STANDARDISATION IN E-ARCHIVING

REQUIREMENTS AND CONTROLS FOR DIGITISATION AND E-ARCHIVING SERVICE PROVIDERS

Alain Wahl

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

OBJECTIVES OF THIS PRESENTATION

Understand what information security is

Understand what an Information Security Management System (ISMS) is

Understand what are the activities of risk assessment and risk treatment

Understand what information security controls are

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

ILNAS

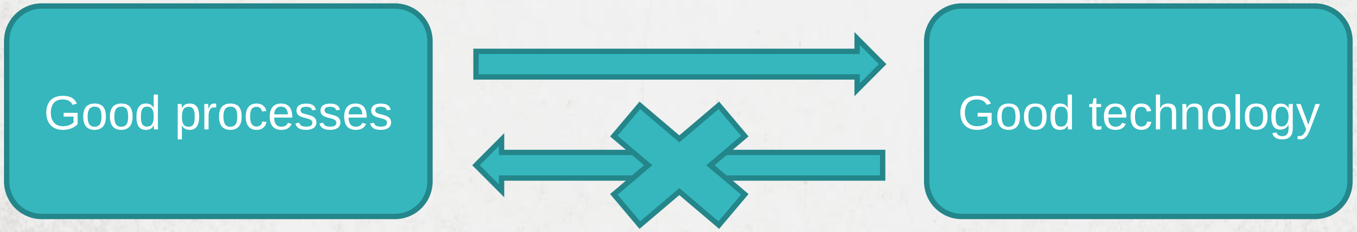
STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

INTRODUCTION

Information Security Management System (ISMS)

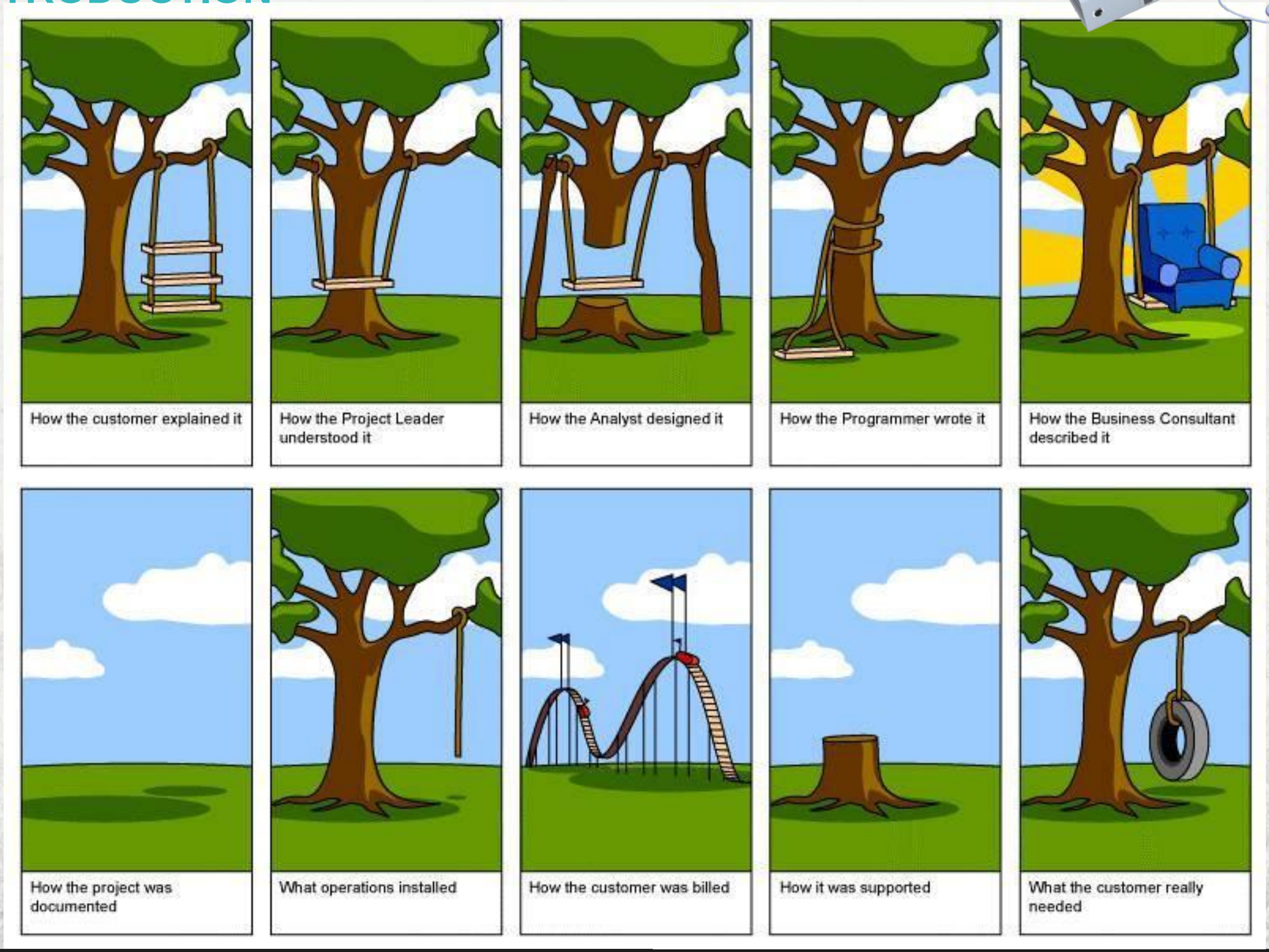
- Information security needs good management



STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

INTRODUCTION


How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
How the project was documented
What operations installed
How the customer was billed
How it was supported
What the customer really needed

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

INTRODUCTION

Information Security Management System (ISMS)

- Objectives
  - Reduce the number of incidents
  - Reduce the impact of incidents
  - Learn from own and others' experience

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

INTRODUCTION

Information Security Management System (ISMS)

- Bruce Schneier:
  - “Security is a chain: it is as strong as its weakest link”
- Kevind Mitnick:
  - “People are the weakest link.”

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

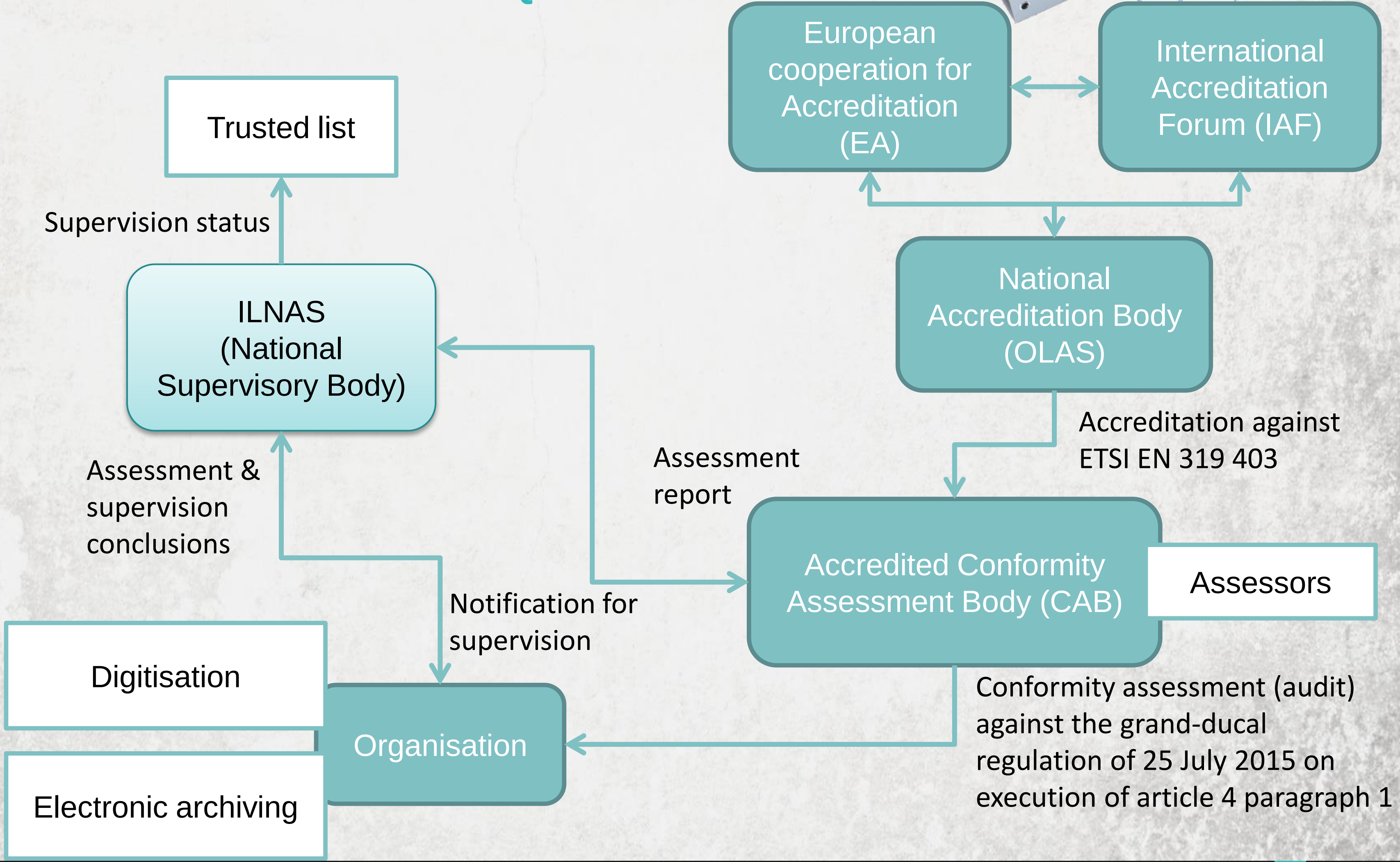
Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

STANDARDISATION IN E-ARCHIVING

Digital trust and e-archiving

SUPERVISION SCHEME FOR QUALIFIED PSDC



European cooperation for Accreditation (EA)

International Accreditation Forum (IAF)

Trusted list

Supervision status

National Accreditation Body (OLAS)

ILNAS (National Supervisory Body)

Accreditation against ETSI EN 319 403

Assessment & supervision conclusions

Assessment report

Accredited Conformity Assessment Body (CAB)

Assessors

Notification for supervision

Digitisation

Organisation

Electronic archiving

Conformity assessment (audit) against the grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Requirements and controls for certifying digitization or e-archiving service providers

Unique reference containing all the conditions for obtaining the qualified PSDC status

Based on international standards

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO 30301:2011

Published in the *Mémorial A* – N° 150 of 4 August 2015 (www.legilux.lu)

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

General concepts

- Description of the digitization and e-archiving processes
- Security framework

Information Security Management System (ISMS)

- Based on ISO/IEC 27001:2013
- Complements related to the digitisation process
- Complements related to the e-archiving process

Objectives and controls related to the security management and the operational management

- Based on ISO/IEC 27002:2013
- Complements related to the digitisation process
- Complements related to the e-archiving process

Appendixes

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Digitisation process

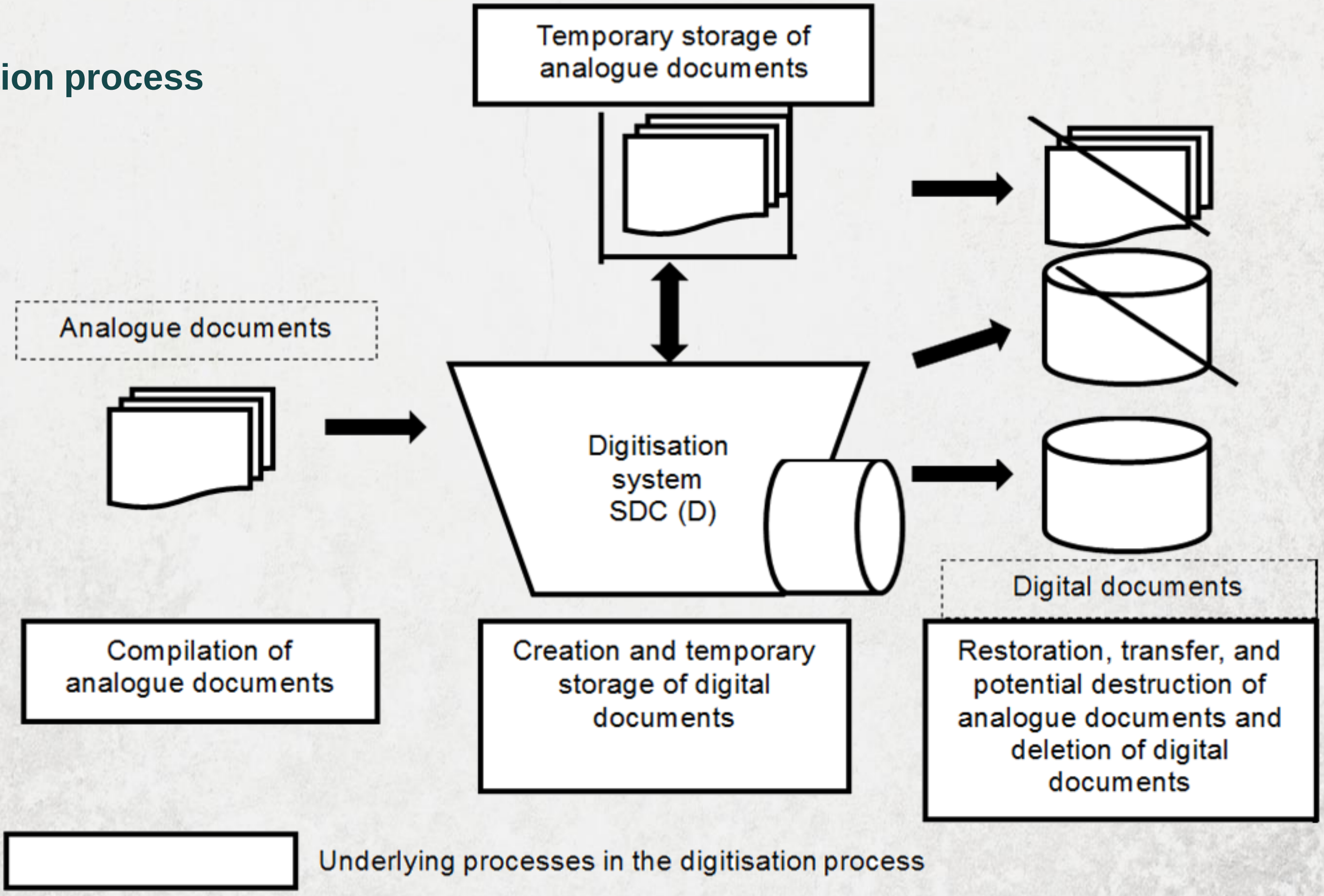

Temporary storage of analogue documents
Analogue documents
Digitisation system SDC (D)
Digital documents
Compilation of analogue documents
Creation and temporary storage of digital documents
Restoration, transfer, and potential destruction of analogue documents and deletion of digital documents
Underlying processes in the digitisation process

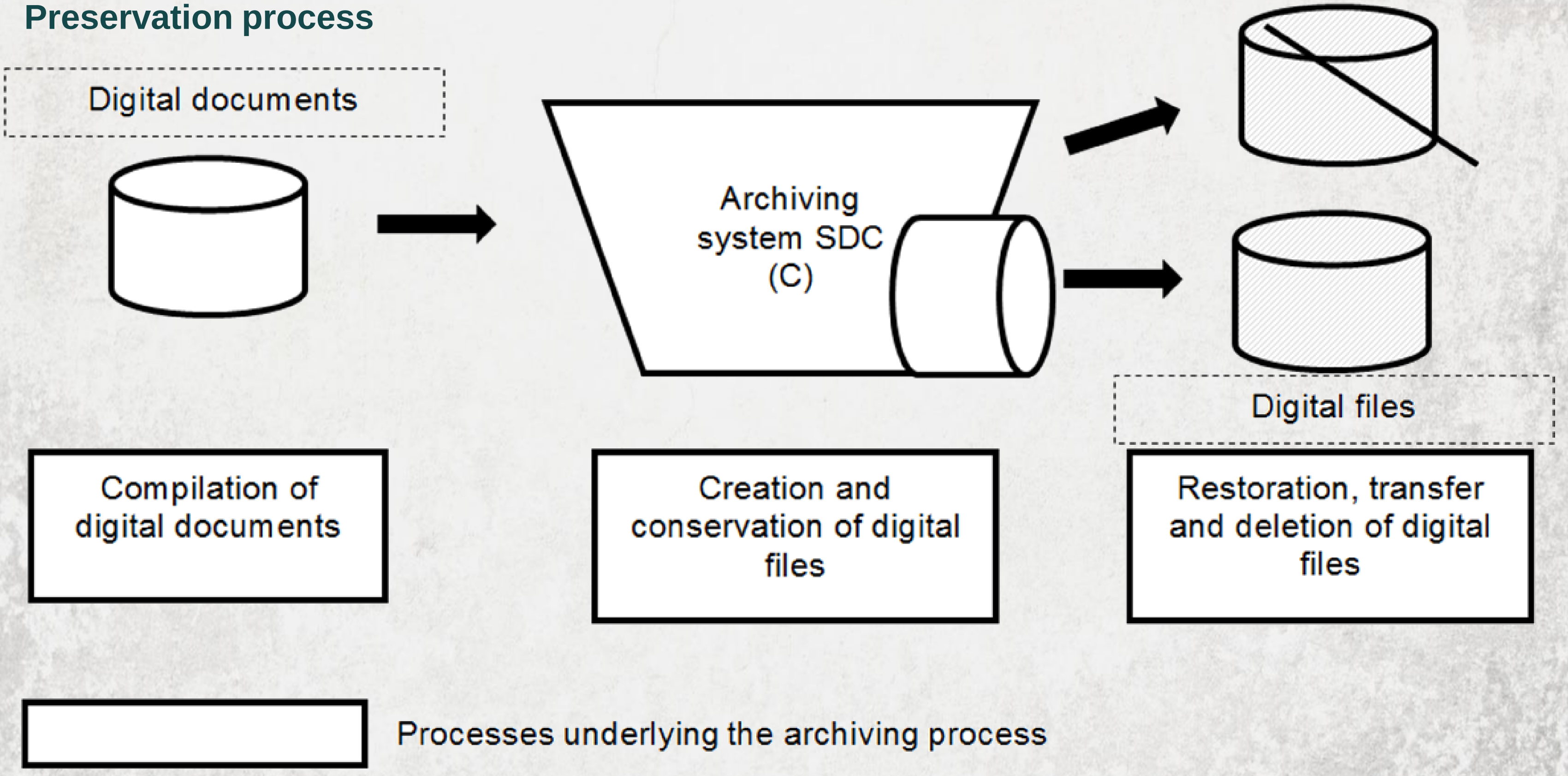
Figure 1: Digitisation process and underlying processes

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Preservation process



Digital documents

Archiving system SDC (C)

Digital files

Compilation of digital documents

Creation and conservation of digital files

Restoration, transfer and deletion of digital files

Processes underlying the archiving process

Figure 2: Archiving process and underlying processes

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- Management of the Information Security – Confidentiality, Integrity, Availability, Non-repudiation
- Management system
  - Set of procedures an organisation shall apply in order to reach its objectives
  - Systemizing of the organisation in its way of operating
- Define, implement, maintain and improve an ISMS
  - In order to manage the risks related to the processes of digitization and e-archiving
- Qualified PSDCs shall respect all the information security requirements specified in :
  - The international standard ISO/IEC 27001:2013
  - The clause 6 of the appendix of the grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1, completing the requirements

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- Applicable to any organisation
  - Small or big, for any product or service, for any sector
  - Everyone is concerned within the scope of the standard
- Continual improvement
  - An organisation or a company evaluates its situation, determines objectives and creates a strategy, invests actions to achieve these objectives, then evaluates the results and adapts the processes to improve (PDCA)
- Assessable
  - Someone may assess that there is no gap between the standard and the management system
  - Documentation – transition form oral tradition to scriptural tradition
  - Conformity assessment
  - Provides trust to stakeholders

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- Security controls
  - Organisational and technical setting allowing to reduce one or several security risks
  - Reducing vulnerability of the assets
  - Reducing impact of incidents
  - Prevent and anticipate threats

- Final aim of the discipline: Security of information system

- Management of security controls
  - Who is doing what?
  - When?
  - How?

- These controls are they:
  - Documented?
  - Appropriate and proportional? Efficient?

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- Management of conformity
  - Do I know the applicable requirements:
    Legal and regulatory
    Contractual
  - Am I able to listen them in terms of:
    Security controls?
    Security needs?

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- Risk Management
  - Which events on the information system could harm my information and my core business processes?
  - Do I know controls to reduce the risk of these events or to reduce the consequences?
  - Do I invest the resources needed for the risk management?
- Management of incidents
  - Do I identify events harming security of my information processes?
  - Do I establish the needed resources:
    To minimise the consequences?
    To insure business continuity?
  - Do I learn from my incidents?

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- Security policy
  - Are my management processes applicable to all my activities?
  - Are my activities coordinated?
  - Is my leadership involved in the security management?
  - Does my security management improve?

ILNAS

STANDARDISATION IN E-ARCHIVING
Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- 6.1 General requirements
  - ISMS in accordance with all the requirements specified in ISO/IEC 27001
- 6.2 Context of the organization
  - Understand the organisation and its context
  - Understand the needs and expectations of the stakeholders
  - Define the scope of the ISMS
- 6.3 Leadership involvement for the ISMS
  - Information security policy with objectives shall be defined
  - Necessary resources are available
  - ISMS achieves given goals
  - Guarantee of continued performance, in case of cessation of activity

ILNAS

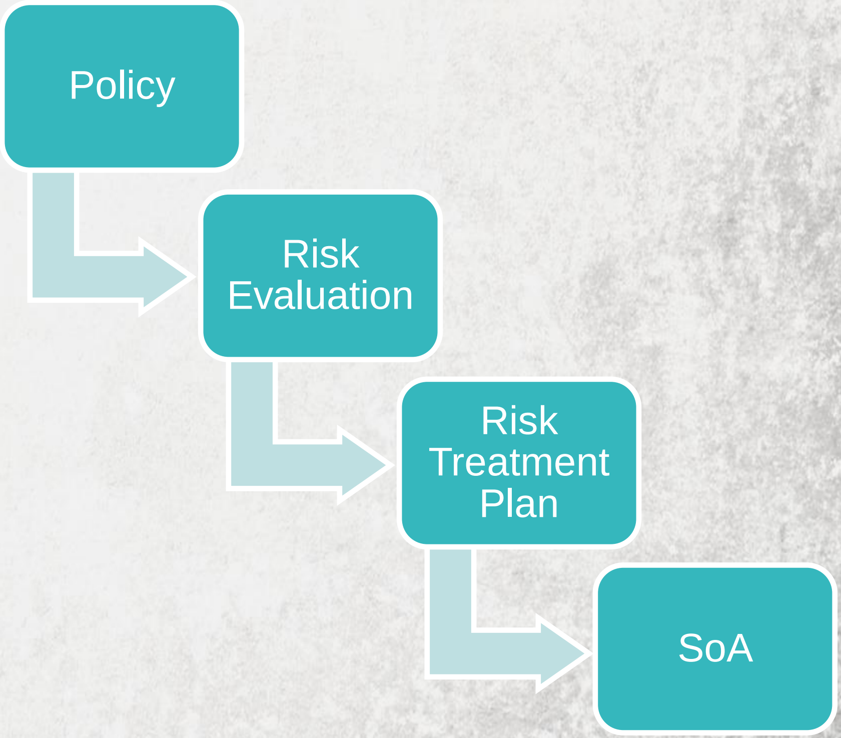
STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- 6.4 Planning the ISMS
  - The management shall establish a Security policy (objectives, commitment of the management, improvement)
  - Risk evaluation
  - Statement of Applicability (SoA) including controls of ISO/IEC 27002:2013
  - Controls can only be excluded if no risks or below level of risk acceptance
  - Any exclusion shall be documented and justified in SoA



Policy

Risk Evaluation

Risk Treatment Plan

SoA

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Management System (ISMS)

- 6.5 Evaluation of the performance of the ISMS
  - Internal audit, impartiality of auditors
  - Review at least once a year or in case of major changes
  - The Results of risk analysis
  - The financial stability of the organization
  - Management review
- 6.6 Improvement
  - Non-conformity and corrective action
  - React to non-conformities – corrective actions – management of consequences
  - Evaluate the need to eliminate causes of non-conformity
  - Establish actions and changes to ISMS if needed
  - Check effectiveness of corrective actions
  - Documentation

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management

- What is a risk?
  - Effect of uncertainty on objectives
  - An effect is a deviation from the expected – positive or negative (in information security we deal with negative effects)
  - Risk is often characterized by reference to potential events and consequences, or a combination of these.
  - Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

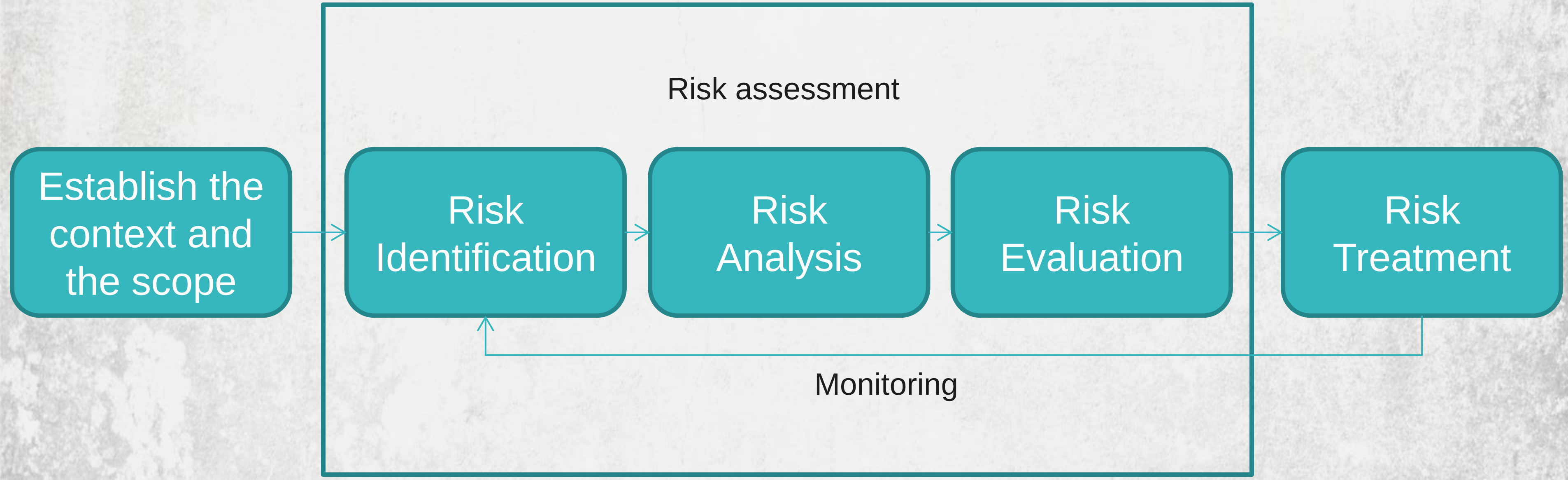
ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management



Risk assessment

Establish the context and the scope

Risk Identification

Risk Analysis

Risk Evaluation

Risk Treatment

Monitoring

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management

- Information security risk assessment
  - Identify the risks: threats
  - Examples:
    Virus intrusion
    Fire
    Spying
    Overload of information network
    Corruption of the data, violation of user rights
  - Vulnerabilities:
    Missing of daily update
    Portable database
    Policy of easy password
    Light internet network security
  - ISO/IEC 27005:2011

ILNAS

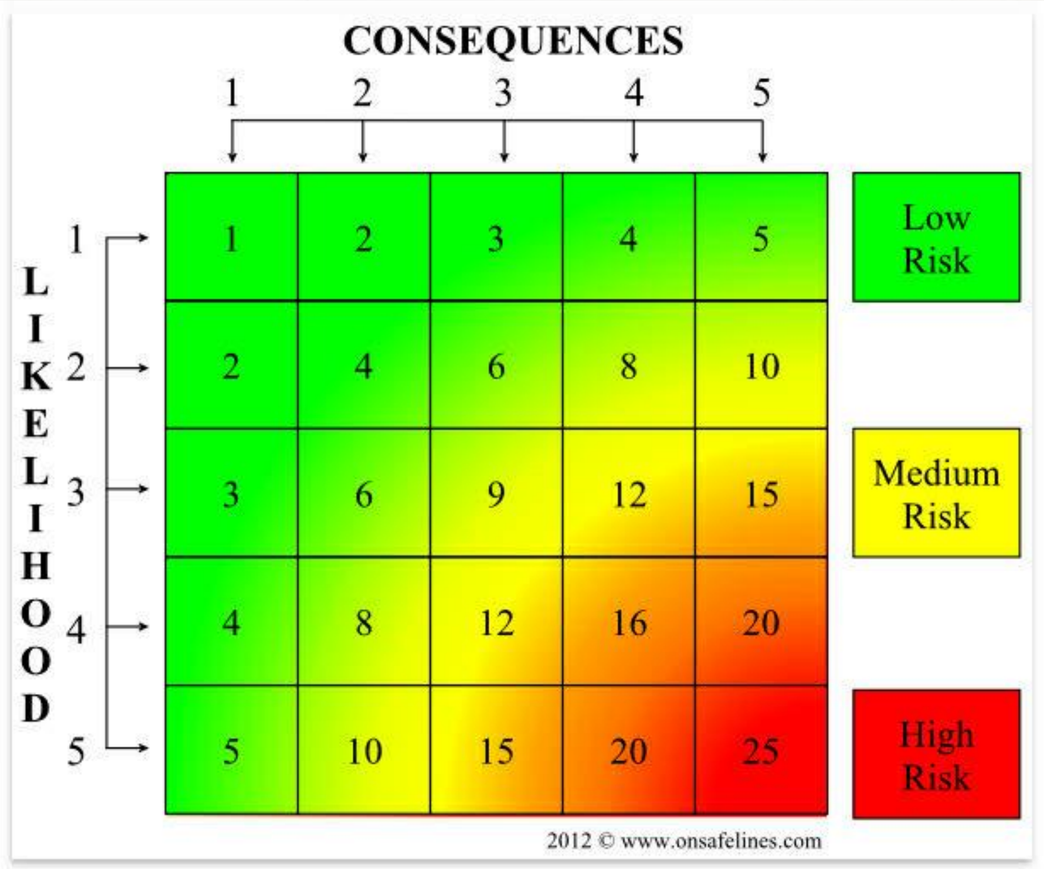
STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management

- R = L * C



CONSEQUENCES

LIKELIHOOD	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

🟩 Low Risk

🟨 Medium Risk

🟥 High Risk

2012 © www.onsafelines.com

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management

- Level of risk: magnitude of a risk expressed in terms of the combination of consequences and their likelihood

  $R = L * C$

- Threat: potential cause of an unwanted incident, which may result in harm to a system or organisation
- Consequence: outcome of an event affecting objectives
- Vulnerability: weakness of an asset or control that can be exploited by one or more threats

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management

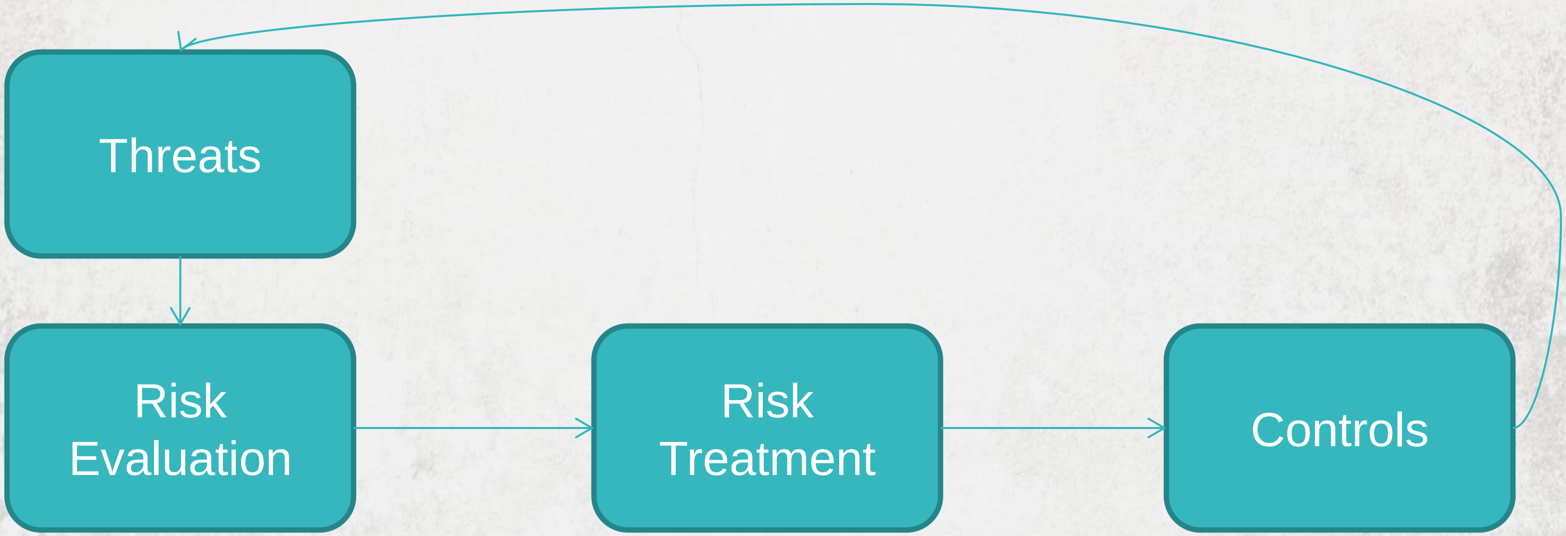
- Risk treatment
  - Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
  - Taking or increasing risk in order to pursue an opportunity
  - Removing the risk source (i.e. the threat; not applicable to information security)
  - Changing the likelihood (i.e. of the threat; to read as "changing the likelihood that and incident happens")
  - Changing the consequences
  - Sharing the risk with another party or parties (including contracts and risk financing)
  - Accepting the risk by informed choice

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Risk Management



Threats

Risk Evaluation

Risk Treatment

Controls

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

SUMMARY

Introduction

Supervision scheme for qualified PSDCs

Grand-ducal regulation of 25 July 2015 on execution of article 4 paragraph 1 of the law of 25 July 2015 on electronic archiving

- Information Security Management System (ISMS)
- Information Security Risk Management
- Information Security Controls

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Security recommendations or requirements
- Classical recommendations of security experts
  - Some controls are quite general, some precise
  - Some controls are applicable to all the organisation, some are applicable to specific areas
  - Provide recommendations which may be large and may include other security controls
- Selected to reduce risk to an acceptable level after their evaluation
- Policies (rules), documented procedures, guidelines, practices, organizational structures
  - Administrative
  - Technical
  - Legal

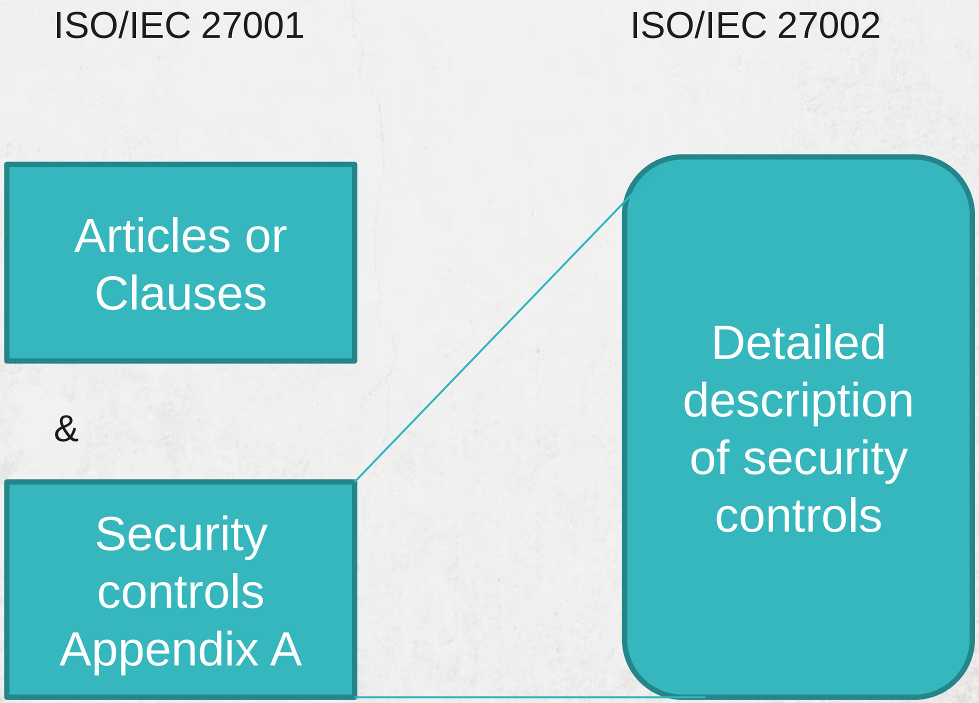
ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls


ISO/IEC 27001
ISO/IEC 27002
Articles or Clauses
&
Security controls Appendix A
Detailed description of security controls

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Security Policy
  - Provide a security orientation
  - Management support
  - Digitization policy
  - E-archiving policy
  - Take in account strategy, legal & contractual requirements, threats
  - Contain definition of information security, objectives and principles, responsibilities
  - Examples of content: access control, classification of information, physical security, backup, transfer of information, protection against malware, management of vulnerabilities, …
  - Revue of policies:
    Within regular intervals or during significant changes
    Shall be validated regularly by management

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Organisation of the information security
  - Management of information security
  - Control the implementation of information security
  - Roles and responsibilities in information security:
    Formalised attribution of responsibilities
  - Segregation of duties:
    Identification of roles
    Action, validation and supervision
    Limitation of gathering functions
  - Relationship with authorities:
    Updating the related listing
    Incident management to communicate

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Management of assets
  - Inventory of assets
  - Owners and responsibilities related to assets
  - Correct use of assets
  - Classification of information:
    Criteria – value, legal requirements, sensibility and criticality
  - Media handling – USB key, CDs, physical transfer

- Security of human resources
  - Before recruitment
  - During contract
  - End or modification of contract

ILNAS

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Access control
  - ○ Manage access to information
  - ○ User access management
    Registration and suppression of users
    Creation of accounts and access rights
    Management of privileged access rights
    Management of secret information for authentication
    Review of access rights
    Suppression and modification of access rights
  - ○ User responsibilities
  - ○ System and application access control
    Restricted access to information
    Procedure for secured connexion
    Use of software for privileged rights
    Access control to source code

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Physical and environmental security
  - Prohibit any non authorized access
  - Security zones
  - Material security

- Operational security and telecommunication
  - Documentation of operational procedures
  - Separate domains and tasks of responsibility
  - Separate testing, development and operational equipment
  - Protection against malware
  - Establish back-up copies
  - Management of network security
  - Supervision
  - Provide a correct and secured management of digitization and e-archiving processes

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015 ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Cryptography:
  - Policy for use of cryptography
  - Management of cryptographic keys
  - Management of keys and certificates
  - PKI
- Acquisition, development and maintenance of information systems
  - Monitoring the inclusion of security issues in the information systems
  - Good functioning of the application
  - Cryptographic controls

STANDARDISATION IN E-ARCHIVING

Requirements and controls for qualified PSDCs

GRAND-DUCAL REGULATION OF 25 JULY 2015
ON EXECUTION OF ARTICLE 4 PARAGRAPH 1

Information Security Controls

- Management of information security incidents
  - Reporting of incidents and failures
  - Management of improvements and incidents

- Management of business continuity activity
  - Prevent interruptions

- Conformity
  - Conformity with legal requirements
  - Conformity to policy and standards
  - Consideration of the audit report

THANK YOU

For Your Attention

For more information:

ILNAS

ILNAS – Département de la confiance numérique
1, Avenue du Swing
L-4367 Belvaux

☎ (+352) 247 743 50
(+352) 247 943 50

www.portail-qualite.lu

alain.wahl@ilnas.etat.lu