO/IEC 27000:2016]

Note 2: The term organisation shall designate the provider which is or would like to be a dematerialisation or conservation service provider.

3.18 dematerialisation or conservation service provider (PSDC)

any person exercising the activity of dematerialisation or electronic conservation, as a primary or secondary activity, for own needs or on behalf of third parties, and, under the conditions and arrangements set out in the [Law of 25 July 2015], certified to this end and registered on the list referred to in Article 4(3) [of this law]

[Law of 25 July 2015, Article 2(h)]

Note: The providers are only concerned by the processes they manage. In the whole document, “or” may be inclusive or excusive depending on the operational context of the provider.

3.19 evidence

document demonstrating the effectiveness of an operation

Note 1: The evidence of an operation means that it can be demonstrated to have been created in the normal course of business of the organisation and that it is intact and complete. It is not limited to the legal sense of the term.

Note 2: Definition adapted from ISO/IEC 30300:2011, definition 3.1.5.

3.20 process

set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2015]

3.21 information security

preservation of confidentiality, integrity and availability of information

Note: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[ISO/IEC 27000:2016]

Note for PSDCs: properties, such as authenticity, accountability, non-repudiation, reliability and usability are included in the notion of security.

3.22 system

set of interrelated or interacting technical assets

3.23 conservation system

system composed of a set of technical assets allowing the temporary storage of digital documents with a view to conserving them, converting them into digital archives, deleting them and conserving the digital archives for as long as necessary, using them, partially or totally returning them, transferring them or deleting them

3.24 dematerialisation system

system composed of a set of technical assets allowing the creation of digital documents from analogue documents, the temporary storage of analogue and digital documents, their return, their transfer, the possible destruction of analogue documents and the deletion of digital documents

3.25 dematerialisation or conservation system (SDC)

dematerialisation system, conservation system or a system combining both systems

4 Specific requirements for PSDCs and supplementary to ISO / IEC 27001:2013

4.1 Structure of this standard

This standard is a standard associated with ISO/IEC 27001:2013. It is specific to PSDCs within the meaning of the Law of 25 July 2015 on e-archiving.

The specific security objectives and security measures are indicated in Annex A.

4.2 Requirements specific to the management systems of PSDCs

All the requirements under Chapters 4 to 10 of ISO/IEC 27001:2013 which are not included below shall remain applicable without modification.

4 Context of the organisation

An additional requirement to ISO/IEC 27001:2013 shall be:

4.0 Management system of dematerialisation or conservation processes

The organisation must manage a management system of dematerialisation or conservation processes, incorporated in the ISMS or meeting the same requirements, in order to ensure the appropriate running of dematerialisation or conservation processes, the financial stability of the organisation and its capacity to fulfil the contractual, legal and regulatory responsibilities associated with the dematerialisation or conservation processes.

This process management system and the ISMS or the management system incorporating these two aspects must apply to processes and activities associated with the provision of the PSDC's services and with all assets supporting these processes.

Requirement 4.3 of ISO/IEC 27002:2013 shall be supplemented as follows:

4.3 Determination of the scope

In order to establish the scope of the management system of the dematerialisation or conservation processes, the organisation must determine the limits and applicability thereof.

It must define the nature of the processes (dematerialisation or conservation), the type of documents concerned and the type of clients (internal or external to the organisation, sectors concerned) which may benefit the services of the PSDC.

An additional requirement to ISO/IEC 27001:2013 shall be:

4.5 Authenticity, reliability and usability

In addition to the basic security properties which are

a. confidentiality,

b. integrity, and

c. availability,

the management system must manage the following additional security properties:

d. authenticity (often considered as a particular element of integrity):

   The organisation must be able to demonstrate that all the activities carried out when managing the dematerialisation or conservation processes are authentic, i.e.:

   i. The analogue or digital documents have indeed been transmitted by the person who supposedly transmitted it.

   ii. The digital document resulting from the scanning of an analogue document or the digital archive has indeed been created by the person or system at the presumed time.

   iii. The digital document or archive is indeed what it is supposed to be.

e. reliability:

   The organisation must be able to demonstrate that all the activities carried out when managing the dematerialisation or conservation processes are reliable, i.e.:

   i. All activities carried out to establish the dematerialisation or conservation processes shall be performed in accordance with the relevant policies and procedures defined and implemented by the organisation.

   ii. The created and used digital document or archive shall be in compliance with its original state and unchanged by unauthorised modifications.

f. usability:

   The organisation must be able to demonstrate that the usability of the dematerialisation or conservation processes create a digital document or archive which is locatable, readable, intelligible, usable at all times, with the information necessary to understand its origin and available for as long as necessary.

Note: Through the addition of these properties in the scope of the ISMS, the management system of ISO/IEC 27001:2013, limited to information security, is generalised as a management system of all properties required for dematerialisation or conservation activities.

5 Leadership

An additional requirement to ISO/IEC 27001:2013 shall be:

5.4 Roles, responsibilities and authorities in relation to the dematerialisation or conservation processes

The management must ensure that the responsibilities and authorities in relation to the roles concerned by the dematerialisation or conservation processes are allocated and communicated within the organisation.

The management must designate who has responsibility and authority to:

a. ensure that the management system of the dematerialisation or conservation processes complies with the requirements of this document;

b. define the performance criteria;

c. report to the management the performances of the management system of the dematerialisation or conservation processes;

d. manage the documentation (policies, procedures) supporting these processes;

e. define the system, functioning and security at operational level;

f. oversee the implementation of the policy;

g. issue recommendations to improve the operational management;

h. define and approve the methods relating to the management of risks which may impact the financial stability and the capacity to fulfil the contractual, legal and regulatory responsibilities;

i. manage the risks which may affect the organisation's financial stability and its capacity to fulfil the contractual, legal and regulatory responsibilities related to the dematerialisation or conservation;

j. evaluate the suitability of the measures adopted to mitigate the risks which may affect the financial stability and the capacity to fulfil the contractual, legal and regulatory responsibilities related to the dematerialisation or conservation and which are deemed unacceptable by the management of the organisation;

k. evaluate the merit of an insurance to ensure the continuity of the organisation's performance of the dematerialisation or conservation processes in case of cessation of business and during a minimum transition period;

l. identify the changes in terms of risks which may affect the financial stability and the capacity to fulfil the contractual, legal and regulatory responsibilities related to the dematerialisation or conservation;

m. raise awareness of the (organisation's and third parties') staff concerned regarding risks;

n. identify and evaluate the problems and incidents;

o. issue recommendations on preventive and corrective actions to be taken in response to the evaluated problems and incidents.

The management must allocate each role and responsibility to a person or an entity whose members and operating methods are documented and regularly review this allocation.

An additional requirement to ISO/IEC 27001:2013 shall be:

5.5 Leadership and commitment of PSDC

The management must demonstrate leadership and affirm its commitment in favour of the management system by:

a. ensuring that a policy and objectives are established with respect to the dematerialisation or conservation processes and that they are compatible with the duly documented strategic orientation of the organisation and with the information security policy;

   Note: A policy dedicated to the dematerialisation processes and a policy dedicated to the conservation process may be established by the organisation. If one of the processes does not fall within the scope, this policy and all the relevant requirements are obviously not required.

b. ensuring that the requirements of this policy are incorporated in the processes;

c. ensuring that the resources necessary to the management system of the dematerialisation or conservation processes are available (particularly, in order to provide elements evidencing the integrity and reliability);

d. communicating on the importance to have effective management of the dematerialisation or conservation processes and to comply with its requirements;

e. ensuring that the management system of the dematerialisation or conservation processes produce the expected result(s);

f. guiding and supporting the people so that they contribute to the effectiveness of the dematerialisation or conservation process;

g. promoting continual improvement;

h. helping other managers concerned to also demonstrate leadership when it applies to their areas of responsibility;

i. providing evidence of the organisation's legal existence;

j. providing evidence of an adequate financial situation and a stable situation to meet the expectations of the parties interested in the PSDC activity;

Note: The organisation may carry out a study on the cost of a transfer of activity or the return of documents to all clients, including all required information to maintain the probative value of a dematerialised document and a digital archive. The study may demonstrate that the cost is lower than the organisation's provisions, reserves or available capital and that these parameters are stable. The organisation may implement a monitoring process for these parameters, which ensures the management of incidents in case the financial stability degrades.

Note: An organisation governed by private law may, for example, provide the following information:

- a study on the cost of an activity transfer and the justification of the capacity to carry it out at all times, in view of its capital, its reserves or its provisions;
- the balance sheets and profit and loss accounts of the last three fiscal years, if the age of the organisation allows it;
- a report or opinion issued by a Luxembourg supervisory authority;
- the level of exposure of the business activities to factors external to the organisation;
- report of the financial auditors.

k. providing guarantee of performance continuity (i.e. for a minimum transitional period allowing a transfer) of the dematerialisation or conservation processes, particularly in the following cases:

1. the dematerialisation process performed by the organisation on behalf of a third party;
2. the electronic conservation process performed by the organisation on behalf of a third party;
3. the sub-process of return, transfer and deletion of digital archives performed by the organisation on its own behalf.

This guarantee of continuity must be managed by the organisation and cover the economic risk of cessation of business.

Note: One way for the organisation to guarantee the performance continuity during a minimum transition period is, for example, to take out a specific insurance or to obtain formal commitment from an institutional or private majority shareholder to act as guarantor.

6 Planning

An additional requirement to ISO/IEC 27001:2013 shall be:

6.1.4 Risks associated with the PSDC activity

The organisation must

a. incorporate information security and operational risks associated with the management of the dematerialisation or conservation processes in its process of identification (6.1.2.c), analysis (6.1.2.d) and assessment of risks (6.1.2.e), including also the risks which may impact the financial stability of the organisation and its capacity to fulfil the contractual, legal and regulatory responsibilities related to these processes;

b. apply its process for the treatment of security risks to risks determined in the previous point;

c. compare the objectives and measures determined under 6.1.3.b to those of Annex A of this document and verify that no necessary measure has been omitted;

d. supplement the statement of applicability determined under 6.1.3.d with the measures of Annex A of the Technical Regulation and the justification of their insertion or their exclusion, as well as, where appropriate, the indication of their implementation;

e. bring to the clients' and ILNAS' attention the statement of applicability, in particular if it includes exclusions.

An exclusion must be rejected if it creates non-compliance with a legal, regulatory or contractual requirement.

7 Support

An additional requirement to ISO/IEC 27001:2013 shall be:

7.4 Raising awareness regarding the dematerialisation or conservation policy

People carrying out work under the supervision of the organisation must:

1. be made aware of the dematerialisation or conservation policy and comply with all the documents relating to this policy;
2. be aware of their contribution to the effectiveness of the management system, including to the positive effects of a performance improvement;
3. be aware of the implications of any non-compliance with the requirements of the management system;
4. know their responsibilities under the Luxembourg law relating to dematerialisation or conservation and regarding the dematerialisation or conservation processes.

An additional requirement to ISO/IEC 27001:2013 shall be:

7.5.4 Non-repudiation of documented information

The organisation must implement a documentary environment which allows demonstrating to a third party compliance with the security properties indicated under Chapter 4.5 of this document and the integrity of the documentation.

8 Operation

An additional requirement to ISO/IEC 27001:2013 shall be:

8.4 Risk acceptance

The organisation must have the management approve the risk assessment, the plan to treat the risks including an indication of the required resources, the current risk level and the level of risk after treatment.

The organisation must conserve the evidence of this approval and the documentation of the management's deliberations.

9 Performance evaluation

Requirement 9.1 of ISO/IEC 27001:2013 shall be supplemented as follows.

9.1 Monitoring, measurement, analysis and evaluation

Similarly to the information security management system, the organisation must evaluate the performance of its SDC, as well as the effectiveness of the management system of the dematerialisation and conservation processes.

Requirement 9.2 of ISO/IEC 27001:2013 shall be supplemented as follows.

9.2 Internal audit

Similarly to the information security management system, the organisation must carry out scheduled internal audits in order to gather information determining whether the management system of the dematerialisation and conservation processes

a. complies with:

   1. the organisation’s own requirements regarding its management system of the dematerialisation or conservation processes;

   2. this Technical Regulation;

b. is effectively implemented and updated.

The organisation must thus include these audits in the audit programme(s), define the audit criteria and the perimeter of each audit, select the auditors and carry out audits which ensure objectivity and impartiality of the audit process, ensure that the audit results are reported to the management concerned and conserve the documented information as evidence of the implementation of the audit programme(s) and the audit results.

Requirement 9.3 of ISO/IEC 27001:2013 shall be supplemented as follows.

9.3 Management review

Similarly to the information security management system, the management must review the management system of the dematerialisation or conservation processes implemented by the organisation in order to ensure that it is still appropriate, adapted and effective.

The management review must take into account:

g. the results of the risk analysis which may impact the organisation’s financial stability and its capacity to fulfil the contractual, legal and regulatory responsibilities related to the dematerialisation or conservation processes on a regular basis.

The management review must take place at least once a year and following significant changes:

1. impacting the organisation’s operation;
2. arising from the current needs of the organisation;
3. of a legal and regulatory nature, impacting the organisation’s activities and processes.

10 Improvement

Requirement 10.2 of ISO/IEC 27001:2013 shall be supplemented as follows.

10.2 Continual improvement

The organisation must continually improve the relevance, adequacy and effectiveness of the management system of the dematerialisation or conservation processes.

5 Code of practice specific to PSDCs in relation to ISO/IEC 27002:2013

All categories of measures, security objectives, implementation recommendations and additional information of ISO/IEC 27002:2013 which are not included below remain applicable without modification.

Annex A summarises the specific objectives and the specific security measures referred to in this chapter while making their review compulsory in the risk treatment.

5 Information security policies

A category of measures additional to ISO/IEC 27002:2013 shall be:

5.2 Management guidance regarding the dematerialisation or conservation policy

Objective: Provide the management of the dematerialisation or conservation processes with guidance and support from the management, in accordance with the business requirements and the laws and regulations in force.

5.2.1 Dematerialisation or conservation policies

Measure

A “dematerialisation or conservation policy” should be defined, approved by the management, implemented and disseminated and communicated to the employees and the third parties concerned.

Implementation recommendations

The dematerialisation or conservation policy should define the scope of the dematerialisation or conservation processes and the information security and operational management applied to these processes.

The document should include the following elements:

a. a presentation of the organisation, its history and its business activities;
b. the link with the strategy or motivation to implement this activity;
c. a definition of the scope of the dematerialisation or conservation processes;
d. a general organisational and technical description of the following processes underlying
   1. the dematerialisation process:
      i. collection of analogue documents;
      ii. creation and temporary storage of digital documents;
      iii. temporary storage of analogue documents;
      iv. return, transfer, possible destruction of analogue documents and deletion of digital documents;
      v. name of the suppliers whenever a process activity is outsourced.
   2. the conservation process:
      i. collection of digital documents;
      ii. creation and conservation of digital archives;
      iii. return, transfer, deletion of digital archives;
      iv. name of the suppliers whenever a process activity is outsourced;

e. the general technical description of the SDC and its level of compliance with the recognised standards and frameworks;
f. the roles and responsibilities specific to the dematerialisation or conservation process and to the underlying processes performed by the organisation and relating to information security and operational management;
g. the main information security principles applied to the dematerialisation or conservation process performed by the organisation, in particular regarding authenticity, reliability and usability;
h. the references to laws and regulations applicable to the organisation and specific to the dematerialisation or conservation process;
i. the management of the documentation supporting the dematerialisation or conservation process;
j. references to documents such as, for example, administration, operation and security procedures supporting the dematerialisation or conservation policy;
k. the arrangements for reviewing the dematerialisation or conservation policy.

5.2.2 Review of the dematerialisation or conservation policy

Measure

To ensure on-going relevance, adequacy and effectiveness of the dematerialisation or conservation policy, these policies and processes should be reviewed at scheduled intervals and in case of significant change.

Implementation recommendations

The same recommendations as those for the information security policy shall apply to this policy.

The category “6 Information security organisation” shall be supplemented as follows.

6 Organisation of information security and dematerialisation or conservation processes

6.1 Internal organisation

Objective: Establish a management framework to begin and then verify the implementation and operation of information security and dematerialisation or conservation processes within the organisation.

6.1.1 Functions and responsibilities associated with information security and dematerialisation or conservation processes

Measure

All responsibilities regarding information security, in particular those related to the performance of the dematerialisation or conservation processes and those consisting of ensuring compliance of the processes and operational management with the applicable documents, should be defined and allocated.

Implementation recommendations

The responsibilities should be allocated in accordance with the information security policy (cf. 5.1.1 of ISO/IEC 27002:2013) and the dematerialisation or conservation policy (cf. 5.2.1 of this document).

The responsibilities in relation to asset protection and the implementation of specific security processes and dematerialisation or conservation processes should be determined.

The responsibilities related to risk management activities regarding the information security and the use of dematerialisation or conservation processes and in particular those associated with residual risk acceptance, should be determined. If necessary, these responsibilities should be supplemented by detailed guidance which is suitable to some sites and means to treat information.

The area of responsibility of everyone should be specified and in particular the following measures should be taken:

a. the assets and the security processes as well as the dematerialisation or conservation processes should be identified and determined;

b. a person or an entity responsible should be allocated to each asset or process and its responsibilities should be documented in detail (cf. 8.1.2);

c. the different levels of authorisation should be defined and documented;

d. in order to be able to ensure the responsibilities, the designated people should be competent in this area and they should benefit from facilitations in order to keep themselves informed of the developments;

e. the coordination and supervision activities associated with the relations with suppliers should be identified and documented.

For each dematerialisation or conservation process, a person should be designated for each of the following responsibilities:

a. the management of the documentation (policies, procedures) supporting these processes;

b. their definition at operational level, including the SDC and the relating security mechanisms;

c. the supervision of their implementation;

d. the definition of their performance criteria;

e. their evaluation according to the performance criteria;

f. the issue of recommendations to improve their operational management.

Additional information

The people to whom responsibilities have been allocated can delegate tasks. However, they remain responsible and they should ensure the proper execution of any delegated task.

6.1.2 Segregation of duties

Implementation recommendations

It should be ensured that the people who have roles and responsibilities in the management of information security or operational processes or activities related to the dematerialisation or conservation do not also review the effectiveness of the discharge of these roles and responsibilities nor evaluate their compliance with the defined objectives.

Effective separation of the administrative, operational and security activities should be ensured not only when describing the roles but also when allocating privilege profiles for the accounts of users authorised to access the SDC, so as to reduce the risk of conflicts of interest and unauthorised access.

In order to comply with the non-repudiation principle, it should be possible to demonstrate that the access privileges established for all the SDC users, including access through technical accounts, comply with the principle of effective separation of administrative, operational and security activities of the conservation system.

6.1.5 Information security in project management

Implementation recommendations

The SDC management procedures should be drawn up and approved when defining and implementing dematerialisation or conservation projects.

A category of measures additional to ISO/IEC 27002:2013 shall be:

6.3 Internal organisation specific to the dematerialisation and conservation processes

Objective: Establish a management framework to ensure compliance with the specific legal requirements for the dematerialisation or conservation processes within the organisation.

6.3.1 Verification of digital documents following the dematerialisation

Measure

The content of the digital documents should be verified in relation to the corresponding analogue documents.

Implementation recommendations

As regards the dematerialisation process, mechanisms should be implemented to check

a. that the number of incoming analogue documents (or the number of pages in these documents) matches the number of outgoing documents or pages (rejected digital and analogue), and

b. the content of the digital documents generated by scanning analogue documents to ensure the faithful reproduction of the original.

6.3.2 Dual control principle regarding the modification or deletion of digital archives

Measure

Any modification or deletion of the created digital archives which was not scheduled during the definition of the conservation project must be approved by two users authorised to perform these operations.

6.3.3 Evidence management

Measure

A procedure should be established and appropriate management should be implemented regarding evidence of the operation of the SDC and activities carried out by the staff concerned.

Implementation recommendations

Checks of the integrity of SDC operation, the digital documents and the digital archives managed by the SDC, on a regular basis and following significant changes to the SDC and the conservation process, should be ensured.

6.3.4 Relations with the national authority

Measure

Procedures should be implemented to notify the competent authorities, in particular ILNAS, of the anticipated significant changes which may impact the information security and the operational activities, as well as of any security breach or loss of integrity which has a potentially significant incidence on the dematerialisation or conservation service as soon as possible and in any event within twenty-four hours after becoming aware of it.

Implementation recommendations

The following should be considered as significant changes:

a. change of the organisation’s management;

b. modification of the SDC impacting the relevant processes;

c. modification of the scope of activities managed by suppliers impacting the dematerialisation or conservation processes performed by the organisation.

A category of measures additional to ISO/IEC 27002:2013 shall be:

6.4 Organisation of the dematerialisation and conservation processes involving clients

Objective: Clarify the responsibilities of the PSDC and of its clients and ensure transparency for clients regarding the security and use of the dematerialisation or conservation processes.

6.4.1 Security in client agreements

Measure

The conditions under which the dematerialisation or conservation processes are performed, as well as the information security requirements associated with these processes, should be established in a contractual document with the client and approved by the client and the PSDC.

Implementation recommendations

If the client is internal to the organisation or belongs to the same legal entity, the contractual document may be replaced by an internal document established and validated according to the organisation’s document management practices.

The following elements should be established with the client as part of the management of a dematerialisation or conservation project:

a. the client information requirements relating to the dematerialisation or conservation processes;

b. a detailed description of the dematerialisation or conservation project, taking into account technical, operational, security, legal and regulatory aspects;

c. the reference base for the security measures and additional measures implemented to guarantee the authenticity, reliability and use of the collected (analogue and digital);

d. documents the digital documents and digital archives of the client during the performance of the dematerialisation or conservation processes;

e. the levels of service associated with the implementation of the SDC;

f. the management of organisational and technical changes that could impact the dematerialisation or conservation processes, as well as the SDC;

g. the management of (major) incidents affecting the dematerialisation or conservation processes, as well as the SDC;

h. the process and arrangements to be applied for the evaluation of the services as well as acceptance of the services by the client;

i. the roles and responsibilities of the client and of the organisation during the implementation of the project and the consequences of non-fulfilment of these roles and responsibilities;

j. the contractual, operational and information security contacts for the client and the organisation;

k. the involvement of the client in the assessment and treatment of risks.

The reference base for the security measures and additional measures implemented may be documented in the statement of applicability (cf. ISO/IEC 27001) or in a document named “security assurance requirements” according to the Common Criteria (cf. ISO 15408).

The client should commit, in particular, to provide and maintain a list of people authorised to:

a. submit and recover analogue documents;

b. access the digital documents generated by scanning analogue documents or the digital archives;

c. use the SDC;

d. request the destruction and the deletion of the collected (analogue and digital) documents, the digital documents generated by scanning analogue documents or the digital archives.

Additional information

Any change in a contractual document requires the approval of the contracting parties.

It is at this level that the particular security measures required by the client which are additional to those that the PSDC establishes on its own initiative may be specified.

6.4.2 Obligation to inform the client in advance

Measure

Prior to any contractual relation with a holder, information relating to the conditions for service provision, in particular, any information legally required to ensure a transparent service should be made available on a durable medium and in easily understandable terms.

Implementation recommendations

Before establishing a contract, the PSDC should include the following in the information given to its clients:

a. the procedure in place for dematerialisation or conservation;

b. the procedure in place for returning the copies with probative value under a readable form while guaranteeing fidelity to the original;

c. the terms and conditions for potential outsourcing including the location of data storage;

d. the legal obligations with which the PSDC must comply;

e. the contractual conditions for providing the services, including any limitation of liability of the PSDC;

f. the implemented standards and procedures as well as the key technical characteristics of the equipment used for the provision of the services;

g. the arrangements for informing the client in case of changes.

An agreement should be reached with the clients (internal or external to the organisation) who are impacted by the detailed process and the rules to be followed when performing the dematerialisation and conservation processes.

This detailed process and these rules should be included in the operational procedures of the dematerialisation and conservation processes and should be approved by the clients concerned.

The clients should be involved in the changes of the procedures they approved. The following detailed process should be included in these procedures:

a. the collection of analogue documents (only for the dematerialisation process);

b. the collection of digital documents (for conservation);

c. the temporary storage of digital documents;

d. the creation and the conservation of digital archives (for conservation);

e. the return, the transfer and the deletion of digital archives (for conservation).

The clients should be notified of scheduled deletions of digital archives belonging to the client if a specific deletion schedule was drawn up for the said archives when defining the conservation project.

If no deletion schedule is provided for a given digital archive, prior authorisation of the clients should be sought to delete it.

6.4.3 Classification of the client’s assets

Measure

For all their analogue or digital documents and all their digital archives, the clients should define with the PSDC the classification level, the retention time, as well as other possible security requirements such as specific access rights.

Implementation recommendations

The clients should assume the role of owner of the information which belongs to them and which is managed by the organisation.

The clients should be made aware that they are responsible for the classification requirements defined and applied to these documents (collected documents, digital documents or digital archives).

6.4.4 Obligation to inform the client in the event of changes or incidents

Measure

Prior to the application or at the earliest opportunity, the internal or external clients concerned should be informed of any changes to the prior information and to the information associated with the contractual obligations, as well as of any incidents which may jeopardise the clients’ information, whilst providing them with the necessary justifications.

Implementation recommendations

The client should be immediately informed

a. in the event of any incidents that could affect:

   1. the client's documents;

   2. the dematerialisation or conservation processes used by the client or on its behalf;

   3. the SDC used by the client or on its behalf;

b. any attempt to access the client's documents managed by the organisation using the client's connection identifiers under abnormal usage conditions, for example outside of normal office hours.

Changes reported to the national authority should be considered as significant changes (cf. 6.3.4).

Digital archives should only be converted into a format other than their original format upon written confirmation of the client (internal or external to the organisation) concerned with the archive.

The client should be informed about the effect of the change on the risk assessment.

Evidence should be kept that this information took place and, where time before its application is short, approval of the client should be requested.

7 Human resource security

7.2 During employment

An additional measure to ISO/IEC 27002:2013 shall be:

7.2.4 Policy commitment

Measure

If the internal staff or the suppliers' staff are involved in the operational management of the security or the dematerialisation or conservation processes, they should understand and commit in writing to complying with the security policy and the dematerialisation or conservation policy.

Implementation recommendations

The internal staff and the suppliers' staff, who are involved in the operational management of the security or the dematerialisation or conservation processes, should

1. be correctly informed of their roles and responsibilities related to the dematerialisation or conservation processes;

2. commit in writing to complying with the dematerialisation or conservation policies and the information security policy;

3. take part in an initial awareness training to present the policies, the expectations and the needs of the organisation in this respect in order to ensure common understanding of these elements;

4. take part in ongoing training to remind of the requirements regarding the dematerialisation or conservation and to present the procedures related to these requirements and the recent changes made to all the documentation related to the areas concerned.

8 Asset management

8.1 Responsibility for assets

Additional implementation recommendations shall be:

8.1.1 Inventory of assets

Implementation recommendations

The following should be identified:

a. dematerialisation or conservation processes;

b. components of the dematerialisation or conservation systems;

c. clients;

d. collected (analogue and digital) documents of clients;

e. digital documents resulting from the scan of the clients' analogue documents;

f. digital archives of clients.

8.1.2 Share ownership

Implementation recommendations

The owner of each active dematerialisation or conservation process should

d. approve the evaluation of the operational aspects of the SDC at least once per year and following any significant changes;

e. review the detailed SDC description and the specifications of the security mechanisms of the conservation system on a regular basis (at least once a year) and following any significant changes to the SDC.

An additional measure to ISO/IEC 27002:2013 shall be:

8.1.4 Partitioning of secret information or personal information

Measure

Any confidential information or personal information should be sufficiently partitioned so that it is possible, in particular, to respond to the owner's request to destroy it without endangering other archived information or evidence of the proper management of other dematerialised or conserved information.

Implementation recommendations

The client or the PSDC should refrain from including personal information in the metadata, if these metadata are part of the operation traceability system, with a view to comply with European regulations on the protection of personal data, in particular the right to be forgotten.

8.2 Information classification

Additional implementation recommendations shall be:

8.2.1 Information classification

Implementation recommendations

Classification levels should be defined and attributed to inventoried assets, incorporating requirements relating to authenticity, reliability and use, for as long as is necessary.

These guidelines should be reviewed in the event of any changes to the specificities of the SDC and in the event of any changes in the client's expectations.

Additional information

A 'reliability' criterion may be defined in addition to other criteria. It may contain multiple levels of precision of a dematerialisation (colour versus black and white, colour coding, resolution) and attribute such a level specifically to the documents collected from clients and to the clients' digital archives.

The integrity criterion may be used to include the requirements associated with authenticity.

The availability criterion may be used to include the requirements associated with usability.

8.3 Media handling

Additional implementation recommendations shall be:

8.3.2 Disposal of media

Implementation recommendations

Consideration should be given to the following:

a. the destruction of the following elements using secure mechanisms:

   1. the clients' analogue documents according to the conditions set out in the contractual documents drawn up between the clients and the organisation;
   2. all storage media of the organisation containing the clients' information (including digital documents and archives) or information which is confidential for the organisation;
   3. all the clients' information contained in the storage media of the organisation using secure mechanisms if these media cannot be destroyed securely;

b. the evaluation by a third party able to attest to the effectiveness of the destruction and deletion;

c. in the event of use of a supplier, production of a certificate from this supplier stipulating that:

   1. the storage media provided to the third party by the organisation for destruction were indeed those that were destroyed;
   2. the information stored in the storage media transferred by the organisation for deletion has indeed been deleted;
   3. the destruction of analogue documents and storage media and the deletion of information stored on these media were undertaken respectively using a secure method based on the relevant best practice.

9 Access control

9.1 Business requirements concerning access control

An additional measure to ISO/IEC 27002:2013 shall be:

9.1.3 Effective segregation associated with access rights

Measure

Three different people should be involved in the management of an access right: one to authorise the access, one to check compliance with the security requirements and finally one to grant access on the systems.

Implementation recommendations

An SDC access rights administrator should not grant this right unless the right has been formally authorised according to the access rights policy for another person and a different person has validated compliance of the security requirements with this right.

10 Encryption

10.1 Encryption measures

Additional implementation recommendations shall be:

10.1.1 Policy on the use of encryption measures

Implementation recommendations

When developing an encryption policy, due regard should be given to the following point:

h. application of qualified trust services in accordance with the eIDAS regulation to ensure the security of dematerialised documents and digital archives.

Additional information

Standard ETSI TS 102 176-1 lists the encryption algorithms and recommends a term of validity for their use.

An additional measure to ISO/IEC 27002:2013 shall be:

10.1.3 Two-factor authentication

Measure

For persons interacting with the technical assets of the conservation system or accessing digital documents and digital archives, appropriate secure authentication should be provided based on encryption mechanisms and, if access is possible from premises not requiring two-factor authentication, a two-factor authentication process.

Implementation recommendations

A secure device should be used, such as a smart card or USB encryption key containing an electronic authentication certificate, a physical authentication device or biometrics technology, to ensure the secure authentication of users accessing the technical assets of the conservation system, the digital documents and the digital archives managed by the conservation system.

An IP address filter should be used in conjunction with an encryption means, for example an SSL certificate, to ensure the secure authentication of a technical asset of the conservation system to other assets of the conservation system, the digital documents and digital archives managed by the conservation system.

An additional measure to ISO/IEC 27002:2013 shall be:

10.1.4 Protection of the integrity of digital documents or digital archives

Measure

The integrity of digital documents collected by the conservation system and digital archives generated by the conservation system should be protected using appropriate encryption algorithms and techniques.

Implementation recommendations

The integrity of the digital documents collected by the conservation system and the digital archives generated by the conservation system should be protected, to ensure that these documents are correctly stored, processed and deleted and that these archives are correctly created, used, returned, transferred or deleted.

The digital fingerprint of each digital document to be archived should be calculated by the issuer of the document and securely sent to the organisation, which then checks the integrity of the digital document received by calculating and obtaining a digital fingerprint identical to the one sent by the document issuer.

An additional measure to ISO/IEC 27002:2013 shall be:

10.1.5 Protection of the integrity of internal documents

Measure

The integrity of internal SDC documents and associated processes should be protected, particularly the SDC event logs, with protocols using appropriate encryption algorithms and techniques.

Implementation recommendations

The integrity of internal documents should be protected over time, particularly the event logs or checking operations.

In particular, it ought to be ensured that:

a. a system for interlinking the events recorded in a log is established in order to detect any deletion of past events;

b. event logs are regularly time-stamped, e.g. once a day, by a qualified time-stamping authority.

An additional measure to ISO/IEC 27002:2013 shall be:

10.1.6 Electronic signature of internal documents

Measure

Users of the SDC should use a qualified signature or a mechanism offering a similar guarantee to validate the internal documents necessary in order to demonstrate the correct operation of the SDC and its associated processes.

Implementation recommendations

A secure device should be used to enable:

a. conservation system users to electronically sign administrative, operational and security activity reports of the conservation system, in order to guarantee the authenticity of the activities performed.

b. someone from the organisation to electronically sign the information, digital documents and digital archives sent to clients (internal or external to the organisation) and to the competent authorities, to guarantee the authenticity of such transmissions.

The device used to create the electronic signatures and qualified electronic certificates used must meet the relevant requirements defined by the European Union.

Electronic signature formats such as CAdES [5], XAdES [6] and PAdES [7] should be used to ensure the durability of the electronic signature, the information, the digital documents and the digital archives attached to the signature.

An additional measure to ISO/IEC 27002:2013 shall be:

10.1.7 Protection of document transmissions

Measure

Transmissions of digital documents and information should be protected by protocols using appropriate encryption algorithms and techniques.

Implementation recommendations

Secure protocols (SFTP, TLS, PPP, L2TP and IPSec, etc.) should be used to secure the transmission of information, digital documents and digital archives between the following elements:

a. technical assets of the conservation system, even if they are on the same network;

b. the parties involved in the conservation process, such as the organisation, the clients (internal or external to the organisation) and the competent authorities.

An additional measure to ISO/IEC 27002:2013 shall be:

10.1.8 Conservation of electronic signatures

Measure

If the integrity of a digital document to be archived depends on an electronic signature, the document should be conserved together with evidence that the signature has been verified no later than at the time of archiving.

Implementation recommendations

The integrity of the document should be demonstrated by showing that:

a. at the time of archiving, the electronic signature was correct, the qualified electronic certificate applied to it was valid and issued by a recognised certification authority;

b. the archiving system conserves the integrity of the archived documents for as long as necessary.

Additional information

There are a number of possible techniques, such as:

a. using the Online Certificate Status Protocol (OCSP) of the certification authority issuing the qualified electronic certificate;

b. time-stamping the signed activity report and obtaining the Certificate Revocation List (CRL) regularly published by the certification authority issuing the qualified electronic certificate.

11 Physical and environmental security

11.1 Secure areas

An additional measure to ISO/IEC 27002:2013 shall be:

11.1.7 Accompanying visitors

Measure

An authorised member of the organisation should constantly accompany all visitors to the organisation, even if they have already been authorised to access these areas.

Implementation recommendations

Visitors should be excluded from areas associated with the dematerialisation process, in particular when the clients' analogue documents are being processed, to reduce the risk of unauthorised disclosure of information.

The necessary measures should be taken to ensure that the visitors are unable to see the clients' information.

Third parties who are permanently authorised to access secure areas of the organisation should be effectively monitored when they access the SDC technical assets and the clients' documents.

The SDC technical assets should be protected against unauthorised access:

a. in the event of evacuation of the areas hosting these assets;

b. in the event that they are located in multiple-occupancy sites.

11.2 Equipment

Additional implementation recommendations shall be:

11.2.1 Equipment location and protection

Implementation recommendations

The clients' analogue documents should be considered assets requiring special protection (within the meaning of 11.2.1.d of ISO/IEC 27002:2013) from environmental conditions and other associated threats.

11.2.5 Removal of assets

Implementation recommendations

Analogue documents from the dematerialisation process should not be removed from the organisation without the client's prior consent, except to prevent the destruction of these assets in the event of a catastrophe.

12 Operations security

12.1 Operational procedures and responsibilities

An additional measure to ISO/IEC 27002:2013 shall be:

12.1.5 SDC usage procedures

Measure

Procedures should be defined, implemented and monitored by the staff concerned (of the organisation and the suppliers), concerning administration, SDC operations, use of the dematerialisation or conservation process and control of the SDC security and processes, including all of the necessary rules to be followed in order to guarantee the properties of confidentiality, integrity, availability, authenticity, reliability and usability.

Implementation recommendations

The following activities should be included in the SDC management procedures:

a. management of the SDC access and privileges associated with SDC accounts;

b. management of the SDC administration, operation and security functions and instructions for performing them;

c. SDC configuration management;

d. instructions for operating the SDC in degraded mode, restarting it and recovering it;

e. management of the SDC monitoring mechanisms;

f. management of the SDC event logs and instructions for using them;

g. management of the SDC encryption security mechanisms, such as:

   1. authentication and signature mechanisms for the SDC users;

   2. secure transmission protocols for information, digital documents and digital archives;

   3. integrity mechanisms for digital documents, digital archives and event logs, as well as

4. replacement of these mechanisms should vulnerabilities be discovered, without altering the usability and integrity of the archives;

h. if it is part of the agreement with the clients, management of the mechanisms for detecting and deleting malicious codes;

i. management of the mechanisms used to regularly monitor the integrity of the SDC;

j. management of the mechanisms for deleting digital documents and digital archives managed by the SDC;

k. management of the SDC storage media, their replacement and disposal;

l. management of the SDC backups and the backups of digital documents and digital archives managed by the SDC and their respective restoration;

m. management of the SDC continuity and recovery, including in the event of disaster;

n. management of changes to the SDC;

o. management of incidents liable to affect the SDC;

p. maintenance of technical assets with the suppliers' support management in the event of malfunction of the SDC;

q. management of description and control metadata associated with digital archives;

and also for the dematerialisation processes:

r. management of the mechanisms used to check that the number of scanned analogue documents (or pages in these documents) is correct;

s. management of the mechanisms used to check the content of digital documents.

Additional implementation recommendations shall be:

12.4 Logging and monitoring

12.4.1 Event logging

Implementation recommendations

All events relating to the SDC should be identified and logged, in particular:

a. system events of SDC assets;

b. errors and malfunctions of SDC assets;

c. errors and malfunctions relating to the generation of event logs;

d. events relating to the analogue documents, digital documents and digital archives processed by the SDC.

12.4.3 Administrator and operator logs

Implementation recommendations

All actions performed by the SDC user accounts should be identified and logged, including actions associated with the SDC but performed outside the normal SDC conditions of use; in particular:

a. user login attempts outside of normal office hours;

b. actions performed by users more rapidly than usual, suggesting that they were performed by technical assets and not by natural persons;

c. duplication of user sessions.

12.4.4 Clock synchronisation

Implementation recommendations

It should be ensured that:

a. the technical assets supporting the SDC are synchronised to the coordinated universal time (UTC), via an authoritative time source;

b. the events associated with the regular synchronisation of the system clock for the technical assets of the SDC are recorded and conserved for as long as necessary;

c. a unique date and time format is adopted for generating events in the SDC to facilitate the traceability of the performed actions;

d. the synchronisation with the master clock is performed with sufficient regularity to ensure that any variation between the master clock and the clock of the systems within the perimeter remains below the threshold of one second;

e. any variation greater than the tolerated variation is detected without delay so that corrective actions may be taken;

f. clock accuracy checking elements, such as time-stamping tokens, are generated during the SDC operation.

An additional measure to ISO/IEC 27002:2013 shall be:

12.4.5 Usability of the event logs

Measure

The event logs generated should be conserved in a usable form and protected against any unauthorised use and deletion, to ensure that all of the events recorded by these mechanisms remain traceable for as long as necessary.

Implementation recommendations

The logged information should be centralised in relation to the SDC.

Permanent storage media should be used to ensure that the event logs are properly conserved for as long as is necessary.

A category of measures additional to ISO/IEC 27002:2013 shall be:

12.8 Correct and secure management of the SDC

Objective: To ensure the correct and secure management of analogue documents to be dematerialised, digital documents and digital archives during the dematerialisation or conservation process.

12.8.1 Adequacy of the SDC

Measure

It should be demonstrated that the SDC is made up of technical assets and security mechanisms that meet the needs of clients and make it possible to guarantee the authenticity, reliability and usability of the analogue documents to be dematerialised, the digital documents and the digital archives managed by this system.

12.8.2 Detailed description of the SDC

Measure

A detailed and comprehensible description of the SDC should be defined and maintained, comprising the technical assets, functional and operational aspects, as well as the flows and dependencies between the various components.

Implementation recommendations

A detailed and comprehensible description of the SDC should be defined and maintained:

a. by identifying and documenting the technical assets supporting the processes underlying the dematerialisation or conservation process, namely:
   1. the collection of analogue or digital documents;
   2. the temporary storage of these documents;
   3. the creation of digital documents or digital archives;
   4. the return, transfer, possible destruction of analogue documents and the deletion of digital archives;

b. by regularly identifying, evaluating and documenting the functional and operational aspects of the SDC, such as:
   1. for the dematerialisation system, for each scanner;
      - i. the maximum and minimum numbers of colours and grey tones;
      - ii. the maximum and minimum figures for DPI, bits per pixel;
      - iii. the option of dematerialising one or both sides of a page;
      - iv. the various input formats, such as A3, A4 and A5;
      - v. the image correction methods available, such as de-skewing, despeckling and cropping;
      - vi. the image compression methods available;
      - vii. the number of analogue documents or number of pages in the analogue documents that can be scanned within a given time;
   2. for the conservation system;
      - i. the maximum number or maximum size of digital documents that may be sent as one batch;
      - ii. the transmission rate for digital documents or for the return of digital archives;
      - iii. the response times;
      - iv. the issue frequency of batches or returns of digital archives;
      - v. the secure information transmission protocols for supported digital documents and digital archives, such as SFTP, TLS, PPP, L2TP and IPSec;

c. by documenting the network architecture, the data flow between assets and the dependencies between assets.

12.8.3 SDC security mechanisms

Measure

The SDC security mechanisms guaranteeing the authenticity, reliability and usability of the analogue documents, digital documents and digital archives managed by this system should be managed and documented.

Implementation recommendations

In particular, the following security mechanisms should be managed:

a. SDC access management mechanisms.

   Access to the SDC technical assets, the analogue documents, the digital documents and the digital archives managed by the SDC should be protected by:

   1. ensuring that the conditions of access to these assets apply to all natural persons and all assets attempting to access them;
   2. ensuring adequate management of the user accounts authorised to access the SDC and the technical accounts of the SDC technical assets, with the ability to immediately revoke these accounts;
   3. unambiguously identifying the system activities and actions performed and being able to attribute them unequivocally to an author, for example by attributing personal accounts to each user;
   4. managing appropriate and secure authentication mechanisms for the authorised user accounts and the technical accounts of the SDC technical assets.

b. Rights management mechanisms.

   A rights management system should be set up for all of the SDC user accounts and the technical accounts of the SDC technical assets. (cf. 6.1.2 and 6.1.6).

c. Monitoring mechanisms (cf. 12.4.3).

d. Secure encryption mechanisms (cf. 10.1).

e. Mechanisms for detecting and eliminating malware in the digital documents collected for electronic conservation, if this is requested by the client.

   At the very least, antivirus software should be used to check that all digital documents collected for electronic conservation do not contain any malware such as viruses, Trojan horses or network worms.

   This antivirus software should be used from the time the SDC receives the digital documents and before the process to create the digital archives begins.

f. Mechanisms for securely deleting digital documents and archives, such as multiple overwriting of the information, preventing it from being recovered.

g. Mechanisms for converting (where necessary) digital archives into a format other than their original format.

12.8.4 Supervision of the SDC operational aspects

Measure

The SDC operational aspects should be evaluated regularly, such as the space available and the failure rate of redundant components.

Implementation recommendations

It is recommended:

a. defining a list of the SDC operational aspects to be checked;
b. including it on the list of the elements needing to be monitored according to the requirements of the management system performance evaluation (cf. ISO/IEC 27001 2013, Chapter 9.1);
c. establishing availability indicators for the operational characteristics, such as the disc lifespans.

12.8.5 Regular control of the integrity of the SDC

Measure

Mechanisms should be implemented for regular controls of the SDC integrity and of the information necessary in order to ensure traceability.

Implementation recommendations

Concerning the SDC, it should be ensured that:

a. the operation of the SDC has not been altered following:
   1. maintenance work or updates;
   2. replacement of SDC assets, such as scanners, the electronic conservation platform or components of these assets, such as storage media;

b. SDC configuration files have not been subject to unauthorised modification;

c. integrity is preserved with regard to the
   1. stored digital documents;
   2. associated metadata;
   3. digital archives;
   4. event logs.

13 Communications security

The objectives, measures, implementation recommendations and additional information of ISO/IEC 27001:2013 shall apply without amendment.

14 Information system acquisition, development and maintenance

14.1 Security requirements applicable to information systems

Additional implementation recommendations shall be:

14.1.1 Information security requirements analysis and specification

Implementation recommendations

It should be ensured and demonstrable that the critical applications and information systems supporting the SDC are implemented in accordance with recognised secure development methods.

The principle of lodging source code with a third party should be evaluated and, where applicable, established for any SDC application provided by a supplier that is necessary in order to ensure the integrity and availability of information.

15 Supplier relations

15.1 Information security in supplier relations

An additional measure to ISO/IEC 27002:2013 shall be:

15.1.4 Contractual conditions for the suppliers involved in the dematerialisation and conservation process

Measure

The contracts concluded with each supplier involved in the dematerialisation and conservation process should include conditions that ensure compliance with the security policy and the dematerialisation and conservation policy.

Implementation recommendations

For all suppliers supporting the dematerialisation or conservation processes performed by the organisation, the following conditions should be studied and then the necessary conditions for controlling the risks associated with the supplier's activity should be included in the contractual document concluded with this supplier:

a. the provisions concerning ownership of the products and services, such as documents and applications, provided by the supplier as part of its support for the dematerialisation or conservation processes performed by the organisation;

b. the provisions concerning the continuous supply of the products and services by the supplier to support the dematerialisation or conservation processes performed by the organisation, including in the event of disaster;

c. the compliance with the organisation's dematerialisation or conservation policy;

d. the measures guaranteeing:

   1. the swiftest possible notification of any security changes applied to the assets of the supplier and its suppliers that could impact the dematerialisation or conservation processes performed by the organisation;
   2. that the information belonging to the organisation will be used exclusively for the purposes for which it was made available to the supplier and its suppliers;
   3. that changes impacting the supplier's suppliers involved in the dematerialisation or conservation processes performed by the organisation will be approved in advance by the organisation;

e. the commitment of the supplier to cooperate with the organisation in any investigations undertaken by the organisation to resolve incidents that could affect the services or products provided to the organisation by the supplier and that are assumed or shown not to be attributable to the supplier or its suppliers;

f. the right to audit the supplier's suppliers equally to the supplier and within the scope of their involvement in the dematerialisation or conservation processes performed by the organisation;

g. the compliance of the supplier and its suppliers with the Luxembourg laws and regulations in force;

h. the contacts for each of the parties concerned with the contractual document, from a contractual, operational and information security point of view.

16 Information security incident management

16.1 Management of information security incidents and improvements

Additional implementation recommendations shall be:

16.1.1 Responsibilities and procedures

Implementation recommendations

The instructions specifying the point at which the incident management was activated, the restoration begun, and the authorities or clients concerned (internal or external to the organisation) were notified of this incident should be documented in a procedure.

Additional information

Cf. measure 6.1.6.

17 Information security aspects of business continuity management

A category of measures additional to ISO/IEC 27002:2013 shall be:

17.3 Business continuity and continuity of the SDC

Objective: To ensure correct management of the continuity of the SDC and the dematerialisation or conservation processes.

17.3.1 Organisation of continuity

Measure

The requirements should be determined for continuity of the dematerialisation or conservation processes in the event of an adverse situation such as a crisis or accident.

Implementation recommendations

The Return Time on Objective (RTO) and Recovery Point Objective (RPO) should be defined for assets within the perimeter, taking into account the requirements of clients and the obligation to return documents.

Additional information

The international standard ISO/IEC 22301:2014 on “Societal security – Business continuity management systems – Requirements” specifies the requirements for planning, setting up, implementing, operating, monitoring, reviewing, maintaining and improving a documented effective management system on an ongoing basis, in order to protect against disruptive incidents, reduce the probability of their arising, prepare for them and recover from them when they do arise. It enables any organisation, including a PSDC, to design a business continuity management system that is suited to its needs and which satisfies the requirements of the interested parties.

17.3.2 Implementation of continuity

Measure

Processes, procedures and measures should be established, documented, implemented and maintained to ensure the required level of continuity during an adverse situation.

Implementation recommendations

An activity resumption process should be defined which includes the dematerialisation or conservation processes and which takes into account the requirements of clients, the obligation to return documents, and risk scenarios that may interrupt the proper operation of an activity.

Continuity plans should be managed for the dematerialisation or conservation processes that make it possible to address adverse situations according to the defined conditions.

An activity resumption plan should be managed for the SDC that makes it possible to address adverse situations according to the defined conditions.

17.3.3 Verifying, reviewing and evaluating continuity

Measure

The implementation of measures relating to the continuity of the SDC should be verified at regular intervals to ensure that they are still valid and applicable during an adverse situation.

Implementation recommendations

The key elements of continuity plans and resumption plans should be tested.

18 Compliance

18.1 Compliance with legal and regulatory obligations

Additional implementation recommendations shall be:

18.1.3 Protection of records

Implementation recommendations

Evidence that the activities of the staff concerned comply with the policies and procedures relating to the dematerialisation or conservation process performed by the organisation should be conserved using appropriate storage media to ensure that they are properly conserved for as long as is necessary.

In particular, the following evidence should be kept:

a. SDC user activity reports;

b. SDC update and change reports;

c. event and incident reports associated with the dematerialisation or conservation processes;

d. SDC event log review reports;

e. in the case of dematerialisation processes:

   1. collection or delivery manifests for analogue documents;

f. in the case of archiving processes:

   1. conversion reports for the conversion of digital documents into digital archives;
   2. conversion reports for digital archives in the case of format changes.

Any evidence of the actions performed by the staff concerned should contain the following information in particular:

a. the identities of those responsible for the performed actions;
b. the dates and times of the performed actions;
c. the places where the actions were performed;
d. the assets used to perform these actions;
e. the assets involved in these actions;
f. the description of the performed actions;
g. any problems or errors encountered when performing these actions;
h. the clients concerned (internal or external).

18.2 Information security review

An additional measure to ISO/IEC 27002:2013 shall be:

18.2.4 Independent review of the compliance of the system and the dematerialisation or conservation processes

Measure

An internal SDC compliance audit should be performed in order to attest to the compliance of its operation, and of the actions performed by the staff concerned, with the detailed SDC description, with the specifications of the security mechanisms, with the dematerialisation and conservation policy, with the procedures and rules defined in these procedures and with the laws and regulations in force.

Implementation recommendations

This evaluation should ensure:

a. by sampling that the collected analogue documents have been correctly transformed into digital documents and subsequently destroyed or returned, and that the digital documents have been correctly maintained, returned or entered in an archiving process;
b. by sampling that the collected digital documents have been correctly conserved in the form of digital archives and then deleted and that these archives have been correctly created, maintained, returned, transferred or deleted;
c. that the critical SDC assets and the security mechanisms, such as the encryption mechanisms, have been evaluated and certified by independent bodies specialising in this type of review or that they are compliant with recognised reference systems or standards and that they are used in accordance with the relevant best practices;
d. by sampling that the administration, operation and security procedures, the process operating procedures and the rules defined in these procedures are respected.

Additional information

ISO/IEC 27007, entitled “Guidelines for information security management systems auditing” provides recommendations for the performance of ISMS audits, as well as guidelines on the competences of auditors, in addition to the guidelines of ISO 19011, which apply to management systems in general.

An additional measure to ISO/IEC 27002:2013 shall be:

18.2.5 Independent review of the SDC security

Measure

A technical audit should be performed of the SDC and its security mechanisms, in order to attest to the adequate security of the SDC and the correct operation of its security mechanisms, as indicated in the detailed SDC description.

Implementation recommendations

This technical audit should include tests, in particular, intrusion tests and privilege escalation tests and a conclusion by an experienced intrusion tester.

Additional information

The ISO/IEC TR 27008 technical report entitled “Guidelines for auditors on information security controls” provides recommendations for the review of the implementation and use of the security measures, including monitoring the compliance of the security measures. It explains the techniques that may be used for such a technical audit. The audit generally consists of an audit of the configuration of the systems and the activity of the system to verify the correct operation of each security mechanism, an external intrusion test and a privilege escalation test.

Annex A (normative): Objectives and reference measures specific to PSDCs

The objectives and measures listed in Table A.1 are based directly on those set out in Chapter 5, with which they are aligned, and must be used in the context of paragraph 6.1.4. of Clause 4.2 of this document. The declaration of applicability must justify the exclusion of all measures using the method adopted for risk assessment and treatment.

Table A.1 - Objectives and measures

A.5 Information security policies		
A.5.2 Management guidance regarding the dematerialisation or conservation policy		
Objective: Provide the management of the dematerialisation or conservation processes with guidance and support from the management, in accordance with the business requirements and the laws and regulations in force.		
A.5.2.1	Dematerialisation or conservation policies	*Measure* A dematerialisation or conservation policy must be defined, approved by the management, implemented, disseminated and communicated to the employees and the third parties concerned.
A.5.2.2	Review of the dematerialisation or conservation policy	*Measure* In order to guarantee that the dematerialisation or conservation policies are consistently relevant, appropriate and effective, these policies must be reviewed at scheduled intervals and in the event of major changes.
A.6 Organisation of information security and dematerialisation or conservation processes		
A.6.1 Internal organisation		
Objective: Establish a management framework to begin and then verify the implementation and operation of information security and dematerialisation or conservation processes within the organisation.		
A.6.1.1	Functions and responsibilities associated with information security and dematerialisation or conservation processes	*Measure* All responsibilities regarding information security and dematerialisation or conservation processes, in particular those related to the performance of the dematerialisation or conservation processes and those consisting of ensuring compliance of the processes and operational management with the policies and applicable documents, must be established and allocated.
A.6.3 Internal organisation specific to the dematerialisation and conservation processes		
Objective: Establish a management framework to ensure compliance with the specific legal requirements for the dematerialisation or conservation processes within the organisation.		
A.6.3.1	Verification of the digital documents before destruction of the corresponding analogue documents	*Measure* The content of digital documents must be checked against the analogue documents if the latter are scheduled to be destroyed after they have been scanned.
A.6.3.2	Dual control principle regarding the modification or deletion of digital archives	*Measure* The organisation must ensure that any modification or deletion of the created digital archives which was not scheduled during the definition of the conservation project must be approved by two users with operator rights.

A.6.3.3	Evidence management	*Measure* A procedure must be established and implemented for adequate evidence management for the SDC's operations and the actions performed by the staff concerned.
A.6.3.4	Relations with the national authority	*Measure* Procedures must be implemented to notify the competent authorities, in particular ILNAS, of the anticipated significant changes which may impact the information security and the operational activities, as well as of any security breach or loss of integrity which has a potentially significant incidence on the dematerialisation or conservation service as soon as possible and in any event within twenty-four hours after becoming aware of it.
A.6.4 Organisation of the dematerialisation and conservation processes involving clients		
Objective: Clarify the responsibilities of the PSDC and of its clients and ensure transparency for clients regarding the security and use of the dematerialisation or conservation processes.		
A.6.4.1	Security in client agreements	*Measure* The PSDC must define the conditions under which the dematerialisation or conservation processes are performed, as well as the information security requirements associated with these processes, with the client, in a contractual document approved by the client and the PSDC.
A.6.4.2	Obligation to inform the client in advance	*Measure* Prior to any contractual relation with a holder, the PSDC must make information relating to the condition for service provision, in particular, any information legally required to ensure a transparent service, available on durable media and in easily understandable terms.
A.6.4.3	Classification of the client's assets	*Measure* For all their analogue or digital documents and all their digital archives, the clients must define with the PSDC the classification level, the retention time, as well as other possible security requirements such as specific access rights.
A.6.4.4	Obligation to inform the client in the event of changes or incidents	*Measure* Prior to the application or at the earliest opportunity, the PSDC must inform the internal or external clients concerned of any changes to the prior information and to the information associated with the contractual obligations, as well as of any incidents which may jeopardise the clients' information, whilst providing them with the necessary justifications.

A.7 Human resource security		
A.7.2 During employment		
A.7.2.4	Policy commitment	*Measure* If the internal staff or the suppliers' staff are involved in the operational management of the security or the dematerialisation or conservation processes, they must understand and commit in writing to complying with the security policy and the dematerialisation or conservation policy.
A.8 Asset management		
A.8.1 Responsibility for assets		
A.8.1.4	Partitioning of secret information or personal information	*Measure* Any secret information or personal information must be sufficiently partitioned so that it is possible to respond to the owner's request to destroy it without endangering other archived information or evidence of the proper management of other dematerialised or conserved information.
A.9 Access control		
A.9.1 Business requirements concerning access control		
A.9.1.3	Effective segregation associated with access rights	*Measure* Three different people must be involved in the management of an access right: one to authorise the access, one to check compliance with the security requirements and finally one to grant access to the systems.
A.10 Encryption		
A.10.1 Encryption measures		
A.10.1.3	Two-factor authentication measures	*Measure* For persons interacting with the technical assets of the conservation system or accessing digital documents and digital archives, the PSDC must provide appropriate secure authentication based on encryption mechanisms and, if access is possible from premises not requiring two-factor authentication, a two-factor authentication process.
A.10.1.4	Protection of the integrity of digital documents or digital archives	*Measure* The integrity of digital documents collected by the conservation system and digital archives generated by the conservation system must be protected using appropriate encryption algorithms and techniques.
A.10.1.5	Protection of the integrity of internal documents	*Measure* The integrity of internal SDC documents and associated processes must be protected, particularly the SDC event logs, with protocols using appropriate encryption algorithms and techniques.

A.10.1.6	Electronic signature of internal documents	*Measure* Users of the SDC must use a qualified signature or a mechanism offering a similar guarantee to validate the internal documents necessary in order to demonstrate the correct operation of the SDC and its associated processes.
A.10.1.7	Protection of document transmissions	*Measure* The transmission of information and digital documents must be protected with protocols using appropriate encryption algorithms and techniques.
A.10.1.8	Conservation of electronic signatures	*Measure* If the integrity of a digital document to be archived depends on an electronic signature, the document must be conserved together with evidence that the signature has been verified no later than at the time of archiving.
A.11 Physical and environmental security		
A.11.1 Secure areas		
A.11.1.7	Accompanying visitors	*Measure* An authorised member of the PSDC must constantly accompany all visitors to the PSDC, even if they have already been authorised to access these areas.
A.12 Usage security		
A.12.1 Usage procedures and responsibilities		
A.12.1.5	SDC usage procedures	*Measure* Procedures must be defined, implemented and monitored by the staff concerned (of the PSDC and its suppliers), concerning administration, SDC operations, use of the dematerialisation or conservation process and control of the SDC security and processes, including all of the necessary rules to be followed in order to guarantee the properties of confidentiality, integrity, availability, authenticity, reliability and usability.
A.12.4.5	Usability of the event logs	*Measure* The event logs generated must be conserved in a usable form and protected against any unauthorised use and deletion, to ensure that all of the events recorded by these mechanisms remain traceable for as long as necessary.
A.12.8 Correct and secure management of the SDC		
Objective: To ensure the correct and secure management of analogue documents to be dematerialised, digital documents and digital archives during the dematerialisation or conservation process.		
A.12.8.1	Adequacy of the SDC	*Measure* The PSDC must demonstrate that the SDC is made up of technical assets and security mechanisms that meet the needs of clients and make it possible to guarantee the authenticity, reliability and usability of the analogue documents to be dematerialised, the digital documents and the digital archives managed by this system.

A.12.8.2	Detailed description of the SDC	*Measure* A detailed and comprehensible description of the SDC must be defined and maintained, comprising the technical assets, functional and operational aspects, as well as the flows and dependencies between the various components.
A.12.8.3	SDC security mechanisms	*Measure* The PSDC must manage and document the SDC security mechanisms guaranteeing the authenticity, reliability and usability of the analogue documents, digital documents and digital archives managed by this system.
A.12.8.4	Supervision of the SDC operational aspects	*Measure* The SDC operational aspects such as the space available and the failure rate of redundant components must be regularly evaluated.
A.12.8.5	Regular control of the integrity of the SDC	*Measure* Mechanisms must be implemented for regular controls of the SDC integrity and of the information necessary in order to ensure traceability.
A.15 Supplier relations		
15.1 Information security in supplier relations		
A.15.1.4	Contractual terms and conditions for the suppliers involved in the dematerialisation and conservation process	*Measure* The PSDC must include conditions that ensure compliance with the security policy and the dematerialisation and conservation policy in the contracts concluded with each supplier involved in the dematerialisation and conservation process.
A.17 Information security aspects of business continuity management		
A.17.3 Business continuity and continuity of the SDC		
Objective: To ensure correct management of the continuity of the SDC and the dematerialisation or conservation processes.		
A.17.3.1	Organisation of continuity	*Measure* The requirements must be determined for continuity of the dematerialisation or conservation processes in the event of an adverse situation such as a crisis or accident.
A.17.3.2	Implementation of continuity	*Measure* Processes, procedures and measures must be established, documented, implemented and maintained to ensure the required level of continuity during an adverse situation.
A.17.3.3	Verifying, reviewing and evaluating continuity	*Measure* The implementation of measures relating to the continuity of the SDC must be verified at regular intervals to ensure that they are still valid and applicable during an adverse situation.

A.18 Compliance		
A.18.2 Information security review		
A.18.2.4	Independent review of the compliance of the system and the dematerialisation or conservation processes	*Measure* An internal SDC compliance audit must be performed in order to attest to the compliance of its operation, and of the actions performed by the staff concerned, with the detailed SDC description, with the specifications of the security mechanisms, with the dematerialisation and conservation policy, with the procedures and rules defined in these procedures and with the laws and regulations in force.
A.18.2.5	Independent review of the SDC security	*Measure* A technical audit must be performed of the SDC and its security mechanisms, in order to attest to the adequate security of the SDC and the correct operation of its security mechanisms, as indicated in the detailed SDC description.