eurolab aisbl
European Federation of National Associations of Measurement, Testing and Analytical Laboratories

Technical Report No. 01/ 2024

October 2024

Technical Report

Guidelines for the management of digitalised systems in laboratories accredited to ISO/IEC 17025

Author:
Edouard Salingros
Gembloux Agro-Bio Tech, University of Liège, 5030 Gembloux, Belgium

Impressum

EUROLAB Technical Report 1/2024
“Guidelines for the management of digitalised systems in laboratories accredited to ISO/IEC 17025”

October 2024

EUROLAB General Secretariat
Rue du Commerce 20-22
1000 Brussels
BELGIUM

Phone: +32 2 511 50 65
e-Mail: info@eurolab.org
URL: www.eurolab.org

Table of contents

Foreword

EUROLAB (the European Federation of National Associations of Measurement, Testing and Analytical Laboratories) is a not-for-profit organisation representing laboratories, coordinating their efforts to address common challenges and promote good practices by sharing knowledge, organizing seminars and working groups; and publishing position papers, technical reports and newsletters.

The present guidelines have been reviewed by EUROLAB members and a special thanks are addressed to Anton Blöth (convenor of the Digitalisation working group, VUP), other VUP members, Tobias Pflock and Alexander Frenzl (Audittrails) and to Christian Mueller-Schoell (Mettler-Toledo) for their feedback.

Comments and feedback for the next edition can be sent to the following e-mail addresses:

- edouard.salingros@uliege.be
- secretariat@eurolab-aisbl.eu

1. Introduction and scope

1.1 Introduction

The ISO/IEC 17025:2017 standard [1] lays down requirements for laboratories to demonstrate that they are competent, operate consistently and deliver reliable results. These requirements include the implementation of a management system based on risks and opportunities.

Digitalisation of laboratory activities represents an opportunity with considerable benefits, including reduced risks of human mistakes, faster communication, improved measurement performance, safety, workforce efficiency, information security and data processing capability. However, it also comes with specific risks that the laboratory has the responsibility to keep under control. Digitalisation has often taken place (and sometimes still does) without these risks being properly considered and addressed.

Because few requirements of the ISO/IEC 17025:2017 [1] explicitly mention computer systems and digital technologies, it can be difficult to determine how to meet ISO/IEC 17025:2017 [1] requirements when they apply to digitalised processes.

Topics and purposes of ISO/IEC 27001 [2] (on information security management systems) and ISO/IEC 27002 [3] (on related controls) are closely related to those of the present guidelines. However, although compliance to ISO/IEC 27001 [2] (with the support of ISO/IEC 27002 [3]) will drastically help laboratories to meet requirements of ISO/IEC 17025 [1] and recommendations of the present guidelines, it is likely not sufficient to fully address all of them.

Compliance to ISO/IEC 27001 [2] is likely not sufficient to fully address requirements of ISO/IEC 17025 [1] which apply to information security and digitalised system management (although it helps).

1.2 Scope

The goals of the present guidelines are: - To help laboratories meet requirements of ISO/IEC 17025:2017 [1] when they apply to digitalised processes - To help accreditation bodies to evaluate these requirements; - To advise on good practices that can be found in other guidance documents; - To be accessible to all readers without specific knowledge or expertise in information technology.

For this purpose, clauses of the ISO/IEC 17025:2017 [1] that are directly or indirectly applicable to computer systems are identified, and recommendations are formulated based on ISO/IEC 27002 [3] and other standards and guidelines.

The present guidelines are not intended to: - Be exhaustive; - Substitute for sector-specific standards, guidelines or regulation (especially personal data regulation such as the GDPR regulation [4], and national regulation adopted in application of Directive 2022/2555 (NIS2) [5]); - Explain or comment in detail specific technologies and techniques; - Serve as a standard or check-list that should be fully implemented to satisfy ISO/IEC 17025:2017 [1].

The chapters of the present guidelines are as follows:

- Section 3 lists definitions of relevant terms from other standards and guidelines. Definitions specific to the present guidelines are formulated where no appropriate definition was found;
- Section 4 provide general recommendations regarding risk assessment of digital processes and expand on a specific risk assessment approach consisting in the definition of risk classes attributed to the laboratory's computer systems;
- Section 5 identifies relevant risks that may result in compromised accuracy of test results and/or information security, factors influencing them and controls that can be implemented to mitigate them;
- Section 6 provides recommendations on the implementation of certain controls, based on ISO/IEC 27002:2022 [3] and other standards and guidelines;
- Section 7 summarises links between ISO/IEC 17025:2017 [1], ISO/IEC 27001:2022 [2] and the present guidelines.

2. Normative references

The present guidelines are non-binding. Therefore, only ISO/IEC 17025:2017 [1] is considered a normative reference. All other references are informative.

Since the present guidelines specifically deal with information security, further reference to ISO/IEC 27002:2022 [3] is highly recommended.

3. Definitions

This section defines important terms and concepts required to understand the present guidelines. Definitions from existing standards documents are adopted when available.

Acceptance testing

"Test to determine that a system, subsystem, component or functional part is capable of meeting performance requirements prescribed in a purchase specification or other document specifying what constitutes the adequate performance capability for the item and to demonstrate that the item is free from manufacturing defects." [6]

"Formal testing conducted to enable a user, customer, or other authorised entity to determine whether to accept a system or component." [7]

For the purpose of the present guidelines, acceptance testing is defined as "form of validation of digitalised process and computer systems".

Acceptance criteria

"Criteria that a system or component must satisfy in order to be accepted by a user, customer, or other authorised entity." [7]

Note: acceptance criteria are used during acceptance testing.

Access control

"Means to ensure that access to assets is authorized and restricted based on business and security requirements." [8]

"Granting or denying an operation to be performed on a resource. Note 1 to entry: A primary purpose of access control is to prevent unauthorised access to information or use of ICT (information and communications technologies) resources based on the business and security requirements; that is, the application of authorisation policies to particular access requests. Note 2 to entry: When an authenticated subject makes a request, the resource owner will authorise (or not) access in accordance with access policy and subject privileges." [9]

Access right

"Authorisation to a subject to access a resource. Note 1 to entry: Privilege is a necessary but not sufficient condition for access. Access occurs when the access request is granted according to its access control policy. The access control policy is based on privileges and may include other environmental factors (*e.g.* time-of-day, location, *etc.*). […] Note 3 to entry: A resource may have multiple distinct privileges associated with it which correspond to various defined levels of access. For example, a data resource could have read, write, execute and delete privileges available for assignment to subjects. A request by a subject for access to the resource might be allowed for some levels of access request but disallowed for other levels depending on the level of access requested and the resource privileges that have been assigned to the subject." [9]

"Permission for a subject to access a particular object for a specific type of operation. Note 1 to entry: Example: Permission for a process to read a file but not write to it." [10]

Note: examples of access rights are:

- Consultation of items;
- Introduction/creation of items;
- Modification of items;
- Deletion of items;
- Modification of access rights to the items.

For the purpose of the present guidelines, "access right" is considered a synonym of "permission".

Accuracy (of a measurement)

"Closeness of agreement between a measured quantity value and a true quantity value of a measurand." [11]

"Closeness of agreement between a test result and the accepted reference value." [12]

Adaptability

"Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments." [13].

Advanced electronic signature

Electronic signature which meets the requirements laid out in Article 26 of eIDAS regulation [14]

Agile development

"Software development approach based on iterative development, frequent inspection and adaptation, and incremental deliveries, in which requirements and solutions evolve through collaboration in cross-functional teams and through continuous stakeholder feedback." [7]

Amend

"Make changes in record content in order to make it fairer, more accurate, consistent, complete and/or up-to-date." [15]

Analogue data

"Data represented by a physical quantity that is considered to be continuously variable and whose magnitude is made directly proportional to the data or to a suitable function of the data." [10]

Anonymisation

"Process of removing, obscuring, aggregating, or altering identifiers with the aim of preventing the identification of individuals to whom data originally related." [16]

Antivirus software

"Software used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system." [17]

Application software

"Software or program that is specific to the solution of an application problem. Note 1 to entry: Example: A spreadsheet program." [10]

Archiving

"Process of protecting records from the possibility of being further altered or deleted and storing these records under the control of independent data management personnel throughout the required retention period. Archived records should include, for example, associated metadata and electronic signatures." [18]

For the purpose of the present guidelines, "archiving" means "Process of indexing and applying access control measures for the purpose of protecting what is being archived against alteration or loss."

See also the definition of "electronic archiving".

Asymmetric encryption system

"System based on asymmetric [cryptographic] techniques whose public transformation [defined by the public key] is used for encryption and whose private transformation [defined by the private key] is used for decryption." [19]

Audit

"Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled." [20]

Audit trail

"Secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record." [1]

"Aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information system." [21]

"Form of metadata that contains information associated with actions that relate to the creation, modification or deletion of electronic data. An audit trail provides an automated secure way of recording life cycle details such as creation, additions, deletions or alterations of information in an electronic record without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record, including the 'who, what, when and why' of the action." [22,23]

Note: examples of audit trail include:

- At the document level: the "track changes" features in popular text processing and spreadsheets application software;

- Automatic versioning of EDMS.

Authentication

“Provision of assurance that a claimed characteristic of an entity is correct.” [8]

“Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.” [17]

Authenticity

“Property that an entity is what it claims to be.” [8]

“Capability of a product to prove that the identity of a subject or resource is the one claimed.” [13]

Availability

“Property of being accessible and usable upon demand by an authorized entity.” [8]

“Degree to which a system, product or component is operational and accessible when required for use.” [7]

Backdoor

“An intentional and undisclosed mechanism (to the customer/user) in a product, service, or facility which is intended to provide access to assets and artifacts by an unauthorized party.” [24]

Backup

“Process to copy/export data to the data storage of an external backup device to retrieve and restore this data in case of a storage fault. The copy is referred to as backup copy.” [25]

“Duplicate of stored data. Note 1 to entry: It is recommended to store the backups at a remote site in case of a disaster.” [26]

“A copy of one or more electronic files created as an alternative in case the original data or system are lost or become unusable (for example, in the event of a system crash or corruption of a disk). It is important to note that backup differs from archival in that back-up copies of electronic records are typically only temporarily stored for the purposes of disaster recovery and may be periodically overwritten. Such temporary back-up copies should not be relied upon as an archival mechanism.” [18]

Backward compatibility

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “backward compatibility” is defined as “interoperability between newer and older computer system, module, hardware or software”.

Backward recovery

"Kind of recovery in which a system, program, file, database, or other resource is restored to a previous state in which it can perform required functions. Note 1 to entry: Example: The reconstruction of a file to a given state by reversing all changes made to the file since it was in that state." [10]

Baseline

"Formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle." [27]

"Specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures." [28]

"A baseline, together with all approved changes to the baseline, represents the current approved configuration. The term is thus used to refer to a particular version of a software configuration item that has been agreed on, *e.g.*, as a stable base for further development or to mark a specific project milestone. In either case, any new baseline is agreed through the project's agreed change control procedures." [7]

Brute-force attack

"Trial-and-error attempt to violate computer security by trying possible values of passwords or keys." [10]

Burning (on an optical storage medium)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "burning" is defined as "Process of transcribing electronic data on an optical storage medium".

Note: burning is often achieved using laser technology.

Biometric authentication

"Authentication where biometric verification or biometric identification is applied and the identity is linked to the biometric reference." [29]

Black-box testing

"Testing that ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions." [7]

"Testing conducted to evaluate the compliance of a system or component with specified functional requirements." [7]

For the purpose of the present guidelines, "black-box testing" is considered a synonym of "functional testing".

Blockchain

“Distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links. Note 1 to entry: Blockchains are designed to be tamper-resistant and to create final, definitive and immutable ledger records.” [30]

Calibration

“Operation that, under specified conditions, in a first step, establishes a relation between the quantity values with measurement uncertainties provided by measurement standards and corresponding indications with associated measurement uncertainties and, in a second step, uses this information to establish a relation for obtaining a measurement result from an indication.” [11]

Centralised data storage

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “centralised data storage” is defined as “data management paradigm where the storage and remote access of data is under the control and management of a single party/entity, usually using its own data storage system(s) and server(s).”

Note: the opposite of centralised data storage is decentralised data storage.

Change control

“A process whereby modifications to documents, deliverables, or baselines associated with the project are identified, documented, approved, or rejected.” [7]

For the purpose of the present guidelines “change control” is considered a synonym of “version control”.

Ciphertext

“Data which has been transformed to hide its information content.” [19]

Credentials

“Data that are transferred to establish the claimed identity of an entity.” [10]

Cryptographic deletion

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “cryptographic deletion” is defined as “process of encrypting data without retaining the key necessary for decryption for the purpose of deleting them by making them unusable”.

Cloud computing (services)

“Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.” [20]

Cloud computing services may consist of the provision of various capabilities and categories. For more details, see definitions in the ISO/IEC 22123-1 [20].

Note: cloud computing does not necessarily involve external providers. Cloud computing can be developed, hosted and maintained on-premise.

Code injection attack

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “code injection attack” is defined as “a type of cyberattack in which the attacker executes malicious code by injecting it through a text field such as a search box”.

Note: SQL injection attacks are a common type of code injection attack where malicious SQL code is inserted in a query to reach an SQL database and thereby unduly steal, modify or delete data.

Commercial Off-The-Shelf (COTS)

“COTS software products are ready-made packages sold off-the-shelf to the acquirer who had no influence on its features and other qualities. Typically, the software is sold pre-wrapped with its user documentation.” [31]

“Product available for purchase and use without the need to conduct development activities” [32]

Note: COTS are a subcategory of OTS and are usually proprietary.

Computer system

“One or more computers, peripheral equipment, and software that perform data processing” [10]

“A system containing one or more computers and associated software.” [33]

Computer system related services

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “computer system related services” is defined as “any service related to computer system, including (but not limited to) delivery, installation, license activation, maintenance, training, provision of other cloud computing services as defined in ISO/IEC 22123-1 [20]”.

Computerisation

“Automation by means of computers” [10]

Note: computerisation is a form of digitalisation.

Computerised system

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

Note: the terms "computerised system" are often used with the same signification as the retained definitions of the terms "digitalised process" in the present guidelines. Therefore, these terms are considered as synonyms.

Confidentiality

"Degree to which a product or system ensures that data are accessible only to those authorized to have access." [13]

"Property that information is not made available or disclosed to unauthorized individuals, entities, or processes." [8]

Configuration item

"Entity within a configuration that satisfies an end use function and that can be uniquely identified at a given reference point." [28]

"Configuration items can vary widely in complexity, size and type, ranging from an entire system including all hardware, software and documentation, to a single module or a minor hardware component." [7]

Control

"Measure that is modifying risk. Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk." [2]

Note: preventive actions and corrective actions can be regarded as example categories of controls aimed to reduce the risk of non-conformity.

Corrective action

"Action to eliminate the cause of a nonconformity and to prevent recurrence. […] Corrective action is taken to prevent recurrence whereas preventive action is taken to prevent occurrence." [34]

Cryptographic key

"Sequence of symbols that controls the operation of a cryptographic transformation [*e.g.* encryption, decryption]" [19]

Cryptojacking

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "cryptojacking" is defined as "a type of cyberattack in which an attacker exploits the computational power of its target to mine cryptocurrencies".

Note: the victims are often unaware of the attack as the only sign of it is slower operation in general. This type of attack can be conducted through code embedded in a web page (such as an advertisement) and therefore does not necessarily involves any malware to be downloaded on the victim's machine.

Custom (or customised) (system or software)

"Software product developed for a specific application from a user requirements specification" [35]

Note: a custom-made system can be either developed and provided by an external provider or developed in-house.

Cyber threat

"Potential cause of an unwanted cybersecurity incident, which can result in harm to a system, people, society, organisation, or other entities in cyberspace" [36]

Cyberattack

"Malicious attempts to exploit vulnerabilities in information systems or physical systems in cyberspace and to damage, disrupt or gain unauthorized access to these systems. Note 1 to entry: Expression of an offensive operation in or through the cyberspace leading to unauthorized use of services, creating illicit services, orchestrating denial of service, altering or deleting data or resources." [36]

"Attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." [37]

"Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." [38]

Note: examples of cyberattacks techniques include:

- Malwares such as Ransomware;
- Distributed denial of service (DDoS) attacks;
- Man-in-the-middle attacks;
- Code injection attacks;
- Cryptojacking;
- Spoofing;
- Phishing;
- Brute-force attacks;
- Exploitation of backdoors or other kind of vulnerabilities.

Cyberspace

"Interconnected digital environment of networks, services, systems, people, processes, organisations, and that which resides on the digital environment or traverses through it." [36]

Data

“Reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.” [39]

“Quantitative or qualitative facts, figures and statistics collected for reference or analysis.” [22]

“Data can have different formats (*e.g.* analogue, digital) and structure, layouts (*e.g.* on paper or on screen), sources (*e.g.* chromatography charts, text, image, video, *etc.*), and media used to store or present (paper, DVD, photo film, tape, electronic files, *etc.*).” [22]

“Data may be captured or recorded: - by manual recording, on paper or in an electronic system, of an observation or of an activity; - by automatic recording, on paper (by automatic printing) or in an electronic system, using equipment that range from simple instruments through to complex highly configurable computerised systems; - using a hybrid system where combinations of paper (or other non-electronic media) and electronic records constitute the raw data; - on other means of media such as photography, imaging methodologies and technologies, chromatography plates, *etc.* that could be generated manually, or automatically or using a hybrid system.” [22]

For the purpose of the present guidelines, “data” include raw data, derived data and metadata from all sources, including (but not limited to) testing activities, calibration, SST and other forms of verification (such as quality control samples), monitoring of environmental conditions, client, external provider, personnel.

Data can be mono-dimensional (*e.g.*, a mass) or multi-dimensional (*e.g.*, a chromatogram is a set of data points, each being a set of multiple quantities including time among them).

Data breach

“Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed” [40]

Note: a data breach is a potential consequence of cyber threats such as a cyberattacks or insider attacks.

Data logger

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “data logger” is defined as “a computer system used to measure environmental parameters (such as temperature and humidity) at relative interval and store and/or transmit the acquired data.”

Data masking

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “data masking” is defined as “process of obfuscating or anonymizing specific data within a database to protect sensitive information while maintaining the data’s usability for various purposes such as testing, development, or analytics.” The goal is to create a

version of the data that is structurally similar but with masked or altered details, ensuring that sensitive information cannot be easily accessed or identified.

Note: examples of Data masking techniques include:

- Anonymisation;
- Encryption;
- Replacing a value with their hash value

Data model

"Pattern of structuring data in a database according to the formal descriptions in its information system and according to the requirements of the database management system to be applied." [10]

Data processing system

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "data processing system" is considered a synonym of "computer system".

Data wiping

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "data wiping" is defined as "process of overwriting data with random data at its specific physical location in a file system for the purpose of non-recoverable deletion".

Database

"Collection of machine-readable information organized so that it can be easily accessed, managed and updated." [39]

"Collection of data organized according to a conceptual structure describing the characteristics of these data and the relationships among their corresponding entities, supporting one or more application areas." [10]

Decentralised data storage

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "centralised data storage" is defined as "data management paradigm where the storage and remote access of data is under the control and management of multiple independent parties/entities (also called"nodes")."

Note: the blockchain is an example of decentralised data storage. The opposite of decentralised data storage is centralised data storage.

Decryption

"Reversal of a corresponding encryption." [19]

Degaussing

"Render magnetically stored data unreadable by applying a strong magnetic field to the storage medium." [40]

Note: this method does not work for storage devices using SSD technology.

Derived data

"Data created as a result of processing that involves steps other than or in addition to direct retrieval and validation of information from data functions." [41]

Data "obtained and reconstructed from raw data (*e.g.*, final concentrations as calculated by a spreadsheet relying on raw data obtained from an instrument; result tables as summarised by a Laboratory Information Management System (LIMS), *etc.*). Derived data are obtained by data processing." [22]

For the purpose of the present guidelines, "derived data" is considered a synonym of "processed data".

Design qualification (DQ)

"Process for verification that the proposed specification for the facility, equipment or system of the assay meets the expectation for the user requirement specifications (URS)." [42]

"Documented verification that the proposed design of facilities, systems, and equipment is suitable for the intended purpose." [33]

Dictionary attack

"(On a password-based system) Attack on a crypto-system that employs a search of a given list of passwords." [43]

Digital (*e.g.*, data)

"Data in the form of a structured sequence of bits/bytes that represents information content." [39]

Formally speaking, "digital" refers to the way data are encoded (*i.e.*, binary information), whereas "electronic" refers to the physical medium on which data are stored (*i.e.*, medium relying on electrical or electromagnetic signals). However in many sources and context, the terms "digital" and "electronic" are used interchangeably since digital data are practically always electronic, and most electronic data are digital or converted to digital format shortly after acquisition.

Digital signature

"Data which, when appended to a digital document, enable the user of the document to authenticate its origin and integrity." [21]

Digital transformation

"Process of profound and radical change through digital technologies (including big data, blockchain, cloud computing, internet of things, artificial intelligence, analytics, cognitive solutions, *etc.*) that orients an organization in a new direction and takes it to an entirely different level of effectiveness, which is based on analytics of data."

Digital transformation is considered to be the "ultimate" phase of digitalisation.

Digitalisation

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "digitalisation" is defined as "the process of integrating the use of digital technologies with the support of computer systems in processes."

Note: computerisation is an example of digitalisation. The two terms are often used interchangeably in other documents, although the signification slightly differ.

Note: digitalisation should not be confounded with digitisation.

Digitisation

"Process of converting analogue materials into digital form." [44]

"Conversion of an analogue document (paper, microform, film, analogue audio or audiovisual tapes) to digital format for the purpose of preservation or processing." [21]

Note: digitisation should not be confounded with digitalisation.

Digitalised process

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

The following definitions of "computerised system" can be found in other reference documents:

"A computerised system collectively controls the performance of one or more automated processes and/or functions. It includes computer hardware, software, peripheral devices, networks and documentation, *e.g.* manuals and standard operating procedures, as well as the personnel interfacing with the hardware and software, *e.g.* users and information technology support personnel." [18].

"A broad range of systems including, but not limited to, automated laboratory equipment, laboratory information management, and document management systems. The computerised system consists of the hardware, software, and network components, together with the controlled functions and associated documentation." [33].

"A computerised system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating procedures performed by personnel." [45].

The first definition [18] is centred on the purpose of automation and is therefore in line with the definition of "computerisation" retained in the present guidelines. Although the second definition includes the concept of automation, this characteristic is not as central. The third definition does not mention automation at all.

All of the above definitions agree in describing a "computerised system" as a process (*i.e.*, an ordered set of actions/functions integrating a computer system, together with its supporting inputs (which include personnel, procedure and documentation).

Also considering the definitions of "digitalisation" as compared to "computerisation", the terms "digitalised process" are preferred to "computerised system" to both avoid confusion with the terms "computer system" (which are very similar in writing) and to emphasize that it refers to a process and not only to an object used in that process.

For the purpose of the present guidelines, the definition of "digitalised process" is "process integrating one or more computer system(s), together with its other components including personnel, procedure and documentation."

Distributed denial of service (DDoS) attack

"Unauthorized access to a system resource or the delaying of system operations and functions in the way of compromising multiple systems to flood the bandwidth or resources of the targeted system, with resultant loss of availability to authorized users." [46]

Document

"Information and the medium on which it is contained." [34]

Documented information

"In a management system standard (MSS) implementation, the records created to conduct and direct the management system and to document its implementation are called documented information." [47]

"Information required to be controlled and maintained by an organization and the medium on which it is contained. Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer to:

- the management system, including related processes;
- information created in order for the organization to operate (documentation);
- evidence of results achieved (records)." [8]

Note: a "documented procedure" refers to a procedure for which records are retained as evidence of the performed activities.

Document life cycle

"Period from the conceptual idea to the logical and physical deletion of a document." [48]

See also the definition of "life cycle".

Dynamic application security testing (DAST)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "dynamic application security testing (DAST)" is defined as "method of security testing that analyses a running application to identify vulnerabilities by simulating attacks from the perspective of an external attacker without prior knowledge of the source code".

Note: DAST belongs to black-box testing.

Driver

"Software component that permits a system to control and communicate with a peripheral device." [49]

Dual authorisation (or "two-person authentication")

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "dual authorisation" is defined as "system […] designed to prohibit individual access to certain resources by requiring the presence and actions of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed." [50]

Electronic

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "electronic storage" is defined as "a form of data storage where data is physically stored in the form of electrical or electromagnetic signal". Examples of electronic storage media include HDD and SSD.

Note: The term "electronic" refers to the physical medium on which data are stored whereas "digital" refers to the way data are encoded (*i.e.*, binary information). However in many sources and context, the terms "digital" and "electronic" are used interchangeably since most digital data are electronic, and most electronic data are digital or converted to digital format during their life cycle.

Note: Electronic data can be digital or analogue.

Note: Other forms of data storage include paper storage and optical storage.

Electronic archiving

"Storage of electronic information in an independent physical or logical space where the information is protected from loss, alteration and deterioration." [51]

"Collection of documents in a storage device for historical purposes or as a backup. Note 1 to entry: Example: A stored collection of various versions of a document." [10]

See also the definition of "archiving".

Electronic Document Management System (EDMS)

"Software program that manages the creation, storage and control of documents electronically." [52]

"Computer-based application dealing with the management of documents throughout the document life cycle." [48]

Note: EDMS often have features related to digital signatures, access control, archiving, version control and change control.

Electronic signature

For the purpose of the present guidelines, "electronic signature" is considered a synonym of "digital signature".

Encryption

"(Reversible) transformation of data by an encryption algorithm to produce ciphertext, *i.e.* to hide the information content of the data." [19]

Endpoint device

"Network connected information and communication technology (ICT) hardware device. Note 1 to entry: Endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and Internet of things (IoT) devices." [2]

For the purpose of the present guidelines, "endpoint device" means "any device connected to a laboratory's network for a purpose other than supporting the network itself.

Enterprise Resource Planning software (ERP)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "enterprise resource planning software" is defined as "application software designed to assist companies (the users) in managing, controlling and tracking its business operations such as inventory and purchase management, human resource management, accounting, orders management."

Exhaustive attack

For the purpose of the present guidelines, "exhaustive attack" is considered a synonym of "brute-force attack." [10].

External provider

"Provider that is not part of the organisation." [34]

Externally provided

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “externally provided” is defined as “pertaining to something (product or service) that is provided to the laboratory by an external provider.”

Note: this includes products and services provided by any personnel that is not part of the laboratory itself. Personnel from the IT department of the laboratory’s parent organisation is considered as an external provider.

Failure

“Termination of the ability of an item to perform a required function. Note 1 to entry: After failure, the item has a fault. Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.” [53]

Faulty

“State of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. […] Note 1 to entry: A fault is often the result of a failure of the item itself, but can exist without prior failure.” [53]

File

“An unambiguously named collection of structured information having a common set of attributes.” [54]

File format

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “file format” is defined as “the structure used to encode, organize, compress and store data in a digital file.”

File system

“Software structure which specifies how the data is digitally organized on a given storage medium.” [55]

Firewall

“Type of barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic as defined by the local security policy is allowed to pass.” [56]

Firmware

“Software that is included in read-only memory (ROM).” [57]

Functional testing

For the purpose of the present guidelines, “functional testing” is considered a synonym of “black-box testing.” [7]

Hard disk drive (HDD)

“Electromechanical device consisting of one or more magnetic disks (platters), read & write heads, a motor, and control electronics usually contained within an enclosure and used to store data. Note 1 to entry: Also commonly referred to as hard drives or disk drives.” [26]

Hardware

“Physical equipment used to process, store, or transmit computer programs or data.” [7]

“All or part of the physical components of an information processing system.” [10]

Hash function

“Function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output; — for a given input, it is computationally infeasible to find a second input which maps to the same output.” [58]

“Mathematical algorithm used for turning some kinds of data into a relatively small integer.” [21]

The output of a hash function is called a hash values.

Hash value (or “hash code”)

“Mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously changed.” [46]

Note: hash values are obtained by using a hash function. For the purpose of the present guidelines, hash values are considered a form of digital signature.

Hybrid license

At the time of writing and to the author’s knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, “hybrid license” is defined as “license that incorporates elements of both proprietary and open-source licensing.” The documentation (design, blueprints and/or source code) of creation under hybrid license may or may not be publicly available.

Identity management system (IMS)

“Mechanism comprising of policies, procedures, technology and other resources for maintaining identity information including associated metadata. Note 1 to entry: An identity management system is typically used for identification or authentication of entities.” [59]

Impartiality

“Presence of objectivity. Note 1 to entry: Objectivity means that conflicts of interest do not exist, or are resolved so as not to adversely influence subsequent activities of the laboratory.” [1]

In-house developed (or in-house built) (system or software)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "in-house developed" is defined as "pertaining to an item that is created by the end-user himself."

Indexing

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "indexing" is defined as "Process of classifying and possibly assigning an identifier to make items easier to retrieve."

Information management system

"Facilities, processes and procedures used to collect, store and distribute information between producers and consumers of information in physical or electronic format." [7]

An information management system integrating a computer system is an example of digitalised process.

Information processing system

"One or more data processing systems and devices, such as office and communication equipment, that perform information processing." [10]

"System that processes, provides and distributes information together with associated organisational resources." [47]

Information security

"Preservation of confidentiality, integrity and availability of information. Note 1 to entry: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved." [8]

Information security event

"Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant." [2]

Installation qualification (IQ)

"Process of establishing by objective evidence that all key aspects of the process equipment and ancillary system for the assay instrument installation comply with the approved user requirement specifications (URS)." [42]

"Documented verification that a system is installed according to written and pre-approved specifications." [33]

“Installation Qualification (or system installation testing) builds upon the system design specifications. It shows that the system has been properly installed in the user’s environment and that all components are operative.” [60]

Integrated development environment

“Set of software tools or applications to provide comprehensive facilities for software development” [7]

Integrity

“Property of accuracy and completeness.” [8]

“Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data.” [13]

“Property that data has not been altered or destroyed in an unauthorized manner.” [40]

“Attribute of a document whose content is complete and unaltered.” [21]

Note: principles for data integrity are summarised below:

- All data and documents are always associated with complete metadata, including:
- The nature, origin and form of the data (units, formatting, identification of the samples measured…) or document (*What*);
- The unequivocal identification of people that have performed actions related to the data or document (*Who*);
- The date/time on which each action on the data or document was performed (*When*);
- Data and associated metadata are recorded as soon as possible after completion of the activity that generated them (*i.e.*, contemporaneously);
- Actions related to data and documents are carried out in a way that all data and metadata remain available, readable and unaltered. It follows that:
- Erroneous and/or incomplete data and/or metadata should be retained unaltered. When data or documents must be amended, a new version that refer to the original one shall be generated and reference to this new version shall be added to the original;
- When processed data are generated, the input data must be retained unaltered and available so that the derived data can be completely reconstructed from the underlying data and instructions;
- Data and files should be digitally protected against unduly alteration (*e.g.*, human mistakes, file corruption, falsification…);
- Computer systems used to perform actions related to data and electronic documents should be physically protected (*e.g.*, against humidity, fire, electrical surge, vandalism…) and digitally protected (*e.g.*, against human mistakes, file corruption, falsification and cyberattacks…);
- When data are amended versions of other data or derived from other data, they should be linked unequivocally to the input or original data, respectively;

- Actions related to data and documents should be planned and executed consistently, especially data processing, in order to be reproducible;
- All data shall be authentic (not made up);
- All data and documents should be indexed in a way that they can be easily and promptly retrieved when necessary.

Internet Of Things (IOT)

"Infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world." [61]

Interoperability

"Ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged" [7]

Backward compatibility and portability are two aspects of interoperability.

Insider attack

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "insider attack" is defined as "a type of cyber threat in which an attacker uses its access rights or knowledge of an organisation's resources."

Note: an insider attack can come from laboratory personnel, external providers or customers.

Intranet

"Private computer network that uses Internet protocols and network connectivity to securely share part of an organisation's information or operations with its employees." [56]

Intrusion detection system (IDS)

"Technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks." [46]

Intrusion prevention system (IPS)

"Variant on intrusion detection systems that are specifically designed to provide an active response capability." [46]

Laboratory

"Body that performs one or more of the following activities: testing; calibration; sampling, associated with subsequent testing or calibration. Note 1 to entry: In the context of this document,"laboratory activities" refer to the three above-mentioned activities." [1]

Laboratory Information Management System (LIMS)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "Laboratory Information Management System (LIMS)" is defined as "software application designed to help laboratories manage their operations."

Note: LIMS may cover aspects that are commonly covered by DMS and ERP as well as features that are specific to laboratories, such as sample tracking, test report generation, equipment management, control charts…

License

"Legal agreement between two parties, the licensor and the licensee, as to the terms and conditions for the use or transfer of an intellectual property right from the licensor to the licensee." [7]

Note : software are protected by intellectual property rights (which include namely the rights to use, distribute and modify). By default, these rights are owned by the author(s) of the software (designer(s) and developer(s)) or their employing organisation when the software was developed during employment.

Note: In the case of OTS software, the laboratory usually only acquires the right to use them through a license. This can be done for free (*i.e.*, in the case of open-source software or certain hybrid licenses) or in exchange for a single or recurrent fee (*i.e.*, proprietary).

Note: a laboratory only "owns" a software (in the sense that it owns all related intellectual rights) in two cases:

- When all rights are transferred through a specific contract (usually against payment). This may be the case for custom-made software;
- When the software is developed in-house. Examples of software that are commonly developed in-house are spreadsheets, scripts/macros and databases (even if they have been developed or are used through another software).

Relevant European regulation related to intellectual property of software includes:

- Directive 2009/24/EC on the protection of computer programs [62];
- Directive 96/9/EC on the protection of databases [63];
- Directive (EU) 2019/770 on contracts for the supply of digital content and digital services [64].

Note: OTS software often requires a "license activation" step that is necessary to use it.

Life cycle

"Evolution of a system, product, service, project or other human-made entity from conception through retirement." [27]

Note: he possible stages of an item's life cycle change according to the item's nature (*e.g.*, computer system, software, data, document…) and the viewpoint (the life cycle of a software is rather different from the viewpoints of its developers and users). An item's life cycle can be modelled in many valid ways depending on the context.

Note: the reader may also refer to ISO 12207 [28] and ISO/IEC/IEEE 15288 [27] on software life cycle processes.

Local Area Network (LAN)

"Computer network located on a user's premises within a limited geographical area." [10]

Logbook

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "Logbook" is defined as "a collection of records, most often sorted by date, about an entity and generated for traceability purpose".

Maintenance

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "maintenance" is defined as "set of actions performed with the aim to preserve or restore the integrity and functions of equipment."

Maintenance may include operational testing, verification of wear, tear and tightness; cleaning, tightening or replacing parts. Maintenance can be preventive or corrective.

Malware

"Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity, or availability. Note 1 to entry: Viruses and Trojan horses are examples of malware." [56]

Man-in-the-middle attack

"Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge" [65]

Metadata

"Data about other data, documents, or records that describes their content, context, structure, data format, provenance, and/or rights attached to them." [39]

"Data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths, access rights and data volatility." [10]

"Data describing the content (including indexing terms for retrieval), context and structure of electronic document-based information and their management over time." [51]

"Data describing the context, content and structure of a document and their management over time." [21]

"Metadata give data meaning, provide context, define structure, and enable retrievability across systems, and usability, authenticity, and auditability across time. For electronic data, parts of the metadata can be generated in audit trails. Metadata form an integral part of the data. Without the

context provided by metadata, the data have no or limited meaning. The degree of metadata missing reduces the ability to interpret the data." [22]

"Metadata are data about data that provide the contextual information required to understand those data. These include structural and descriptive metadata. Such data describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. Metadata necessary to evaluate the meaning of data should be securely linked to the data and subject to adequate review. For example, in weighing, the number 8 is meaningless without metadata, *i.e.* the unit, mg. Other examples of metadata include the time/date stamp of an activity, the operator identification (ID) of the person who performed an activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities." [18]

Note: as a rule of thumb, metadata is generally regarded as complete when they include the "five Ws": "Who did What, Where, When and Why". To these, the "How" is often added to describe the materials and methods employed.

Note: for example, a unit is a metadata associated with a value.

Migration (of digital data)

"Process to copy data from one storage device or medium to another." [66]

Modified Off-The-Shelf (MOTS)

"Software product that is already developed and available, usable either "as is" or with modification, and provided by the supplier, acquirer, or a third party." [67]

Note: in the present document, MOTS may refer to either or both software and hardware.

Modularity

"Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components." [7]

Note: examples of modules of an analytical system include autosampler, injection system, separation system, detector and desktop computer for instrument control. Peripheral devices are examples of modules of a desktop computer.

See also replaceability.

Multi-factor authentication

"Authentication using two or more of the following factors:

- knowledge factor, "something an individual knows";
- possession factor, "something an individual has";
- biometric factor, "something an individual is or is able to do"." [68]

Note: examples of multi-factor authentication mechanisms include:

- Biometric authentication;

- One-time passwords;
- Dual authorisation;
- Authentication based on IP, MAC/physical address and/or geographical location;
- Physical key.

Network

"Infrastructure that connects a set of endpoints, enabling communication of data between the digital entities reachable through them." [61]

Network Attached Storage (NAS)

"Storage device or system that connects to a network and provide file access services to computer systems." [40]

Nonconforming work

This term is indirectly defined in clause 7.10.1 of ISO/IEC 17025 [1] as pertaining to an "any aspect of its laboratory activities or results of this work [which does] not conform to its own procedures or the agreed requirements of the customer."

Non-repudiability

"Degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later." [13]

"Ability to prove the occurrence of a claimed event or action and its originating entities." [8]

Off-premises (or off-site)

Opposite of "on-premises".

Off-The-Shelf (OTS) (or "ready-to-use") system

"Product or system already developed and available." [67]

Note: in the present document, OTS may refer to either or both hardware and software and is defined as a system or component that:

- has been developed to meet common requirements of a community of potential users (*i.e.*, it has not been tailored to fit the needs of specific identified user(s));
- has been developed by an entity independent from the user;
- has been developed without influence or participation from a specific user;
- can be used right after the acquisition without needs of further development or customisation other than those intended by the designer;
- may be customised (thereby becoming MOTS) or not;

- may be delivered and used for free or commercial, *i.e.*, in exchange of any form of payment (including single-purchase or subscription model) (COTS);
- may be open-source or not;
- is provided to the user by an external provider.

On-premise(s) (or on-site)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "on-premise(s)" is defined as "software deployment method in which all the resources required for normal use are present within the user's facility. On-premises resources can be normally accessed and used without reliance on internet nor external provider services."

One-Time Password (OTP)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "one time password" is defined as "Single-use password or code sent to a legitimate user through confidential channels to prove its identity during authentication."

One-time passwords are an example of multi-factor authentication mechanism.

Open file format

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "open file format" is defined as "file format whose encoding and decoding protocols are publicly available and freely usable".

Open-source

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, the definitions from the Open Source Initiative[1] and the Open Source Hardware Association[2] are applicable for software and hardware, respectively.

Note: for the sake of conciseness, "open" (for data) and "open-source" (for software, hardware and computer system) are defined as "pertaining to something fulfilling the following conditions:

- The documentation (design, blueprints and/or source code) are publicly available;

[1] https://opensource.org/osd/
[2] https://www.oshwa.org/definition/

- The license transfers all intellectual property rights (including modification, reproduction, redistribution and use) to the licensee without restriction, except for attribution of the licensor;
- The license must not restrict or discriminate any person, group(s), field(s) of endeavour, product or technology;
- The license must automatically apply to all to whom the work is redistributed without the need for execution of an additional license by those parties."

Note: for the purpose of the present guidelines, the terms "open-source" and "proprietary" are considered mutually exclusive.

Operating system (OS)

"Software to control program operation and to provide the services for resource allocation, task scheduling, I/O control, and data management." [25]

Note: an operating system is an example of platform software.

Operational qualification (OQ)

"Process of obtaining and documenting evidence that installed equipment operates within predetermined limits when used in accordance with its operational procedures." [42]

"Documented verification that a system operates according to written and pre-approved specifications throughout specified operating ranges at the customer." [33]

"Operational qualification has the aim of demonstrating that all functions needed for the intended purpose are available and operate reliably in the user's environment." [60]

Note: oOperational qualification may cover all features and operation of a system regardless of its purpose. The result of a given operational test is typically binary (yes/no, valid/invalid, working/not working).

Optical storage (or memory)

"Storage device that uses optical techniques." [10]

Note: compact disks (CD) are an example of optical storage medium.

Performance qualification (PQ)

"Process of establishing by objective evidence that the assay process, under anticipated conditions, consistently produces a result which meets all predetermined [user requirement](#UR] specifications (URS)." [42]

"Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written and pre-approved specifications, within the scope of the business process and operating environment." [33]

Note: performance qualification only applies when performance can be measured quantitatively. Examples include:

- in chromatography: retention times, peak symmetry, number of plates, peak resolution…;

- in spectrophotometry: wavelength and absorbance accuracy, stray light…;
- in atomic spectroscopy: characteristic concentration/mass…;
- in mass spectrometry: mass accuracy, mass resolution…

Peripheral device

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "peripheral device" is defined as "any module connected to a computer and used for input or output of data into or from the computer."

Note: examples of peripheral devices used for input include mouse, keyboard and other sensor devices in general. Examples of output devices include screens, speakers, printers and other actuator devices in general. External storage devices are peripheral devices that can be used for both input and output.

Permission

For the purpose of the present guidelines, "permission" is considered a synonym of "access right".

Phishing

"Fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication." [69]

"Scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly." [65]

Platform software

"Application-independent software that supports the running of application software, *e.g.* an operating system, a Web browser, or a programming environment." [10]

Note: operating systems, web browsers and programming environment are examples of platform software.

Portability

"Degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another." [13]

"Capability of a program to be executed on various types of data processing systems without converting the program to a different language and with little or no modification." [10]

"Ability to easily transfer data from one system to another without being required to re-enter data." [20]

Note: portability is one aspect of interoperability.

Precision

"Closeness of agreement between indications or measured quantity values obtained by replicate measurements on the same or similar objects under specified conditions." [11]

"Closeness of agreement between independent test results obtained under stipulated conditions." [12]

Preventive action

"Action to eliminate the cause of a potential nonconformity or other potential undesirable situation […] Preventive action is taken to prevent occurrence whereas corrective action is taken to prevent recurrence." [34]

Private key

"Key of an entity's key pair which is known only by that entity." [19]

Privilege

For the purpose of the present guidelines, "privilege" is considered a synonym of "Access right."

Privileged access rights

Access rights that "allows the performance of activities that typical users of processes cannot perform. System administrator roles typically require privileged access rights." [3]

Procedure

"Specified way to carry out an activity or a process." [34]

A procedure should be sufficiently detailed to ensure consistent application and should specify:

- When the process shall be initiated, including triggering events and/or minimal frequency;
- The authorisation and responsibilities of involved personnel for each step of the process;
- The data/documents to be used as inputs;
- The expected outputs.

Processed data

For the purpose of the present guidelines, "processed data" is considered a synonym of "derived data".

Procurement

"Process of obtaining seller responses, selecting a seller, and awarding a contract." [70], as cited by [7]

Proprietary (software, data, file format…)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "proprietary" is defined as "pertaining to something (which may include data, software, hardware or computer system) whose documentation (including design, blueprints and/or source code) and intellectual property rights (including modification, reproduction, redistribution and use) are owned and under the control of an individual, organisation, or entity."

For the purpose of the present guidelines, open-source and proprietary are considered mutually exclusive.

Public key

"Data item of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity." [71]

"Key of an entity's key pair which is publicly known." [19]

Qualification

For the purpose of the present guidelines, "qualification" is considered as a synonym of "acceptance testing".

Qualified electronic signature

"Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures." [14]

Note: The eIDAS regulation [14] can be consulted for further details.

Note: the list of qualified trust services providers can be found on the European Commission website[3].

Ransomware

"Malicious software that infects computer systems, restricts access to the victim's data and requires a ransom." [72]

Raw data

"Data in its originally acquired, direct form from its source before subsequent processing." [39]

Note: what is considered a "raw data" depends on the viewpoint and context. For example, from the viewpoint of the user of a spectrophotometer, absorbance reading may be regarded as the raw data. However, from the viewpoint of, *e.g.*, the manufacturer, the absorbance is derived from analogue data such as voltage or current.

Note: From a philosophical and absolute, viewpoint all electronic digital data are derived from analogue data.

Release note

For the purpose of the present guidelines, "release note" is considered a synonym of "version description document".

[3] https://eidas.ec.europa.eu/efda/home

Record

A considerable number of ISO standards have their own definition for this term, many of which are sector-specific. The definitions that are relevant for the purpose of the present guidelines can be split in two categories:

- Definitions in which "record" is described as a type of document, *e.g.*:
  - "Document stating results achieved or providing evidence of activities performed." [34]
  - "Document(s) containing recorded information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business." [47]
- Definitions in which "record" is described as a set of data, *e.g.*:
  - "Set of related data items treated as a unit." [73]
  - "Part of a document or document containing a structured and internally organized set of self-contained but related data on one person or other object, selected and presented for a predefined specific purpose." [39]

Note: an example of records for which the second category of definitions is suitable are database records.

Note: elements that can be subject to a record include:

- User identity;
- Date/time;
- Activities performed, including:
  - System used/accessed;
  - Software used;
  - Data/files/documents interacted with;
  - Action attempted (consultation, creation, edition, deletion) and their result (success, reject…).

Record system

"Information system that manages records over time." [47]

Record systems can have many forms, such as spreadsheet(s) and databases.

Relational database

"Database in which the data are organized according to a relational model" [10]

Note: relational databases are the most popular type of database.

Relational Model

"Data model whose structure is based on a set of relations." [10]

Replaceability

"Capability of a product to replace another specified product for the same purpose in the same environment." [13]

Note: for example, hardware that meets international technical standards (*e.g.*, pipe/threads dimensions, power requirements…) is more replaceable than non-standard one.

Resource

"Physical, network, or any information asset that can be accessed for use by a subject." [9]

Note: examples of resources include peripheral devices, internet access, computing power, software, data and documents.

Risk

"Effect of uncertainty on objectives. Note 1 to entry: An effect is a deviation from the expected — positive or negative. Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Note 3 to entry: Risk is often characterized by reference to potential "events" […] and "consequences" […], or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" […] of occurrence." [8]

Risk assessment

"Overall process of risk identification, risk analysis and risk evaluation." [8]

Risk identification

"Process of finding, recognizing and describing risks." [8]

Risk analysis

"Process to comprehend the nature of risk and to determine the level of risk." [8]

Risk evaluation

"Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable." [8]

Server

"Computer system that provides data and software to one or more computers on a network." [26]

Note: depending on the context, "server" may refer to a whole computer system (hardware and software) or to the software alone.

Service report

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "service report" is defined as "record issued to the laboratory by an external provider following the provision of a service (such as system delivery, installation or maintenance) an describing the activities performed and their results."

Software

"All or part of the programs, procedures, rules, and associated documentation of an information processing system." [10]

Solid State Drive (SSD)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "solid state drive" is defined as "electronic digital data storage device relying on metal–oxide–semiconductor field-effect transistor technology".

Source code

"Computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator." [7]

Specification

"Document stating requirements." [34]

Spoofing

"Impersonating a legitimate resource or user." [56]

Note: examples of spoofing attacks include IP spoofing (where the attacker pretends to be someone else by sending IP packets with a false source IP address) and DNS spoofing.

Spreadsheet

"Program that displays a table of cells arranged in rows and columns, in which the change of the contents of one cell can cause recomputation of one or more cells based on user-defined relations among the cells." [1]

3.0.1 Standalone (computer system or software)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "standalone" is defined as "pertaining to a computer system which operates without reliance or communication on/with other computer systems."

3.0.2 Standard Operating Procedure (SOP)

"Authorized, documented specified way to carry out an activity or process." [34]

Static application security testing (SAST)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "static application security testing (SAST)" is defined as "method of security testing that analyses an application's source code for vulnerabilities without executing the program."

Note: SAST belongs to white-box testing. Further reference can be found on the OWASP website[4].

3.0.3 Static format (of a record)

"A static record format, such as a paper or pdf record, is one that is fixed and allows little or no interaction between the user and the record content. For example, once printed or converted to static PDFs, chromatography records lose the capability of being reprocessed or enabling more detailed viewing of baselines." [18]

Structure-based testing

For the purpose of the present guidelines, "structure-based testing" is considered a synonym of "white-box testing." [7].

Subject

"Entity requesting access to a resource controlled by an access control system." [9]

System suitability tests (SST)

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "system suitability test" is defined as "acceptance testing activities that are conducted on a regular basis after introduction of a computer system to verify that it is still fulfilling user requirements".

Trojan horse

"Apparently harmless program containing malicious logic that allows the unauthorized collection, falsification, or destruction of data." [10]

Trueness

"Closeness of agreement between the average of an infinite number of replicate measured quantity values and a reference quantity value." [11]

---

[4] https://owasp.org/www-community/Source_Code_Analysis_Tools Consulted 03/07/2024

"Closeness of agreement between the average value obtained from a large series of test results and an accepted reference value." [12]

Tunnel

"Data path between networked devices which is established across an existing network infrastructure. Note 1 to entry: Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits." [56]

Tunnelling

"A means of transporting protocol information between two entities that are interconnected by a network, without the need for that interconnecting network to comprehend the transported protocol information." [74]

User error protection

"Degree to which a system protects users against making errors." [13]

User error protection mechanisms may prevent users from, *e.g.*:

- Enter data of the wrong type (*e.g.*, characters where a pure number is expected);
- Enter a date before the present day (*i.e.*, backdating);
- Enter setting value that cannot be achieved by the hardware or could damage it;
- Save incomplete data.

User endpoint device

"Endpoint device used by users to access information processing services. Note 1 to entry: User endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, *etc.*"

User Requirements (UR)

"The complete description of the set of user needs for the software to be provided. User Requirements include Functional User Requirements, Technical Requirements and Quality Requirements." [75]

Note: for the purpose of the present guidelines, the definition is extended to computer system, software and related services. Also, "Technical Requirements" and "Quality Requirements" are grouped as "Non-functional requirements".

Note: the term "User Requirement Specification" (URS) used by other guidelines [33,60,76] is considered as a synonym.

Utility program

"Program that provides general, frequently needed services for computer users and service personnel. Note 1 to entry: Examples: A diagnostic program, a trace program, a sort program." [10]

For the purpose of the present guidelines, "utility program" is defined as "software designed to help manage, maintain, and control computer resources".

Note: other examples of utility programs include:

- File management software (*e.g.*, for compression, backup, transfer/synchronisation…);
- System management software (*e.g.*, disk clean-up, defragmentation, diagnostic tools…);
- Security software (*e.g.*, firewall, antivirus, intrusion detection system and/or intrusion prevention system);
- Software controlling which other software execute at system start-up.

Validation

"Confirmation, through the provision of objective evidence, that the particular requirements for a specific intended use or application have been fulfilled." [34]

"Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled." [35]

"Test to determine whether an implemented system fulfils its specified requirements." [10]

Validation plan

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

"The validation plan should be an approved document, which describes the validation activities and responsibilities during IQ, OQ and PQ. The validation plan should […] be prepared and approved prior to conducting the tests." [60]

"The validation plan describes all activities such as review of the URS, review of the development plan (design), test strategy, verification of the data migration (if applicable), review of the validation documents and the acceptance testing of the whole system." [33]

Verification

"Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled." [35]

"Provision of objective evidence that a given item fulfils specified requirements. Note 1 to entry: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents. Note 2 to entry: The activities carried out for verification are sometimes called a qualification process." [34]

For the purpose of the present guidelines, "verification" is considered a synonym of "qualification".

Version conflict

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "version conflict" is defined as "situation where modifications made to the same file or set of files stored on the same storage device by multiple users

(human or not) are incompatible, making it unclear how to merge them". Version conflict commonly arise in the following situations:

- When different users edit the same file remotely and simultaneously on a centralised data storage (*e.g.*, file server or NAS);
- When different users edit their own copies of the same file without synchronisation of each other's edits.

Version control

"Establishment and maintenance of baselines and the identification and control of changes to baselines that make it possible to return to the previous baseline" [7]

For the purpose of the present guidelines, "version control" is considered a synonym of "change control".

Version control system

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "version control system" is defined as "software designed for version control purposes".

Note: a version control system usually records changes to files over time and merge them in the same files, allowing multiple parties (users and/or software) to access and edit the same file simultaneously. It can also be used to solve version conflicts. Alternatively, a version control system can "lock" a file being edited by another user (allowing consultation but not edition for other user at the same time) to prevent version conflicts.

Version description document

"Document that accompanies and identifies a given version of a system or component. Note 1 to entry: Typical contents include an inventory of system or component parts, identification of changes incorporated into this version, and installation and operating information unique to the version described." [7]

For the purpose of the present guidelines, "version description document" is considered a synonym of "release note".

Virtual private network

"Restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunnelling links of the virtual network across the real network" [77]

Virus

"Program that propagates itself by modifying other programs to include a possibly changed copy of itself and that is executed when the infected program is invoked. Note 1 to entry: A virus often causes

damage or annoyance and may be triggered by some event such as the occurrence of a predetermined date." [10]

Sometimes, the term "virus" is used with the same meaning as "malware", *e.g.*:

"Type of malware which is software designed with malicious intent containing features or capabilities that can potentially cause harm, directly or indirectly, to the user and/or the user's system" [46]

Vulnerability

"Weakness in an information system, system security procedures, internal controls, or implementation that can be exploited or triggered by a threat" [78]

Web browser

"Client program that initiates requests to a World Wide Web server and displays the information that the server returns." [79]

Web filtering

At the time of writing and to the author's knowledge, no ISO standard provides an appropriate definition for the purpose of the present guidelines.

For the purpose of the present guidelines, "web filtering" is defined as "technology allowing to the content accessible over the internet from their networks".

White-box testing

"Testing that takes into account the internal mechanism of a system or component [including] branch testing, path testing [and] statement testing" [7]

4. Risk assessment

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 8.5**: the laboratory shall:
    1) Identify risks associated with its activities;
    2) Plan proportionate actions to mitigate those risks;
    3) Implement (and document) those actions;
    4) Evaluate the efficiency of those actions;
- **Clause 8.5.2**: the ISO/IEC 17025:2017 [1] has "no requirement for formal methods for risk management or a documented risk management process" and states that it is up to the laboratory to decide "whether or not to develop a more extensive risk management methodology *e.g.* through the application of other guidance or standards";
- **Clause 8.7.1 e)**: risks shall be re-evaluated/updated when a non-conformity occurs.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- The risk assessment process for digitalised processes be subject to written and documented procedure(s);
- A systematic methodology for risk assessment be applied. It is up to the laboratory to decides to apply an existing methodology from an appropriate reference document or to define its own;
- Risk assessment cover risks related to both the accuracy of test results and information security. Section 5 lists common risks which should be considered;
- Risk assessment be conducted for all computer systems, including:
    - Measuring instruments, from electronic scales and electronic thermometers to spectrometers, chromatographic systems, *etc.*;
    - Systems used for sample preparation, *e.g.*, freeze-dryers, microwaves, centrifuges, grinders, ovens, laminar flow hoods, *etc.*;
    - Systems used for monitoring and control of environmental conditions, *e.g.*, air conditioning, data loggers, *etc.*;
    - User endpoint devices, *e.g.*, desktops, laptops, tablets, smartphones, *etc.*;
    - Systems supporting the network and information technology facilities, *e.g.*, servers, NAS, switches, modems, *etc.*;
    - Systems supporting other facilities, *e.g.*, gas generators, *etc.*;
- Risk assessment consider all stages of the life cycle of the considered systems, modules and/or software;

- Risk assessment uses previous experience with similar systems, software and/or services (including failures and non-conforming work) as inputs;
- Risk assessment be conducted, if appropriate, in the following circumstances:
  - Before defining user requirements and therefore, before entering into contract with external provider, starting the in-house development or acquisition of a new computer system, module, software or related service;
  - After installation and before using those items in a digitalised process;
  - After identifying technical failure for those items;
  - After identifying non-conforming work related to those items;
  - After any significant change of the digitalised process, including:
    - Modification of the computer system such as;
      - Software updates (in this case, the release note may serve as input of the risk assessment);
      - Replacement of essential parts (in this case, the service report should serve as input of the risk assessment);
    - Modification of other aspects of the process such as:
      - Personnel rights and responsibilities;
      - Facilities and environment;
      - Procedure for use, handling, calibration, maintenance, *etc.*;

Note: when multiple of the above triggering events occur in a short period of time (*e.g.*, when system suitability tests of a measuring system results are out of acceptance criteria and further investigation brings to light a technical fault, which in turn leads to the replacement of a part), it makes sense (and also reduces workload) to consider all those events as a single triggering event and that the ensuing risk assessment uses information from all those events altogether as input.

Further guidance can be found in the following references:

- ISO 31000 on guidelines for risk management [80];
- IEC 31010 on risk assessment techniques [81];
- ISO/IEC 27000 on information security management systems [8];
- ISO/IEC 27001 on overview and concepts related to cybersecurity [2];
- ISO/IEC TS 27100 on overview and general concepts of cybersecurity [36];
- AGIT guidelines on validation of computerised systems (Appendix 1) [60];
- USP general chapter 1058 on analytical instrument qualification [76];
- GAMP 5 on risk-based approach to Compliant GxP computerised systems [82];
- ENISA guidelines on cloud computing [83];

- ENISA web tools[5].

4.1 Risk-based classification

This section discusses a risk assessment methodology here-called "risk-based classification". This methodology has been recommended in other guidance documents [33,60,76,82] and can be summarised as follows:

1) Define classes of systems with similar levels of risk and specify classification criteria;
2) For each class, define and plan controls that are expected to sufficiently mitigate the identified risks;
3) Attribute a class to each computer system taking into account the digitalised process in which it is used;
4) Systematically and consistently apply the planned controls accordingly with the attributed class.

The criteria and appropriate number of classes depends on many factors such as the field of activity, type of activity (*e.g.*, testing or calibration), computer systems, size of the organization and resources than can be allocated for management. Sometimes, classification can be ambiguous, *e.g.*:

- A given computer system can be used in different digitalised process and/or for different purposes and, thereby, may belong to different risk classes depending on which activity is considered. In such cases, it may be appropriate to assign the risk class with the strictest level of controls;
- A given computer system may include modules belonging to different risk classes (*e.g.*, a keyboard is, in principle, a low-risk module part to a desktop computer). In such cases, the modules can be managed separately if they are proven to be sufficiently independent from each other.

For the purpose of the present document, it is recommended that:

- The risk-based classification remain as simple as possible and contain just the necessary number of risk classes;
- When a computer system does not fit in any existing risk class, the laboratory should consider one of the following options:
  - Update the classification criteria so it can fit an existing risk class with existing set of controls;
  - Create a corresponding new risk class with a different set of controls. This option should be preferred when it is anticipated that other computer systems in the future will fall in the same risk class;
  - Consider the computer system as an exception with its own set of controls. This option should be preferred when it is not expected that other computer systems will fall in

[5] https://www.enisa.europa.eu/tools

the same risk class and/or when the number of existing risk class is already considered as sufficient.

- The risk-based classification include reviewing and documented approval by competent and authorised personnel (*i.e.*, classification should not mean that controls are implemented mindlessly).

5. Identified risks

The present section identifies relevant risks that may result in compromised accuracy of test results and/or information security, briefly discusses factors influencing them and recommends controls that can be implemented to mitigate them.

5.1 Selection of a system, module or related service unfit for purpose

Although identifying the need for a new system may seem simple, it may be difficult to foresee its future uses in details and the technical characteristics and features that will be needed or desired to achieve them.

Factors

- Degree of understanding of the system and related processes as well as the competence of personnel related to it;
- Number of analogous products/services (and external providers) available on the market;
- Time available to select an external provider and/or product or service.

Recommended controls

- Careful and timely definition of user requirements (see section 6.3);
- Appropriate personnel training (see section 6.18);
- Maintaining up-to-date written and documented procedures for the definition of user requirements and the procurement of products and services (see section 6.3).

5.2 Improper use and handling

Computer systems can be complex and misused in many ways. Improper usage can lead to compromised accuracy of test results, compromised information security, or harm to the system itself or personnel. Some common examples of improper usage include:

- Usage with improper settings or materials/reagents;
- Unintentional data edition, migration, deletion, *etc.*;
- Use without verification of the state of calibration, maintenance or fault.

Factors

- Complexity of the system (number of parameters to set, their relationship and how they affect the results of the activity) and its user interface;
- The number of personnel members having the rights to use the system and/or that have edition/deletion rights; and their competence;

- Integration of user error protection mechanisms during development;
- Training and experience of personnel responsible for system use and handling;

Recommended controls

- Maintaining up-to-date written and documented procedures for use and handling (see section 6.1);
- Planning and implementing appropriate system suitability tests (see section 6.5);
- Planning and implementing appropriate calibration;
- Planning and implementing appropriate maintenance (see section 6.6);
- Planning and implementing appropriate backups (see section 6.15);
- Planning and implementing appropriate personnel training (see section 6.18);
- Planning and implementing appropriate development practices (see section 6.4);
- Implementing appropriate access control (see section 6.13);
- Implementing the use and verification of digital signatures and/or hash values (see section 6.16).

5.3 Cyberattacks and insider attacks

Malicious actions committed through cyber means are a permanent threat to businesses [84].

Factors

- The number of people having physical access to system, the rights to use it and/or that have edition/deletion rights;
- The strength of authentication methods;
- The use of cybersecurity software (*e.g.*, web filters, firewall, antivirus, intrusion detection system and/or intrusion prevention system);
- Whether softwares are designed and developed properly and appropriately tested for errors and vulnerabilities;
- Whether software version is up-to-date or not;
- Whether software is still supported by its external provider or not;
- Connection to internet (either directly or indirectly *e.g.*, through LAN or other IOT devices) and/or reliance on cloud computing;
- Personnel awareness against cyberattacks.

Recommended controls

- Planning and implementing sufficient access control (see section 6.13);

- Planning and implementing sufficient acceptance testing for prevention of cyberattacks;
- Planning and implementing appropriate backups (see section 6.15);
- Maintaining software version up to date (see section 6.11);
- Including appropriate provision for cybersecurity in the user requirements, *e.g.*, provision for proficiency of external provider regarding cybersecurity (see section 6.3);
- Planning and implementing appropriate cybersecurity awareness training for personnel (see section 6.18).

5.4 Physical failure due to natural wear and tear

Physical wear and tear of hardware are unavoidable. Still, some computer systems are more susceptible than others and good practices can be implemented to prevent it and/or detect it before it causes harm.

Factors

- Presence of moving parts (which generally wear faster);
- Use of fluids and presence of seals/gaskets (which can leak);
- Exposition to harsh environmental conditions and chemicals.

Recommended controls

- Selecting systems designed for the intended environment (see section 6.3);
- Planning and implementing appropriate system suitability tests (see section 6.5);
- Planning and implementing appropriate preventive maintenance (see section 6.6);
- Planning and implementing appropriate monitoring and control of- and protection against environmental conditions (see section 6.8).

5.5 Service discontinuation

There are multiple reasons for service discontinuation, *e.g.*:

- Bankruptcy of the external provider;
- As new computer systems, modules and software (or new versions thereof) are released, service for older products are progressively discontinued. This constitutes a risk that a computer system can no longer be installed or used.

This risk includes the following services:

- The provision of cloud services such as cloud computing and storage;

- The activation of software license relying on cloud authentication (even if the software itself does not rely on remote resources);
- Maintenance service and provision of spare parts and software updates;

Factors

The factors affecting this risk are inherent to the external provider and cannot be controlled (or usually not even known) by the laboratory.

Recommended controls

- Including requirements for the duration of services availability in the user requirements (see section 6.3);
- For cloud services, planning and implementing regular on-premises backups when possible (see section 6.15);
- Selecting software not requiring remote activation relying on the cloud (see section 6.3).

5.6 Disaster

Disasters include fire, flooding, storms, roof leaks and, to a lesser extent, power outage. Even though modern computer systems are increasingly robust against power outage, such events can still cause various issues, including:

- Hardware damage or downtime;
- Compromised data integrity (*e.g.*, data in case of unexpected shutdown when saving);
- Compromised connexion/communication between computer systems or modules;
- Loss of samples or other materials (*e.g.*, when they must be kept at a certain temperature or analysed within a short time frame).

Factors

- Whether the laboratory uses hazardous materials (*e.g.*, flammable, oxidising, explosive, pressurised, *etc.*) and the quantities that are stored on-site;
- Presence of neighbouring external hazard sources (*e.g.*, laboratory located near a river, next to building storing or using hazardous materials, *etc.*);
- Design and condition of the facilities;

Recommended controls

- Implementing and maintaining appropriate disaster detection and control systems (see section 6.8);
- Implementing appropriate verification and maintenance of facilities;

- Planning, implementing and maintaining appropriate backups with off-site copies (see section 6.15);
- Planning and implementing appropriate event reporting procedures (see section 6.19);
- Implementing emergency power supplies against main power outage (see section 6.9);

5.7 Skill obsolescence or loss

Useful skills may be lost or become obsolete for multiple reasons, *e.g.*:

- Personnel resigning without proper knowledge transfer;
- Evolving technologies and techniques;
- Naturally, when a skill is not exercised.

Factors

Factors affecting skill obsolescence

Recommended controls

- Planning and implementing appropriate personnel training (see section 6.18);
- Maintaining up-to-date written instructions (see section 6.1);

5.8 Unexpected behaviour due to development errors or unsuitable design

There are many reasons that may lead a laboratory to opt for the in-house development of a computer system or software, which can range from a simple spreadsheet or script (*e.g.*, macros) designed to run locally and automate a specific task such as data processing, to complex, possibly cloud-based databases, EDMS, LIMS and ERP designed to digitalise complete laboratory processes.

Factors

- Whether the considered software is developed in-house or not;
- Training and experience of personnel responsible for development;
- Time and resource allocated for design and development activities;
- Whether software is maintained up-to-date or not.

Recommended controls

- Defining exhaustive and precise user requirements (see section 6.3);
- Planning and implementing appropriate procedure for coding and development (see section 6.4);

- Planning and implementing sufficient acceptance testing (see section 6.5);
- Planning and implementing appropriate version control (see section 6.11);
- Planning and implementing sufficient personnel training (see section 6.18).

5.9 Delivery of erroneous data or delivery of data to unauthorised third parties

Delivering data to the wrong party is an obvious breach to confidentiality identified in ISO 19475 [52]. Delivering erroneous data may induce various detrimental consequences on the customers and their activities.

Recommended preventive actions for this risk include:

- Maintaining up-to-date written procedures for the preparation and communication of reports and other data to external parties (see section 6.1);
- Implementing a peer-review and/or dual authorisation step to allow submission of data to external parties.

6. Controls

This section describes controls that can be implemented to mitigate risks related to computer systems and comply with identified requirements from the ISO/IEC 17025:2017 [1].

6.1 Documented procedures and technical records

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 5.5 c)**: procedures shall be documented "to the extent necessary to ensure the consistent application of its laboratory activities and the validity of the results" [1];
- **Clause 6.4.3**: procedures shall be established for "handling, transport, storage, use and planned maintenance of equipment";
- **Clause 6.4.13**: records shall be retained for equipment description, location, calibration, maintenance and acceptance testing;
- **Clause 7.5.1**: records of laboratory activities shall be complete with metadata and information that may influence the result and "enable the repetition of the laboratory activity under conditions as close as possible to the original." [1];
- **Clause 8.4.1**: legible laboratory records shall be established and retained to demonstrate fulfilment of ISO/IEC 17025 requirements [1].

Recommendations

For the purpose of the present guidelines, it is recommended that:

- The different activities carried (or event occurring) through the life cycle of computer systems be subject to written documented procedures, including where appropriate:
  - Installation;
  - Acceptance testing (see also section 6.5);
  - Use and handling;
  - Failures and disaster;
  - Maintenance (see also section 6.6);
  - Calibration;
  - Decommissioning (see also section 6.14);
- The different activities carried through the life cycle of data be subject to written documented procedures, including where appropriate:
  - Capture (including generation from test activities and reception from external sources);
  - Storage (see also section 6.14);
  - Access, use and transmission (see also section 6.13);
  - Modification (see also section 6.11);
  - Disposal (see also section 6.14);
- Activities be performed by competent and authorised personnel;
- Procedures specify personnel responsibilities, competence and authorisation;
- Procedures involving verification activities specify:
  - Acceptance criteria;
  - Instructions in the event acceptance criteria are not met;
- For recurring laboratory activities (including reception and disposal of samples, measurement, data processing, calibration and maintenance of equipment…), templates be established and verified (see section 6.5);
- Records contain complete metadata, including, where appropriate:
  - What: identification of the activity performed, samples processed/analysed, data processed, *etc.*;
  - When: date (and time) of the recorded activity;
  - Who: personnel responsible for the recorded activity;
  - Why: purpose of the recorded activity;
  - Where: location where the activity is performed (*e.g.*, coordinate for activities performed outside laboratory premises, or room for activities performed within laboratory premises);

  - How: identification of the material (equipment, reagents, *etc.*) and method (procedure);

- Completeness and/or validity of records be ensured through "validation rules" (*e.g.*, a validation rule can be implemented to ensure that a digital record in a database can only be saved when complete, or data in a specific field of a spreadsheet can only be entered when other fields are complete and/or valid);
- Records be non-repudiable;
- Data capture, processing and transmission be automated when possible, *e.g.* through the implementation of LIMS, data loggers, scripts, *etc.*

Note: some recommendations in other sections are also applicable to technical records (*e.g.*, in sections 6.10,6.11,6.12,6.13,6.14,6.15,6.16).

Further guidance can be found in the following references:

- ISO/IEC 27002 on information security controls [3];
- ISO 14641 on the design and operation of an information system for the preservation of electronic documents [21].

6.2 Technical documentation

Relevant clauses from ISO/IEC 17025:2017 [1]

Clause 7.2.1.2: "methods, procedures and supporting documentation, such as instructions, standards, manuals and reference data relevant to the laboratory activities, shall be kept up to date and shall be made readily available to personnel"

Recommendations

For the purpose of the present guidelines, it is recommended that:

- For OTS systems, all technical documentation (including specifications and requirements) available from the manufacturer/developer be retained;
- For systems or software developed in-house, detailed technical description and specification be written and retained;
- Technical specification for hardware include:
  - A list of peripheral devices, modules, components and consumables with serial number or other technical identification or description (*e.g.*, thread and tubing sizes);
  - Description of communications, electrical circuit and piping (*e.g.*, on diagrams);
- Technical specification for software include:
  - A list of software that are necessary to operate the system with their version and date of installation (this is especially important when the system comprises a desktop computer because change of software is more frequent);

- The source code;
- Release notes.

6.3 User requirements, procurement and design qualification

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 6.6.1**: externally provided products and services shall be suitable;
- **Clause 6.6.2**: the laboratory shall have documented procedure(s) for establishing and reviewing its requirements and acceptance criteria regarding the provision and verification of externally provided products and services;
- **Clause 6.6.3**: the laboratory shall communicate its requirements and acceptance criteria to external providers;
- **Clause 6.4.2**: requirements of the ISO/IEC 17025:2017 [1] for equipment shall also be met for those outside of the permanent control of the laboratory. For the purpose of this guidelines, this includes off-site computer systems controlled by external providers and used by the laboratory for cloud computing purposes;
- **Clause 7.11.4**: when the laboratory information management system is hosted, maintained and/or otherwise managed by an external providers, the laboratory shall ensure that external providers meets applicable requirements of ISO/IEC 17025:2017 [1].

Related controls from ISO/IEC 27001:2022 [2]

- **Control 8.26**: security requirements should be identified, specified and approved when developing or acquiring software;
- **Control 8.30**: requirements for outsourced development of system and software should be communicated to the external provider; and compliance to these requirements shall be verified.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- The process for the definition and approbation of user requirements and the process for procurement be subject to written and documented procedure(s) (see section 6.1);
- User requirements be defined:
  - Before starting the in-house development or procurement of a new system, module, software or services;
  - Before the need for a new system or service becomes critical;
- User requirements be defined based on:
  - Previously identified failures and non-conforming work;

  - User experience with similar systems, software or services;
  - Risk assessment (see Chapter 4);
- User requirements be divided in (at least) two categories:
  - Essential requirements: those for which an offer cannot be accepted if the requirements are not met;
  - Desired/optional characteristics: based on which an offer will be selected among other offers.
- User requirements include the provision of sufficient evidence of proficiency of the external provider[6], especially fulfilments of ISO/IEC 17025:2017 [1] requirements for equipment (clauses under 6.4). Such evidence can be acquired by conducting audits of the external provider or selecting an external provider having independent recognition of proficiency, *e.g.*:
  - Accreditation to ISO/IEC 17025 [1] for calibration;
  - Accreditation to ISO 27001 [2] for information security;
  - Recognition from a national authority;
  - Recognition from other internationally recognised organisation.
- For custom systems and software, user requirements cover licensing agreement, source code ownership and intellectual property rights;
- User requirements cover the following aspects when relevant:
  - Functional requirements (*i.e.*, what the computer system, software or module should do):
    - For measuring instruments:
      - Parameters to be measured;
      - Presence of a stand-by mode;
      - Automatic operations, *e.g.*:
        - Automatic calibration;
        - Automatic injection/sampling (*i.e.*, with an autosampler);
        - Automatic dilution or injection of a lower or higher volume (*e.g.*, when the signal of a sample is out of the calibration range);
        - Automatic identification of failures to assist maintenance (*i.e.*, diagnostic features);
        - Automatic parameter optimisation (*e.g.*, auto-tuning);

[6] Especially for the hosting and management of information management system and the provision of cloud computing services

- For data processing software:
  - Library-based identification;
  - Handling of calculations related to internal standard, standard addition, *etc.*;
- For software in general, features supporting information security, *e.g.*:
  - Audit trail;
  - Automatic backups;
  - Access control mechanisms (see section 6.13));
  - User error protection mechanisms;

– Non-functional requirements (*i.e.*, how the computer system, software or module should be made or behave):

- The technology:
  - For measuring instruments:
    - the sampling/injection technique(s);
    - the separation technique(s);
    - the detection technique(s);
  - For software:
    - the deployment strategy (offline or cloud-based, on-premises or off-premises);
    - the programming language;
    - the database model (*e.g.*, relational);
- Efficiency, *e.g.*, for measuring instruments:
  - Accuracy;
  - Trueness;
  - Precision;
  - Limits of detection and quantification (working/linear range);
  - Selectivity;
- Effectiveness, *e.g.*, for measuring instruments:
  - Number of samples per unit of time / per sequence;
  - Cost of consumables (gas, energy, water, reagents, solvents, disposable parts such as vials and caps, *etc.*);
  - Cost and frequency of maintenance;

        - Usability and robustness, *e.g.*:
            - Environmental condition in which the system must be able to operate;
            - Battery autonomy;
            - Integrity in case of power outage;
        - Maintainability, *e.g.*:
            - Period during which maintenance will be provided by the external provider;
            - Period during which spare parts will be provided by the external provider;
        - Interoperability and updatability, *e.g.*:
            - Portability;
            - Backward compatibility;
            - Replaceability, *e.g.*, of spare parts;
        - Availability, *e.g.*:
            - For custom software, access to the source code and rights (use, modify and distribute);
        - Security;
        - Non-repudiability of records;
        - Any other aspect covered in the present guidelines;
- The user requirements be impartially communicated to the potential external provider(s) for which an offer is sought;
- Whenever possible, the procurement process include the comparison of several analogous products and/or services available on the market and likely to fulfil the user requirements;
- The most suitable product and/or service be impartially selected based on the user requirements as acceptance criteria. In this regard, the procurement process is considered to include design qualification;
- The provision of externally provided products and services be subject to a legally binding written agreement between the laboratory and the external provider (*i.e.*, a contract) specifying their rights and making both parties accountable for their respective responsibilities;
- The above-mentioned written agreement be concluded (approved by all parties in a binding way) before the provision of the product(s) and/or services begin.

Further guidance can be found in the following references:

- ISO 12207 on software life cycle processes [28];
- ISO/IEC 27102 on guidelines for purchase of cyber-insurance [85];
- ISO/IEC 27002 on information security controls [3];

- ISO/IEC 14143-1 on software functional size measurement [75];
- ISO/IEC 25010 on SQuaRE product quality model [13];
- ISO/IEC TS 25011 on SQuaRE service quality model [86];
- ISO/IEC 25012 on SQuaRE data quality model [87];
- ISO/IEC 27036-1 on cybersecurity and supplier relationship [88];
- PMBOK5 [70];
- AGIT guidelines on the validation of computerised systems [60];
- ISPE GAMP5 [82];
- USP chapter 1058 [76].

6.4 Development

Related controls from ISO/IEC 27001:2022 [2]

- **Control 8.25**: rules for the secure development of software and systems shall be established and applied;
- **Control 8.28**: secure coding principles shall be applied for software development.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Development of in-house software and systems be subject to written and documented procedure(s) (see section 6.1);
- Development activities be conducted in a separate environment from other activities with appropriate access control (*e.g.*, offline, in "sandbox mode", on a different dedicated system or network, *etc.*);
- Development activities be carried through appropriate and dedicated tools such as integrated development environment;
- Acceptance testing be conducted throughout development;
- Appropriate technical guidelines be implemented and audited.

Further guidance can be found in:

- ISO/IEC TR 24772-1 on language-independent guidance to avoiding vulnerabilities in programming languages [78];
- ISO/IEC 27002 on information security controls [3];
- ISO/IEC TR 7052 on the control of frequently occurring risks during development and maintenance of custom software [89];

- OWASP secure coding guidelines [90];
- OWASP Top Ten [91];
- NASA's "10 rules" [92].

6.5 Acceptance testing

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 6.4.4** and **6.4.9**: the laboratory shall verify that equipment meets requirements before being placed or returned to service (for example, after being taken out of service following failure and maintenance);
- **Clause 6.4.10**: intermediate checks shall be performed accordingly with a procedure;
- **Clause 6.4.13 c)**: records shall be retained for equipment verification;
- **Clause 6.4.5**: the laboratory shall verify that equipment used for measurement meets performance requirements;
- **Clause 6.6.1 and 6.6.2**: the laboratory shall verify that externally provided products and services meet the laboratory requirements;
- **Clause 7.2.1.5**: the laboratory shall verify that methods can be properly applied before implementing them. For the purpose of this guidelines, this includes the proper use of computer systems where they can influence the results;
- **Clause 7.11.2**: the laboratory information management system(s) used for the collection, processing, recording, reporting, storage or retrieval of data shall be validated before implementation;
- **Clause 7.11.6**: calculation and data transfer operations shall be verified;
- **Clause 7.7.1 c)**: the laboratory shall have procedure(s) for functional check(s) of measuring and testing equipment.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 8.29**: features related to information security should be tested;
- **Control 8.31**: development, testing and production environment should be separated;
- **Control 8.33**: test information should be appropriately selected and protected.

Recommendations

Various models and workflows describe acceptance testing activities of computer systems and/or software as part of their lifecycle. Some are linear (*e.g.*, the V-model [82], the waterfall model, *etc.*) and other are cyclic (*e.g.*, agile philosophy and the spiral model).

It is not the purpose of the present guidelines to discuss existing models nor to promote a specific one. The choice to follow (or not) a specific methodological standard or guideline document is up to the laboratory.

Note 2 to clause 7.11.2 of ISO/IEC 17025:2017 [1] states that OTS information management system(s) can be considered sufficiently validated. Still, it may be appropriate to verify other aspects, *e.g.*:

- Compatibility and interfacing with other systems and modules within the laboratory;
- Information security in the real operating environment;
- Use and handling by personnel.

For the purpose of the present guidelines, it is recommended that:

- Acceptance testing activities be subject to written and documented procedure(s) (see section 6.1);
- Whenever possible, acceptance testing activities be conducted in a separate environment from other activities (*e.g.*, offline, in "sandbox mode", on a different dedicated system or network, *etc.*), and access to the testing environment should appropriately restricted;
- When the acceptance testing must be conducted in the real/intended working environment, the appropriate precautionary measures should be applied (*e.g.*, conducting acceptance testing at times where its impact on other activities is minimal);
- Acceptance testing be considered at the following stages of the life cycle of computer systems and/or software:
  - Throughout development[7];
  - Before implementation in the operational environment;
  - After installation (or relocation) in the operational environment and before use (those are referred to as installation qualification (IQ));
  - On a regular basis, *e.g.*, before use (those are referred to as system suitability tests (SST));
  - After updates and maintenance;
  - After failures.
- Acceptance testing cover functional and non-functional requirements, especially those related to information security;
- The extent of acceptance testing be scaled accordingly with the importance of the system and risk;
- For systems and software developed in-house, acceptance testing be ultimately conducted by personnel not involved in development;

[7] Accordingly with the maxim "fail early, fail often", which can be understood as "the earlier and the more frequently errors are searched/detected, the less impact they will have on the development process.

- Acceptance testing be conducted using both black-box testing and white-box testing methods whenever possible;
- Acceptance testing of non-functional features/characteristics (*e.g.*, information security, errors, vulnerabilities) be performed both by humans and using automated software (*e.g.*, static application security testing (for white-box testing) and dynamic application security testing (for black-box testing);
- Records related to acceptance testing clearly states whether the tested item conforms to specification and, if not, what corrective actions are required before repeating the test;
- When acceptance testing is performed by an external provider, appropriate records be obtained and retained (*e.g.*, certificate, service reports);
- Dummy data be used for testing purpose (instead of real data) so that confidentiality is preserved even in case of data breach. Realistic dummy data can be obtained by copying real data sets and obfuscating them (randomisation and/or anonymisation) in such a way that data breach does not compromise confidentiality;
- Data used for testing be cleared from the testing environment after completion of the testing activities;
- Installation qualification cover at least the following aspects when relevant:
  - Environmental conditions (*e.g.*, temperature, humidity, dust, vibration, electric and magnetic field and radiation, *etc.*);
  - Facilities (*e.g.*, power, water and gas supplies);
  - For software, the performance of the supporting hardware;
  - Connection and communication with other computer systems, software and modules;
- Acceptance testing of functional features/characteristics cover the full range of intended use, including:
  - For hardware, the full range of parameters (*e.g.*, oven temperature, wavelength, flow rate, pressure, *etc.*);
  - For software, all the used features, including (but not limited to) data processing (peak integration, calculation, *etc.*), data import, export, backup, access control features, audit trail features, *etc.*;
- Appropriate statistical process control tools (*e.g.*, Shewart control charts, cumulative sum control charts, EWMA control charts, *etc.*) be used to support system suitability tests;

Installation qualification and operational qualification can be performed by an external provider with its own procedures. In this case, it does not need to be repeated by the laboratory [33,60,76].

Further guidance can be found the following references:

- ISO/IEC 27002 on information security controls [3];
- ISO/IEC 25019 on SQuaRE quality-in-use model [93];
- ISO/IEC 25022 on SQuaRE measurement of quality in use [94];

- ISO/IEC 25023 on SQuaRE measurement of system and software product quality [95];
- ISO/IEC 25024 on SQuaRE measurement of data quality [96];
- ISO/IEC TR 24772-1 on language-independent guidance to avoiding vulnerabilities in programming languages [78];
- ISO 7870-1 on general guidelines for control charts [97];
- OWASP Top Ten [91].

6.6 Maintenance

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 6.4.3**: procedures shall be established for planned maintenance of equipment;
- **Clause 6.4.13 g) and h)**: records shall be retained for equipment damage, failures and maintenance;
- **Clause 7.11.3 d)**: the information management system shall be maintained in a way that ensures data integrity.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 7.13**: equipment should be maintained appropriately.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Maintenance activities be subject to written and documented procedure(s) (see section 6.1);
- Records be retained for suspected and actual faults as well as maintenance;
- Maintenance plans specify:
  - The frequency or triggers for preventive maintenance;
  - The triggers for corrective maintenance;
- Appropriate tests be conducted after maintenance and before return to service (see section 6.5).

Further guidance can be found the following references:

- ISO/IEC/IEEE 14764 on software maintenance [67].

6.7 General inventory and logbooks

Relevant clauses from ISO/IEC 17025:2017 [1]

Clause 6.4.13 a), b) and d): records shall be retained for equipment description and location;

Clause 7.11.3 e): information management system shall record system failure.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- An up-to-date inventory of all computer systems be maintained, listing for each one the information that are not expected to change on a regular basis, such as:
  - Its unique identifier within the laboratory;
  - The manufacturer;
  - The model;
  - The serial number;
  - The software/firmware version;
  - The physical location of the hardware within the laboratory;
  - The virtual location (*i.e.*, path) of the software files and data;
  - The digitalised process(es) in which it is used and for what purpose(s) (*e.g.*, the same desktop computer can be used to process data (*e.g.*, integrates chromatograms), receive and send emails, *etc.*);
  - Personnel authorisation and responsibilities;
- Records related to the same computer system be linked together in a logbook. Logbook records can be on paper, digital or both. A logbook does not need to be a single document, *i.e.*, it can be a compilation of individual documents; although at some point in time, it is often desirable to gather all the different documents and records constituting a logbook in a single document or file to improve availability and/or for archiving purpose. A logbook does not even need to be a document at all, *i.e.*, records in a database and audit trail records can be considered as a part of a logbook;
- Logbooks records metadata be complete (see section 6.1);
- Logbooks records be non-repudiable;
- Logbooks includes records about:
  - Installation and relocation;
  - Use and handling;
  - Failures and disasters;
  - Maintenance;

  - Calibration;
  - Decommissioning;
- Generation of logbooks records be automated using, *e.g.*, audit trail features when available;
- Logbook data and metadata (or, at minimum, a backup thereof) be stored on a storage medium physically and digitally independent from the computer system to which they relate in order to remain accessible and readable at all times, even when the computer system to which they relate is unusable (*e.g.*, because of power outage or other failure). For example, the laboratory should configure any available audit trail features to save and store data on an independent hardware (*e.g.*, external HDD, SSD, NAS or server) whenever possible. If this is not possible, migration should be planned at appropriate frequency.

6.8 Environmental conditions

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clauses 6.3.1 to 6.3.4**: the laboratory shall have written requirements for environmental conditions where they can adversely affect the result and they shall be monitored and controlled through appropriate measures;
- **Clause 7.11.3 c)**: the information management system "be operated in an environment that complies with provider or laboratory specifications".

Related controls from ISO/IEC 27001:2022 [2]

- **Control 7.5**: physical protection against physical and environmental threats should be implemented;
- **Control 7.8**: equipment should be located securely.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- The monitoring and control of environmental conditions be subject to written and documented procedure(s) (see section 6.1);
- Recommendations from the manufacturer regarding physical environment of computer systems be followed;
- Computer systems be located at a sufficient distance (possibly in a different room) from sources of adverse environmental conditions (*e.g.*, excessive heat, humidity, corrosive substances, dust, electromagnetic fields/radiation, shock, *etc.*);
- Where a sufficient distance between sources of adverse environmental conditions and computer systems cannot be maintained, physical protection be implemented (ventilation, cover, protection screens or grids, cooling, *etc.*);

- Environmental conditions be monitored using automated means (*e.g.*, data loggers) where their control is critical for the accuracy of test results and/or information security (*e.g.*, for storage of samples);
- Appropriate disaster detection systems be implemented and maintained (*e.g.* fire detection, flood detection, intrusion detection, *etc.*);
- Appropriate disaster control systems be implemented (*e.g.*, fire extinguishers and fire-extinguishing system, fire-rated doors, lightning rods, electrical surge protection systems, dykes or pumps to control flooding, alert in case of intrusion, *etc.*).

6.9 Redundancy of facilities

Related controls from ISO/IEC 27001:2022 [2]

- **Control 8.14**: facilities redundancy should be sufficient to meet availability requirements.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Redundancy be implemented for critical facilities when appropriate and possible, *e.g.*:
  - Redundant servers so that the other(s) can take-over when the first is, *e.g.*, overloaded or under maintenance;
  - Redundant data storage for backup, *e.g.*:
    - Multiple storage devices on a computer system;
    - Synchronisation on a cloud;
  - Emergency power supply (*e.g.*, batteries), especially when power outage may result in unacceptable downtime, risks for information security or risks for the integrity of personnel, computer system, samples or other materials;
- Redundant facilities be tested at appropriate frequency and extend to ensure they operate readily and efficiently in case the main facility is out of service;
- The management of redundant facilities be consistent with those of their main analogue to ensure that they do not constitute vulnerabilities for information security.

Further guidance can be found in the following references:

- ISO/IEC 27002 on information security controls [3];
- ISO/IEC TS 23167 on common technologies and techniques for cloud computing [98].

6.10 File format

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 8.4.1**: legible laboratory records shall be established and retained to demonstrate fulfilment of ISO/IEC 17025 requirements [1].

Recommendations

For the purpose of the present guidelines, it is recommended that open file formats be preferred to proprietary file formats for digital records and documents whenever available.

6.11 Change control

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 6.4.13**: records shall be retained for equipment modification;
- **Clause 7.11.2**: changes to information managament systems shall be authorised, documented and validated before implementation;
- **Clause 8.3.2 c)**: modifications and the current revision status of documents shall be identified;
- **Clause 7.5.2**: amendments to technical records shall be tracked to previous or original versions and both the original and amended data/files shall be retained with complete metadata, including the date of alteration, an indication of the altered aspects and the personnel responsible for the alterations.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 8.19**: software installation should be managed accordingly with procedures;
- **Control 8.32**: changes to information processing system should be subject to change management procedures.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Change control be subject to written documented procedure(s);
- Change control cover:
  - Installation and decommissioning of computer systems;
  - Replacement of computer systems parts;
  - Installation, modification/update and uninstallation of software;
  - Creation, modification or deletion of users in identity management systems;
  - Modification of access rights;

    - Modification and deletion of digital records, digital documents and important digital files (*e.g.*, instrument methods, data processing methods, *etc.*). This point is closely related to access control (see section 6.13);

- Change control rely on appropriate access control (see section 6.13);
- Software be updated when updates contribute to improved information security, *e.g.*, solving vulnerabilities and bugs;
- Software installation and update be carried only after appropriate acceptance testing (see section 6.5);
- Changes be approved by authorised personnel before proceeding;
- Changes be communicated to relevant personnel and interested parties;
- Version conflict be managed and/or prevented, *e.g.* by using centralised data storage and version control systems or blockchain;
- Changes be implemented in such a way that information security of previous versions is preserved, *e.g.*, by:
    - Issuing a new version of the item instead of modifying it directly (note that this is mandatory for reports after issue accordingly with **clause 7.8.8.2** [1]);
    - Using audit trail features (*e.g.*, track changes features in text processing and spreadsheets editing software);
- The various versions of an item under change control be systematically and uniquely identified to avoid any confusion (see section 6.12);
- Current and previous versions of software be retained in such a way that backward recovery is ensured;
- Amendments and changes be identified unambiguously and justified, *e.g.*:
    - For documents, the modified parts can be highlighted in a specific colour and a side-note or footnote added for justification;
    - For software, release notes should be obtained or written and retained.

Further guidance can be found in the following references:

- ISO 14641 on the design and operation of an information system for the preservation of electronic documents [21].

6.12 Indexing

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 8.4.7**: records shall be readily accessible.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Digital items be systematically classified and identified;
- Classification and identification of digital items rely on a combination of relevant metadata such as:
  - The type of data, file or document;
  - The issuing date, preferably expressed in the order year-month-day so that alphabetical order corresponds to chronological order;
  - The version of the item;
  - The author name or function;
  - The corresponding entity (*i.e.*, to whom it originates or is addressed), for example:
    - The customer (*e.g.*, invoices, orders, test reports, invoices, *etc.*);
    - The external provider (*e.g.*, invoices, orders, invoices, *etc.*);
- Item identifiers contain a common part for all versions of the same original item.

6.13 Access control

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 4.2.1**: all information and data shall be considered confidential, except when already made public by the customer or otherwise specified in written agreement with the customer;
- **Clause 7.11.3 a) and b)**: the information management system shall be protected from unauthorised access, tampering and loss.
- **Clause 8.4.2**: access to laboratory records shall be consistent with the laboratory confidentiality commitments.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 7.4**: premises should be monitored for unauthorised physical access;
- **Control 8.1**: information accessed via, stored on and/or processed by users endpoint devices should be protected;
- **Control 8.2**: the allocation of access rights should be restricted and managed;
- **Control 8.3**: access control should be implemented for information assets;
- **Control 8.4**: access to source-code should be appropriately managed;
- **Control 8.5**: appropriate authentication technologies should be used;
- **Control 8.7**: protection against malware should be implemented;

- **Control 8.11**: data masking should be considered for the protection of sensitive data;
- **Control 8.16**: access to resources should be monitored to detect anomalous behaviour;
- **Control 8.18** utility programs able to override systems and application controls should be controlled and restricted;
- **Control 8.22**: systems, software and users should be segregated in different networks as appropriate;
- **Control 8.23**: access to external websites should be managed to reduce exposure to malicious content.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- The definition and management of access control measures be subject to written and documented procedure(s);
- Access rights be specified and implemented for personnel, computer systems and software applications;
- Access rights be managed by authorised competent personnel with privileged access rights (*i.e.*, "administrators") through appropriate identity management system(s);
- Authentication and access control rely on appropriate techniques and cryptographic technologies, *e.g.*:
  - Dual authorisation;
  - Multi-factor authentication;
  - Virtual Private Network;
  - Blockchain;
  - Data encryption;
- Hardware be physically monitored and protected against theft, sabotage and unauthorised access, *e.g.*, by:
  - Locating hardware in locked area;
  - Implementing appropriate intrusion systems;
- Utility software be tightly controlled (*e.g.*, stricter authentication requirements), and be only installed/used when necessary by authorised competent personnel;
- Laboratory network(s) be separated from the public network (*i.e.*, internet);
- When necessary, laboratory network be subdivided in different physical or virtual sub-networks with various levels of security and access control, accordingly with the identified level of risk;
- Passwords and cryptographic keys be sufficiently complex to resist to brute-force attacks and dictionary attacks. Usually, the higher the number and variety of characters (*i.e.*, lower-case,

upper-case, numbers and special characters), the longer it takes to find a password or key through brute-force attack and the probability of it being found is low;

- Exchange of (sensitive) data over a network (especially over the internet) be appropriately restricted when the risk of it being intercepted and/or read by an attacker needs to be controlled;
- Sensitive data be encrypted when exchanged over a network (including over the internet) (*e.g.*, sent by email) or taken out of the laboratory on portable storage media devices and/or user endpoint devices;
- Access control be implemented when resources needs to be accessed remotely from outside the laboratory network (*e.g.*, for remote working);
- Storage of (sensitive) data on user endpoint devices be appropriately restricted when the following risks need to be controlled:
  - Version conflict;
  - Physical loss or left of the user endpoint devices or storage media;
  - Malware reaching the user endpoint devices;
- Personal devices (*e.g.*, desktop computers, laptops, tablets and smartphones) not be used for laboratory purposes and therefore, personal devices should not be given access rights to laboratory resources, except for the purpose of multi-factor authentication (*e.g.*, when one-time passwords are used for authentication);
- Laboratory computer systems be only used for laboratory purposes;
- Access to remote resources be terminated after a defined period of inactivity;
- Software for detection and protection against malware be implemented (*e.g.*, by using web filters, firewall, antivirus, intrusion detection system and/or intrusion prevention system) and kept up-to-date;
- Access to laboratory resources be controlled and recorded when appropriate using, *e.g.*, audit-tail features, web filters, virtual Private Network, firewall, antivirus, intrusion detection system and/or intrusion prevention system;
- Access rights be limited to those required and sufficient to fulfil their duties and responsibilities (*i.e.*, by default, access should be restricted unless necessary), for example:
  - Access rights to external websites be restricted as necessary to prevent exposure to malicious content such as phishing and malwares, *e.g.*, by using web filtering;
  - Data masking be implemented (*e.g.*, in database queries) to restrict access to data;
  - Write access to source code be restricted for personnel other than developers, whereas read access to it be restricted to personnel other than personnel responsible for audit and testing;
  - Privileged access rights only be used for tasks that requires them;
- Rights to change date and time should be appropriately restricted.

Further guidance can be found in the following references:

- ISO/IEC 11770-1 on key management [99];
- ISO/IEC 11770-2 on key mechanisms using symmetric techniques [100];
- ISO/IEC 11770-3 on key mechanisms using asymmetric techniques [101];
- ISO/IEC 11770-4 on key mechanisms based on weak secrets [43];
- ISO/IEC 27002 on information security controls [3];
- ISO/IEC 27005 on guidance on managing information security risks [102];
- ISO/IEC 27032 on guidelines for internet security [69];
- ISO/IEC 27033-1 on overview and concepts of techniques for network security [56];
- ISO/IEC 27033-2 on guidelines for the design and implementation of networks security [103];
- ISO/IEC 27033-4 on securing communications between networks using security gateways [77];
- ISO/IEC 27036-1 on overview and concepts of cybersecurity and supplier relationship [88];
- ISO/IEC 27036-2 on requirements for cybersecurity and supplier relationship [104];
- ISO/IEC 27036-3 on guidelines for hardware, software, and services supply chain security;
- ISO/IEC 27036-4 on guidelines for security of cloud services;
- ISO/IEC 27039 on selection, deployment and operations of intrusion detection and prevention systems (IDPS) [46];
- ISO/IEC 27040 on storage security techniques [40];
- ISO/IEC TS 27100 on overview and concepts of cybersecurity [36];
- ISO/IEC 29115 on entity authentication assurance framework [65];
- ISO/IEC 29146 on access management framework [9].

6.14 Archiving and disposal

Digital items can be archived in multiple ways:

- Digitally and electronically, *e.g.*, by:
  - Modifying the access right or assigned privileges related to it (*e.g.*, configure the file(s) to read-only);
  - Transferring the digital data or document to a different storage location of the record system (*e.g.*, different file, directory or table of a relational database) with restricted access rights (*e.g.*, read-only);
  - Transferring or copying the items to a physically distinct and independent hardware with restricted access rights such as HDD, SSD, NAS or server protected against relevant risk sources such as physical deterioration, human mistakes and cyberattacks;

- Digitally but non-electronically, *e.g.*, by burning on optical storage media;
- Non-digitally and non-electronically, *e.g.*, by printing on paper. However, many digital items cannot be printed conveniently or without loss of integrity or reused after printing.

Reciprocally, non-digital data can be archived digitally (*e.g.*, through digitisation).

It must be highlighted that "regular" deletion of data or files may not necessarily be irreversible. Commonly, the action of deletion of a file only marks the storage space occupied by the file as available for writing of new data. As long as this space is not overwritten, the "deleted" data can still be fully or partially recovered by recovery software, and it may takes some times for the original data to be sufficiently overwritten to be properly non-recoverable.

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 8.4.1**: legible records shall be established to demonstrate the fulfilment of ISO/IEC 17025 [1] requirements;
- **Clause 8.4.2**: appropriate controls for the storage, archiving, retrieval, retention time, and disposal of retained records shall be implemented.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 7.14**: the deletion of sensitive and licensed data from equipment containing data storage media shall be verified before proceeding to disposal or re-use;
- **Control 8.10**: data shall be deleted when no longer required.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Processes for archiving, migration and disposal/deletion of archived items be subject to written documented procedure(s);
- Digital items be archived when they no longer need to be edited;
- The following digital items be archived:
  - Raw data;
  - Processed data;
  - Records;
  - Documents;
  - Files;
  - Software;
- Archived items remain available for reading to fulfil laboratory activities;
- Archived items be subject to backups (see section 6.15));
- The retention time before disposal of archived items be specified and recorded;

- Data be migrated and/or deleted from systems before decommissioning and/or disposal;
- Appropriate techniques be implemented for the disposal of data and/or storage medium (*e.g.*, physical destruction (*e.g.*, shredding, drilling, *etc.*), cryptographic deletion, degaussing or data wiping);
- Proper and complete disposal of items be verified.

Further guidance can be found in the following references:

- ISO 13008 on digital records conversion and migration process [105];
- ISO/IEC 27002 on information security controls [3];
- ISO/TR 17797 on the selection of digital storage media for long term preservation [106];
- ISO 14641 on the design and operation of an information system for the preservation of electronic documents [21];
- ISO/TS 18759 on functional and technical requirements for trustworthy storage system (TSS) [72];
- ISO/IEC 27040 on storage security techniques [40].

6.15 Backups

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 8.4.2**: appropriate controls for storage and backup of retained records shall be implemented.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 8.13**: backup of data and software should be maintained and tested.

Recommendations

A widespread rule of thumb for backups is the "3-2-1" rule:

- There should be (at least) **three** backup copies;
- These copies should be stored on (at least) **two** different media;
- Among these media, (at least) **one** should be off-premises (implicitly, at least one should be on-premises).

For the purpose of the present guidelines, it is recommended that:

- Backups generation, testing and backward recovery processes be subject to written and documented procedure;
- Backups be considered for all important digital items (documents, records, files, software, *etc.*);

- Backup frequency and extent be scaled appropriately with the identified risk level. For important data, it is recommended that multiple backup copies be maintained accordingly with the “3-2-1” rule;
- Backups be tested at appropriate frequency for:
  - Integrity;
  - Avalailability;
  - Readability;
  - Backward recovery.

6.16 Digital signatures

When a digital media is rewritable (*i.e.*, most electronic digital formats), digital signatures relying on cryptographic techniques allow to ensure data integrity [21].

Examples of digital signatures include:

- Hash values, which are inherent to the data themselves;
- Other forms of digital signatures relying on a private key and a public key. The eIDAS regulation [14] and related Commission decisions describes two kinds of such digital signatures: advanced electronic signatures and qualified electronic signatures.

For the purpose of the present guidelines, it is recommended that digital signatures be used for the verification of data authenticity and integrity.

- ISO/IEC 10118-1 on hash functions [58];
- ISO/IEC 14533-1 on long term signatures profiles for PDF Advanced Electronic Signatures (PAdES) [107].

6.17 Electronic Document Management Systems (EDMS)

Electronic Document Management Systems (EDMS) are designed for data integrity can be used for the convenient implementation of recommendations of the present guidelines.

For the purpose of the present guidelines, it is recommended that an EDMS be implemented whenever appropriate and possible.

Further guidance can be found in the following references:

- ISO 14641 on the design and operation of an information system for the preservation of electronic documents [21];
- ISO 19475 on document management [52];
- ISO 18759/TS on functional and technical requirements for trustworthy storage system (TSS) [72];

- ISO/TR 15801 on recommendations for trustworthiness and reliability [108].

6.18 Personnel

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Clause 6.2.2**: competence requirements for personnel shall be documented;
- **Clause 6.2.3**: personnel shall "have the competence to perform laboratory activities for which they are responsible and to evaluate the significance of deviations".

Related controls from ISO/IEC 27001:2022 [2]

- **Control 6.2**: personnel employment agreement should state responsibilities of personnel and laboratory regarding information security;
- **Control 6.3 and 8.7**: personnel should receive appropriate training regarding information security and malware awareness;
- **Control 6.4**: disciplinary process should be enforced against personnel infringing policies and rules;
- **Control 6.5**: information security responsibilities remaining valid after employment termination should be communicated and enforced;
- **Control 6.6**: legally binding confidentiality and non-disclosure agreements should be established as necessary to enforce confidentiality policies.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Personnel recruitment, training and resigning be subject to written and documented procedure(s);
- Requirements for personnel competence and/or experience be specified and cover:
  - Technical aspects related to the computer systems they are required to use;
  - Other relevant aspects of the present guidelines;
- Personnel responsibilities regarding aspects covered in the present guidelines be specified in employment contract, procedure(s) and/or code of conduct;
- Personnel employment contract includes necessary non-disclosure agreements that remains applicable after contract termination;
- Training on the use, calibration and/or maintenance of computer systems be provided before first use and after major changes;
- Training on laboratory policies and procedures be provided after recruitment and after major changes;

- Both internal and external training should be considered. Training can be provided in various forms, including lectures, booklets, posters, emails, e-learning modules, *etc.*;
- Personnel training be prepared accordingly with:
  - Attendee's functions and responsibilities;
  - Current personnel competence (and deficiencies);
  - Observed non-conforming work and incidents;
- Personnel training be provided in the following situations:
  - After recruitment or substantial change of functions;
  - Before using a computer system (or using it for a specific procedure or application) for the first time;
  - After major changes of the system such as software updates;
  - After non-conforming work is observed;
  - On a regular basis;
- Personnel's understanding of the training be assessed and training continued until sufficient understanding is verified;
- Disciplinary process be enforced against personnel violating laboratory policies and rules. This process should take into consideration:
  - The nature and gravity of the violation;
  - Whether the violation was intentional or not;
  - Whether other violations have been committed in the past;
  - Whether the violator was properly trained or not;
- Whenever possible, personnel leaving the laboratory be required to document their knowledge and experience;
- When personnel is resigning, their access rights, personnel data, user data and profiles in identity management systems be appropriately revoked and/or deleted.

6.19 Event reporting

Relevant clauses from ISO/IEC 17025:2017 [1]

- **Control 6.4.13 h)**: records shall be retained for damage and malfunction;
- **Clause 8.7.1 a)**: the laboratory shall react to non-conformities by taking actions and addressing their consequences.

Related controls from ISO/IEC 27001:2022 [2]

- **Control 6.8**: a mechanism for timely report of observed information security events should be implemented.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- The actions taken in reaction to- and the reporting of information security events, damage, failures, and non-conformance with regard to the laboratory's own procedures and policies, to regulation or to ISO/IEC 17025:2017 [1] be subject to written and documented procedure(s);
- The following information security events be reported:
  - Cyberattacks;
  - Insider attacks;
  - Accidental delivery of information to the wrong party (*e.g.*, sending a test report to the wrong customer);
  - Accidental delivery of erroneous data;
  - Accidental alteration (edition, deletion) of data;
  - Failure of controls (*e.g.*, access control, version control or backups);
  - Events detected by intrusion detection systems;
  - Other appropriate events.

6.20 Internal audits

Relevant clauses from ISO/IEC 17025:2017 [1]

Clauses 8.8.1 and 8.8.2: internal audits shall be planned to gather evidence on whether the management system is conform to the laboratory's own requirements and to requirements of ISO/IEC 17025:2017 [1].

Related controls from ISO/IEC 27001:2022 [2]

Control 8.34: audit activities should be planned in such a way as to minimize their impact other activities.

Recommendations

For the purpose of the present guidelines, it is recommended that:

- Internal audits be subject to written and documented procedure(s);
- Internal audits cover all aspects discussed in the present guidelines when relevant;

- Audit activities be conducted with only consultation/reading access right whenever possible [3];
- When audit activities requiring access rights other than consultation/reading are conducted:
  - Backup copies be generated before starting the audit activities;
  - Security systems (*e.g.*, firewall, antivirus, intrusion detection system and/or intrusion prevention system) be verified and updated if necessary;
  - Audit activities take place in a specific and secure testing environment when possible [3].

Further guidance can be found in the following references:

- ISO/IEC 27002 on information security controls [3];
- ISO 18829 on the assessment of ECM/EDRM implementations and trustworthiness [109];
- ISO/IEC 25022 on SQuaRE measurement of quality in use [94];
- ISO/IEC 25023 on SQuaRE measurement of system and software product quality [95];
- ISO/IEC 25024 on SQuaRE measurement of data quality [96];

7. Appendices

7.1 Appendix A

The table below links clauses of ISO/IEC 17025:2017 [1] to sections of the present guidelines.

Sections of the present guidelines	Clauses of ISO/IEC 17025:2017
6.1	5.5 c), 6.4.3, 8.4.1
6.3	6.6.1–6.6.3, 6.4.2
6.4	Not covered
6.5	6.4.4, 6.4.5, 6.4.9, 6.4.10, 6.4.13 c), 6.6.1, 6.6.2, 7.2.1.5, 7.11.2, 7.11.6, 7.7.1 c)
6.2	7.2.1.2
6.6	6.4.3, 6.4.13 g)–h), 7.11.3 d)
6.7	6.4.13 a), b) and d), 7.11.3 e)
6.8	6.3.1 to 6.3.4, 7.11.3 c)
6.9	Not covered
6.10	8.4.1
6.11	6.4.13 h), 7.5.2, 7.11.2, 8.3.2 c)
6.12	8.4.7
6.13	4.2.1, 7.11.3 a)–b), 8.4.2
6.14	8.4.1, 8.4.2
6.15	8.4.2
6.16	Not covered
6.17	Not covered
6.18	6.2.2, 6.2.3
6.19	8.7.1 a)
6.20	8.8.1, 8.8.2

7.2 Appendix B

The table below links sections of the present guidelines to clauses of ISO/IEC 17025:2017 [1].

Clauses of ISO/IEC 17025:2017	Sections of the present guidelines
4.2.1	6.13
5.5 c)	6.1
6.2.2–6.2.3	6.18
6.3.1–6.3.4	6.8
6.4.2	6.3
6.4.3	6.1, 6.6
6.4.4	6.5
6.4.5	6.5
6.4.9	6.5
6.4.10	6.5
6.4.13 a), b), d)	6.7
6.4.13 c)	6.5
6.4.13 g)	6.6
6.4.13 h)	6.6, 6.11
6.6.1	6.3, 6.5
6.6.2	6.3, 6.5
6.6.3	6.3
7.2.1.2	6.2
7.2.1.5	6.5
7.5.2	6.11
7.7.1 c)	6.5
7.11.2	6.5, 6.11
7.11.3 a)–b)	6.13
7.11.3 c)	6.8
7.11.3 d)	6.6
7.11.3 e)	6.7
7.11.6	6.5
8.3.2 c)	6.11
8.4.1	6.1, 6.10, 6.14
8.4.2	6.13, 6.14, 6.15
8.4.7	6.12
8.5.1–8.5.3	4
8.7.1 a)	6.19
8.7.1 e)	4
8.8.1–8.8.2	6.20

7.3 Appendix C

The table below lists the links between the present document and the controls listed in Table A.1 from ISO/IEC 27001:2022 [2].

Controls of ISO/IEC 27001:2022 [2]	Sections of the present guidelines
6.1	Not covered
6.2	6.18
6.3	6.18
6.4	6.18
6.5	6.18
6.6	6.18
6.7	6.8, 6.13
6.8	Not covered
7.1	Not covered
7.2	Not covered
7.3	Not covered
7.4	6.13
7.5	6.8, 6.13
7.6	Not covered
7.7	Not covered
7.8	6.8, 6.13
7.9	6.8, 6.13
7.10	6.8, 6.13, 6.14, 6.15
7.11	Utilities are covered by the present guidelines
7.12	Not covered
7.13	6.6
7.14	6.14
8.1	6.13
8.2	6.13
8.3	6.13
8.4	6.13
8.5	6.13
8.6	Not covered
8.7	6.13, 6.18
8.8	Not covered
8.9	Not covered
8.10	6.14
8.11	6.13
8.12	Not covered
8.13	6.15
8.14	6.9
8.15	Definition of the word record
8.16	6.13
8.17	Not covered
8.18	6.13

Controls of ISO/IEC 27001:2022 [2]	Sections of the present guidelines
8.19	6.5, 6.11, 6.18
8.20	Not covered
8.21	Not covered
8.22	6.13
8.23	6.13
8.24	Not covered
8.25	6.3, 6.4, 6.5
8.26	4, 6.3
8.27	Not covered
8.28	6.4, 6.2
8.29	6.5
8.30	6.3
8.31	6.5
8.32	6.11
8.33	6.5
8.34	6.20

References

1. International Organization for Standardization (ISO) *ISO/IEC 17025:2017 – General Requirements for the Competence of Testing and Calibration Laboratories*; Geneva, CH, 2017;

2. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*; Geneva, CH, 2022;

3. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Controls*; Geneva, CH, 2022;

4. European Parliament and Council of the European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* **2016**, *119*.

5. European Parliament and Council of the European Union Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union* **2022**, *333*.

6. International Organization for Standardization (ISO) *ISO 10795:2019 – Space Systems – Programme Management and Quality – Vocabulary*; Geneva, CH, 2019;

7. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) *ISO/IEC/IEEE 24765:2017 – Systems and Software Engineering – Vocabulary*; Geneva, CH, 2017;

8. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27000:2018 – Information Technology – Security Techniques – Information Security Management Systems*; Geneva, CH, 2018;

9. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 29146:2016 – Information Technology – Security Techniques – a Framework for Access Management*; Geneva, CH, 2016;

10. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 2382:2015 – Information Technology – Vocabulary*; International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): Geneva, CH, 2015;

11. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC Guide 99 – International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM)*; International Organization for Standardization and International Electrotechnical Commission: Geneva, CH, 2007;

12. International Organization for Standardization (ISO) *ISO 5725-1:2023 – Accuracy (Trueness and Precision) of Measurement Methods and Results – Part 1: General Principles and Definitions*; Geneva, CH, 2023;

13. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25010:2023 – Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Product Quality Model*; Geneva, CH, 2023;

14. European Parliament and Council of the European Union Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. *Official Journal of the European Union* **2014**, *257*.

15. International Organization for Standardization (ISO) *ISO/TS 21089:2018 – Health Informatics – Trusted End-to-End Information Flows*; Geneva, CH, 2018;

16. International Organization for Standardization (ISO) *ISO 19731:2017 – Digital Analytics and Web Analyses for Purposes of Market, Opinion and Social Research — Vocabulary and Service Requirements*; Geneva, CH, 2017;

17. International Organization for Standardization (ISO) *ISO/TR 22100-4:2018 – Safety of Machinery – Relationship with ISO 12100 – Part 4: Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects*; Geneva, CH, 2018;

18. World Health Organisation (WHO) Expert Committee on Specifications for Pharmaceutical Preparations *WHO Technical Report Series 996 – Fiftieth Report*; World Health Organisation (WHO): Geneva, CH, 2016;

19. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 18033-1:2021 – Information Security — Encryption Algorithms – Part 1: General*; Geneva, CH, 2021;

20. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 22123-1:2023 – Information Technology – Cloud Computing – Part 1: Vocabulary*; Geneva, CH, 2023;

21. International Organization for Standardization (ISO) *ISO 14641:2018 – Electronic Document Management – Design and Operation of an Information System for the Preservation of Electronic Documents – Specifications*; Geneva, CH, 2018;

22. Organisation for Economic Co-operation and Development (OECD) *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring – Number 22 – Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity.*; Organisation for Economic Co-operation; Development (OECD), 2021;

23. Organisation for Economic Co-operation and Development (OECD) *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring – Number 15 – Advisory Document of the Working Group on Good Laboratory Practice Establishment and Control of Archives That Operate in Compliance with the Principles of GLP*; Organisation for Economic Co-operation; Development (OECD), 2007;

24. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 20243-1:2023 – Information Technology – Open Trusted Technology*

ProviderTM Standard (o-TTPS) – Part 1: Requirements and Recommendations for Mitigating Maliciously Tainted and Counterfeit Products; Geneva, CH, 2023;

25. International Organization for Standardization (ISO) *ISO 16484-2:2004 – Building Automation and Control Systems (BACS) — Part 2: Hardware*; Geneva, CH, 2004;

26. International Organization for Standardization (ISO) *ISO 18943:2014 – Imaging Materials – Magnetic Hard Drives Used for Image Storage – Care and Handling*; Geneva, CH, 2014;

27. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) *ISO/IEC/IEEE 15288:2023 – Systems and Software Engineering – System Life Cycle Processes*; Geneva, CH, 2023;

28. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) *ISO/IEC/IEEE 12207:2017 – Systems and Software Engineering – Software Life Cycle Processes*; Geneva, CH, 2017;

29. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 24745:2022 – Information Security, Cybersecurity and Privacy Protection – Biometric Information Protection*; Geneva, CH, 2022;

30. International Organization for Standardization (ISO) *ISO 22739:2024 – Blockchain and Distributed Ledger Technologies — Vocabulary*; Geneva, CH, 2024;

31. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25051:2014 – Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Requirements for Quality of Ready to Use Software Product (RUSP) and Instructions for Testing*; Geneva, CH, 2014;

32. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) *ISO/IEC/IEEE 90003:2018 – Software Engineering – Guidelines for the Application of ISO 9001:2015 to Computer Software*; Geneva, CH, 2018;

33. European Directorate for the Quality of Medicines & HealthCare (EDQM) *General European OMCL Network (GEON) – QUALITY MANAGEMENT DOCUMENT PA/PH/OMCL (08) 69 R7 – VALIDATION OF COMPUTERISED SYSTEMS CORE DOCUMENT*; Swiss Working Group on Information Technology in a GLP Environment: Brussels, BE, 2018;

34. International Organization for Standardization (ISO) *ISO 9000:2015 – Quality Management Systems Fundamentals and Vocabulary*; Geneva, CH, 2015;

35. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 25000:2014 – Systems and Software Engineering – Systems and Software Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE*; Geneva, CH, 2014;

36. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC TS 27100:2020 – Information Technology – Cybersecurity – Overview and Concepts*; Geneva, CH, 2020;

37. Joint Task Force Trransformation Initiative *Guide for Conducting Risk Assessments – Information Security*; National Institue of STandards; Technology (NIST), 2012;

38. Committee on National Security Systems (CNSS) *Committee on National Security Systems (CNSS) Glossary*; Committee on National Security Systems (CNSS), 2022;

39. International Organization for Standardization (ISO) *ISO 5127:2017 – Information and Documentation – Foundation and Vocabulary*; Geneva, CH, 2017;

40. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27040:2015 – Information Technology – Security Techniques – Storage Security*; Geneva, CH, 2015;

41. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 20926:2009 – Software and Systems Engineering – Software Measurement – IFPUG Functional Size Measurement Method*; Geneva, CH, 2009;

42. International Organization for Standardization (ISO) *ISO 11139:2018 – Sterilization of Health Care Products – Vocabulary of Terms Used in Sterilization and Related Equipment and Process Standards*; Geneva, CH, 2018;

43. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 11770-4:2017 – Information Technology — Security Techniques — Key Management – Part 4: Mechanisms Based on Weak Secrets*; Geneva, CH, 2017;

44. International Organization for Standardization (ISO) *ISO 2789:2022 – Information and Documentation – International Library Statistics*; Geneva, CH, 2022;

45. Organisation for Economic Co-operation and Development (OECD) *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring – Advisory Document on GLP & Cloud Computing Supplement 1 to Document Number 17 on Application of GLP Principles to Computerised Systems.*; Organisation for Economic Co-operation; Development (OECD), 2023;

46. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27039:2015 – Information Technology – Security Techniques – Selection, Deployment and Operations of Intrusion Detection and Prevention Systems (IDPS)*; Geneva, CH, 2015;

47. International Organization for Standardization (ISO) *ISO 30300:2020 – Information and Documentation – Records Management – Core Concepts and Vocabulary*; Geneva, CH, 2020;

48. International Organization for Standardization (ISO) *ISO 10209:2022 – Technical Product Documentation – Vocabulary – Terms Relating to Technical Drawings, Product Definition and Related Documentation*; Geneva, CH, 2022;

49. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 13066-1:2011 – Information Technology – Interoperability with Assistive Technology (AT) — Part 1: Requirements and Recommendations for Interoperability*; Geneva, CH, 2011;

50. Ron Ross and Victoria Pillitteri and Kelley Dempsey and Mark Riddle and Gary Guissanie *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Revision 2)*; National Institue of STandards; Technology (NIST), 2020;

51. International Organization for Standardization (ISO) *ISO/TR 18492:2005 – Long-Term Preservation of Electronic Document-Based Information*; Geneva, CH, 2005;

52. International Organization for Standardization (ISO) *Document Management — Minimum Requirements for the Storage of Documents*; Geneva, CH, 2021;

53. International Organization for Standardization (ISO) *ISO 12100:2010 – Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction*; Geneva, CH, 2010;

54. International Organization for Standardization (ISO) *ISO 8571-1:1988 – Information Processing Systems – Open Systems Interconnection – File Transfer, Access and Management*; Geneva, CH, 1988;

55. International Organization for Standardization (ISO) *ISO 12234-2:2001 – Electronic Still-Picture Imaging — Removable Memory — Part 2: TIFF/EP Image Data Format*; Geneva, CH, 2018;

56. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27033-1:2015 – Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts*; Geneva, CH, 2023;

57. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 19678:2015 – Information Technology – BIOS Protection Guidelines*; Geneva, CH, 2015;

58. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 10118-1:2016 – Information Technology – Security Techniques – Hash-Functions*; Geneva, CH, 2016;

59. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 24760-1:2019 – IT Security and Privacy – a Framework for Identity Management – Part 1: Terminology and Concepts*; Geneva, CH, 2019;

60. Swiss Working Group on Information Technology in a GLP Environment (AGIT) *Validation of Computerized Systems V3*; Swiss Working Group on Information Technology in a GLP Environment: Geneva, CH, 2018;

61. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 20924:2021 – Information Technology – Internet of Things (IoT) – Vocabulary*; Geneva, CH, 2021;

62. European Parliament and Council of the European Union Directive 2009/24/EC on the Legal Protection of Computer Programs. *Official Journal of the European Union* **2009**, *111*.

63. European Parliament and Council of the European Union Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases. *Official Journal of the European Union* **1996**, *015*.

64. European Parliament and Council of the European Union Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services. *Official Journal of the European Union* **2019**, *136*.

65. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 29115:2013 – Information Technology – Security Techniques – Entity Authentication Assurance Framework*; Geneva, CH, 2013;

66. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 18630:2023 – Information Technology – Digitally Recorded Media for*

Information Interchange and Storage – Quality Discrimination Method for Optical Disks and Operating Method of Storage Systems for Long-Term Data Preservation; Geneva, CH, 2023;

67. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) *ISO/IEC/IEEE 14764:2022 – Software Engineering – Software Life Cycle Processes — Maintenance*; Geneva, CH, 2019;

68. International Organization for Standardization (ISO) *ISO 19092:2023 – Financial Services – Biometrics –Security Framework*; Geneva, CH, 2023;

69. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27032:2023 – Cybersecurity – Guidelines for Internet Security*; Geneva, CH, 2023;

70. Project Management Institute *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*; 7th ed.; 2017;

71. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 9798-5:2009 – Information Technology – Security Techniques – Entity Authentication – Part 5: Mechanisms Using Zero-Knowledge Techniques*; Geneva, CH, 2009;

72. International Organization for Standardization (ISO) *ISO/TS 18759:2022 – Document Management – Trustworthy Storage System (TSS) – Functional and Technical Requirements*; Geneva, CH, 2022;

73. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) *ISO/IEC/IEEE 15289:2019 – Systems and Software Engineering – Content of Life-Cycle Information Items (Documentation)*; Geneva, CH, 2019;

74. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 21890:2001 – Information Technology — Telecommunications and Information Exchange Between Systems — Interoperation of PISNs with IP Networks*; Geneva, CH, 2001;

75. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 14143-1:2007 – Information Technology – Software Measurement – Functional Size Measurement*; Geneva, CH, 2007;

76. United States Pharmacopeia (USP) *USP <1058> Analytical Instrument Qualification*; United States Pharmacopeia (USP), 2017;

77. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27033-4:2014 – Information Technology – Security Techniques – Network Security – Part 4: Securing Communications Between Networks Using Security Gateways*; Geneva, CH, 2014;

78. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC TR 24772-1:2019 – Programming Languages — Guidance to Avoiding Vulnerabilities in Programming Languages — Part 1: Language-Independent Guidance*; Geneva, CH, 2019;

79. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 18036:2003 – Information Technology – Icon Symbols and Functions for*

World Wide Web Browser Toolbars; International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): Geneva, CH, 2003;

80. International Organization for Standardization (ISO) *ISO 31000:2018 – Risk Management – Guidelines*; Geneva, CH, 2018;

81. International Electrotechnical Commission (IEC) *IEC 31010:2019 – Risk Management — Risk Assessment Techniques*; 2019;

82. International Society for Pharmaceutical Engineering (ISPE) *GAMP 5 Second Edition – a Risk-Based Approach to Compliant GxP Computerized Systems*; International Society for Pharmaceutical Engineering (ISPE), 2022;

83. Catteddu, D.; Hogben, G. *Cloud computing – Benefits, risks and recommendations for information security*; European Union Agency for Cybersecurity (ENISA), 2009;

84. Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Naydenov, A.M.R.S.; Ciobanu, C. *ENISA Threat Landscape 2023*; European Union Agency for Cybersecurity (ENISA), 2023;

85. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 27102:2019 – Information Security Management – Guidelines for Cyber-Insurance*; Geneva, CH, 2019;

86. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC TS 25011 – Information Technology – Systems and Software Quality Requirements and Evaluation (SQuaRE) – Service Quality Models*; Geneva, CH, 2017;

87. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25012:2008 – Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Data Quality Model*; Geneva, CH, 2008;

88. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27036-1:2021 – Cybersecurity — Supplier Relationships – Part 1: Overview and Concepts*; Geneva, CH, 2021;

89. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC TR 7052:2023 – Software Engineering – Controlling Frequently Occurring Risks During Development and Maintenance of Custom Software*; International Organization for Standardization and International Electrotechnical Commission: Geneva, CH, 2023;

90. Open Web Application Security Project *OWASP Secure Coding Practices – Quick Reference Guide*; 2010;

91. Open Web Application Security Project (OWASP) OWASP Top Ten 2021.

92. Gerald, J. The Power of 10: Rules for Developing Safety-Critical Code. *Computer* **2006**, *39*, 95–97, doi:10.1109/mc.2006.212.

93. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25019:2023 – Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Quality-in-Use Model*; Geneva, CH, 2023;

94. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25022:2016 – Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Measurement of Quality in Use*; Geneva, CH, 2016;

95. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25023:2016 – Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Measurement of System and Software Product Quality*; Geneva, CH, 2016;

96. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 25023:2015 – Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Measurement of Data Quality*; Geneva, CH, 2016;

97. International Organization for Standardization (ISO) *ISO 7870-1:2019 – Control Charts – Part 1: General Guidelines*; Geneva, CH, 2019;

98. International Organization for Standardization (ISO) *ISO/IEC TS 23167:2020 – Information Technology — Cloud Computing — Common Technologies and Techniques*; Geneva, CH, 2020;

99. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC/IEEE 11770-1:2010 – Information Technology — Security Techniques — Key Management – Part 1: Framework*; Geneva, CH, 2010;

100. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 11770-2:2018 – Information Technology — Security Techniques — Key Management – Part 2: Mechanisms Using Symmetric Techniques*; Geneva, CH, 2018;

101. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 11770-3:2021 – Information Technology — Security Techniques — Key Management – Part 2: Mechanisms Using Asymmetric Techniques*; Geneva, CH, 2021;

102. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27005:20222 – Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks*; Geneva, CH, 2022;

103. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27033-2:2012 – Information Technology — Security Techniques — Network Security – Part 2: Guidelines for the Design and Implementation of Network Security*; Geneva, CH, 2012;

104. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) *ISO/IEC 27036-2:2022 – Cybersecurity — Supplier Relationships – Part 2: Requirements*; Geneva, CH, 2022;

105. International Organization for Standardization (ISO) *ISO 13008:2022 – Information and Documentation — Digital Records Conversion and Migration Process*; Geneva, CH, 2022;

106. International Organization for Standardization (ISO) *ISO/TR 17797:2014 – Electronic Archiving – Selection of Digital Storage Media for Long Term Preservation*; Geneva, CH, 2014;

107. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *ISO/IEC 14533-1:2017 – Processes, Data Elements and Documents in Commerce, Industry and Administration — Long Term Signature Profiles – Part 3: Long Term Signature Profiles for PDF Advanced Electronic Signatures (PAdES)*; Geneva, CH, 2017;

108. International Organization for Standardization (ISO) *ISO/TR 15801:2017 – Document Management – Electronically Stored Information – Recommendations for Trustworthiness and Reliability*; Geneva, CH, 2014;

109. International Organization for Standardization (ISO) *ISO 18829:2017 – Document Management – Assessing ECM/EDRM Implementations – Trustworthiness*; Geneva, CH, 2017;