Final draft ETSI EN 319 401 V3.2.1 (2025-11)

EUROPEAN STANDARD

Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Reference
REN/ESI-0019401v321

Keywords
cybersecurity, electronic signature, provider,
security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This final draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI), and is now submitted for the Vote phase of the ETSI EN Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of security, makes consumers, businesses and administrations hesitate to carry out transactions electronically and to adopt new services. Trust service providers are often an essential element to establish trust between parties transacting electronically, particularly in open public networks, and can be used, for example, to provide trusted identity information and help establish secure communications between transacting parties. Examples of such trust service providers are issuers of public key certificates, time-stamping service providers, providers of remote electronic signature generation or validation services.

For participants of electronic commerce to have confidence in the security of these trust services they need to have confidence that the Trust Service Providers (TSPs) have established a set of procedures, processes and security measures in order to minimize the operational and financial threats and risks associated.

Further, the cybersecurity of all essential digital services is vital for digital transformation of Europe with digital services and electronic transactions. The provision of eIDAS trust services is identified as an essential element of Europe's digital infrastructure. The Directive (EU) 2022/2555 [i.13] 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 2016/1148 (NIS2 Directive or NIS2) identifies in article 3 that requirements for cybersecurity risk management measures are applicable, as essential entities, to Qualified Trust Services Providers as per eIDAS Regulation. Furthermore, as eIDAS trust services are identified as fundamental element of Europe's digital infrastructure and NIS 2 is applicable to eIDAS trust services the present document also aims to meet the requirements of NIS2.

Furthermore, the present document has been updated to incorporate the requirements set forth in the Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 [i.27] laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant for trust service providers among other essential entities.

The present document specifies baseline policy requirements on the operation and management practices of TSP regardless the service they provide including cybersecurity requirements abiding NIS2 and its implementing regulations. Other standards, addressing particular type of trust service, can build on the present document to identify supplement requirements for particular type of trust service.

The present document is aiming to meet the general requirements to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.1].

EXAMPLE: ETSI EN 319 411-2 [i.7], annex A describes the application of the present document to the requirements of Regulation (EU) No 910/2014 [i.1] requirements for TSPs issuing EU qualified certificates.

1 Scope

The present document specifies general policy requirements relating to Trust Service Providers (TSPs) that are independent of the type of TSP. It defines policy requirements on the operation and management practices of TSPs.

Other specifications refine and extend these requirements as applicable to particular forms of TSP. The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

The present document aims to support the requirements on NIS2 Directive [i.13] and addresses the general requirements for security management and cybersecurity of trust services (qualified and non-qualified).

NOTE: See ETSI EN 319 403-1 [i.2] for details about requirements for conformity assessment bodies assessing Trust Service Providers.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 119 312 (V1.5.1): "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] 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.

[i.2] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.3] CA/Browser Forum: "Network and certificate system security requirements".

[i.4] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

[i.5] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.6] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

[i.7] ETSI EN 319 411-2: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.8] 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).

[i.9] ETSI TS 119 431-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev".

[i.10] ISO/IEC 27701:2019: "Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines".

[i.11] ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection - information security controls".

[i.12] ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection - Guidance on managing information security risks".

[i.13] 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).

[i.14] ETSI EN 319 421: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.15] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

[i.16] ETSI TS 119 461: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.17] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

[i.18] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.19] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.20] ISO Guide 73:2009: "Risk management - Vocabulary".

[i.21] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA).

[i.22] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[i.23] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.24] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[i.25] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[i.26] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.27] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

3 Definition of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the following terms apply:

access control: physical and logical access to assets that is authorized and/or restricted based on business and information security requirements

NOTE: Source: ISO/IEC 27002:2022 [i.11].

asset: anything that has value to the organization

NOTE: Source: ISO/IEC 27002:2022 [i.11].

attack: successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset

NOTE: Source: ISO/IEC 27002:2022 [i.11].

authentication: provision of assurance that a claimed characteristic of an entity is correct

NOTE: Source: ISO/IEC 27002:2022 [i.11].

authenticity: property that an entity is what it claims to be

NOTE: Source: ISO/IEC 27002:2022 [i.11].

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [i.4]

cybersecurity: activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

cyber threat: potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons

impact: harm that may be suffered when a threat compromises an information asset

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

NOTE: Source: NIS2 Directive [i.13].

incident handling: any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident

NOTE: Source: NIS2 Directive [i.13].

information security breach: compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information security event: occurrence indicating a possible information security breach or failure of security controls

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information security incident: one or multiple related and identified information security events that can harm an organization's assets or compromise its operations

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information security incident management: exercise of a consistent and effective approach to the handling of information security incidents

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information system: set of applications, services, information technology assets, or other information-handling components

NOTE: Source: ISO/IEC 27002:2022 [i.11].

large-scale cybersecurity incident: incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States

NOTE: Source: NIS2 Directive [i.13].

multi-factor authentication: authentication mechanism consisting of two or more of the independent categories of credentials (knowledge, possession and inherence factor) to verify the user's identity for a login or other transaction

near miss: event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialize

NOTE: Source: NIS2 Directive [i.13].

policy: intentions and direction of an organization, as formally expressed by its top management

NOTE: Source: ISO/IEC 27002:2022 [i.11].

procedure: specified way to carry out an activity or a process

NOTE: Source: ISO/IEC 27002:2022 [i.11].

process: set of interrelated or interacting activities that uses or transforms inputs to deliver a result

NOTE: Source: ISO/IEC 27002:2022 [i.11].

relying party: natural or legal person that relies upon an electronic identification or a trust service

NOTE: Relying parties include parties verifying a digital signature using a public key certificate.

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

risk analysis: process of estimating the likelihood that an event will create an impact and include as necessary components, the foreseeability of a threat, the expected effectiveness of Safeguards, and an evaluated result

risk assessment: overall process of risk identification, risk analysis and risk evaluation

NOTE: Source: ISO Guide 73:2009 [i.20].

risk management: process for analysing, mitigating, overseeing, and reducing risk

risk treatment: process to modify risk

NOTE: Source: ISO Guide 73:2009 [i.20].

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

trust service: electronic service which enhances trust and confidence in electronic transactions

NOTE: This definition is intended to cover trust services as defined in Regulation (EU) No 910/2014 [i.1], although its formulation allows for applicability beyond that specific regulatory framework.

trust service component: one part of the overall service of a TSP

EXAMPLE: Those identified in clause 4.4 of ETSI EN 319 411-1 [i.5]. Also, ETSI TS 119 431-1 [i.9] defines requirements for a Server Signing Application Service Component (SSASC) which can be implemented as part of TSP's service which also includes other service components.

NOTE: Other standards, including ETSI standards, can specify requirements for other service components which can form part of a wider TSP's service.

trust service policy: set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

NOTE: A trust service policy describes what is offered and provides information about the level of the service. It is defined independently of the specific details of the specific operating environment of a TSP; a trust service policy can apply to a community to which several TSPs belong that abide by the common set of rules specified in that policy. It can be defined for example by the TSP, by standards, by national (e.g. government) or international organizations, by the customers (subscribers) of the TSP and it is not necessarily part of the TSP's documentation.

trust service practice statement: statement of the practices that a TSP employs in providing a trust service

NOTE: See clause 6.2 for further information on practice statement.

Trust Service Provider (TSP): entity which provides one or more trust services

trust service token: physical or binary (logical) object generated or issued as a result of the use of a trust service

NOTE: Examples of trust service tokens are: certificates, CRLs, time-stamp tokens, OCSP responses.

vulnerability: weakness of an asset or control that can be exploited by one or more threats

NOTE: Source: ISO/IEC 27002:2022 [i.11].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA Certification Authority
CER Critical Entities Resilience

NOTE: See Directive (EU) 2022/2557 [i.22].

CRA Cyber Resilience Act

NOTE: See Regulation (EU) 2024/2847 [i.23].

CSIRT Computer Security Incident Response Team

DGA Data Governance Act

NOTE: See Regulation (EU) 2022/868 [i.25].

DORA Digital Operational Resilience Act

NOTE: See Regulation (EU) 2022/2554 [i.21].

DSA Digital Services Act

NOTE: See Regulation (EU) 2022/2065 [i.24].

eIDAS electronic IDentification, Authentication and trust Services

NOTE: Informal name for Regulation (EU) No 910/2014 [i.1] amended by Regulation (EU) 2024/1183 [i.26].

ICT Information & Communication Technology
IP Internet Protocol
IT Information Technology
SLA Service-Level Agreement
SSASC Server Signing Application Service Component
TSP Trust Service Provider
UTC Coordinated Universal Time

3.4 Notation

The requirements identified in the present document include:

a) requirements applicable to any TSP. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) Requirements where the TSP's implementation may be determined based on proportionality criteria as described in clause 4.1. Such requirements are indicated by "[PRO]".

Each requirement is identified as follows:

<3 letters identifier> - < the clause number> - <2 digit number - incremental>.

The service components are:

- **REQ:** General requirement applicable to any TSP.
- **PRO:** Requirements where the TSP's implementation may be determined based on proportionality criteria as described in clause 4.1.

4 Overview

4.1 General

Trust services can encompass but is not limited to the issuance of public key certificates, provision of registration services, time-stamping services, long term preservation services, e-delivery services and/or signature validation services.

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

The requirements specified in the present document are mandatory for TSPs and shall be implemented as indicated, subject to the proportionality criteria established in clause 4.2.

When implementing controls of clause 7, guidance given in ISO/IEC 27002:2022 [i.11] should be applied as appropriate.

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in providing services.

4.2 Applicability of Conditional Requirements

REQ-4.2.01: When implementing the requirements in the present document, the TSP shall take due account of:

- the degree of its exposure to risks;
- the TSP's size;
- the likelihood of occurrence of incidents; and
- the incident's severity, including their societal and economic impact.

REQ-4.2.02: Requirements indicated by "[PRO]" shall be implemented based on proportionality criteria. In addition:

EXAMPLE: Examples of how proportionality criteria can be applied include:

- a micro-sized TSP with limited resources can implement compensating controls where full segregation of duties is not feasible, such as enhanced management oversight or increased monitoring and logging;
- a TSP operating in a single Member State with a limited number of users can implement less complex redundancy arrangements than a TSP operating across multiple Member States; or
- a TSP providing services with lower criticality can apply less frequent security testing intervals than those providing highly critical services.

REQ-4.2.03: The TSP shall document the analysis of applicability of such requirements as part of their risk management framework.

REQ-4.2.04: This analysis and its outcomes shall be maintained as part of the risk assessment documentation and be available for review by relevant authorities.

REQ-4.2.05: PRO requirements shall not be dismissed without proper justification regardless of the TSP's size or scope of operations.

REQ-4.2.06: The TSP shall ensure that the cumulative effect of any non-applied PRO requirements does not compromise the overall security posture of their services or undermine the objectives of the present document.

5 Risk Management Framework and Risk Assessment

REQ-5-01: The TSP shall:

a) perform and document risk assessments to identify, analyse and evaluate trust service risks taking into account business and technical issues;

b) establish, implement and document a risk treatment plan based on the risk assessment results;

c) establish procedures for identification, analysis, assessment and treatment of risks ('cybersecurity risk management process'). The cybersecurity risk management process shall be an integral part of the TSP's overall risk management process, where applicable;

d) establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures taken by the TSP are effectively implemented and maintained;

e) establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems; and

f) review and, where appropriate, update the policy and procedures at planned intervals, at least annually, and when significant incidents or significant changes to operations or risks occur.

REQ-5-02: The TSP shall, based on the risk assessment results, establish, implement and monitor a risk treatment plan. The risk treatment plan shall ensure that the level of security is commensurate to the degree of risk.

NOTE: See ISO/IEC 27005:2022 [i.12] for guidance on information security risk management as part of an information security management system.

REQ-5 -03: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).

REQ-5-04: The TSP shall review and, where appropriate, update the risk assessment results and the risk treatment plan at planned intervals and at least annually, and when significant changes to operations or risks or significant incidents occur.

REQ-5-05: The TSP's management bodies or, where applicable, the persons who are accountable and have the authority to manage risks shall:

a) approve the risk assessment framework, including risk assessment plan and the cybersecurity risk management process; and

b) accept the residual risk identified.

REQ-5-06: When identifying and prioritising appropriate risk treatment options and measures, the TSP shall take into account:

a) the risk assessment results;

b) the results of the procedure to assess the effectiveness of cybersecurity risk-management measures;

c) the cost of implementation in relation to the expected benefit;

d) the asset classification referred to in clause 7.3.2; and

e) the business impact analysis referred to in the business continuity plan.

REQ-5-07: As part of the cybersecurity risk management process, the TSP shall:

a) follow a risk management methodology;

b) establish the risk tolerance level in accordance with the risk appetite of the TSP;

NOTE: For the purposes of this requirement:

- 'Risk appetite' refers to the amount and type of risk that a TSP is willing to accept in pursuit of its business objectives, typically expressed as a high-level statement approved by management bodies.
- 'Risk tolerance level' refers to the specific maximum risk that the TSP is willing to bear for particular risk categories or business processes, typically expressed through quantifiable metrics or thresholds.

EXAMPLE: A TSP's risk appetite statement might indicate 'low appetite for risks affecting trust service availability', whilst the corresponding risk tolerance level might specify 'maximum acceptable downtime of 20 minutes per month for qualified certificate issuance services'.

c) establish and maintain relevant risk criteria;

d) in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;

e) analyse the risks posed to the security of network and information systems, including threat, likelihood, impact, and risk level, taking into account cyber threat intelligence and vulnerabilities;

f) evaluate the identified risks based on the risk criteria;

g) identify and prioritise appropriate risk treatment options and measures;

h) continuously monitor the implementation of the risk treatment measures;

i) identify who is responsible for implementing the risk treatment measures and when they should be implemented;

j) document the chosen risk treatment measures in a risk treatment plan and the reasons justifying the acceptance of residual risks in a comprehensible manner.

REQ-5.08: The policy and procedures referred to in REQ-5.1, c) shall take into account results of the risk assessment pursuant to clause 5 and past significant incidents. The TSP shall determine:

a) what cybersecurity risk-management measures are to be monitored and measured, including processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when the monitoring and measuring is to be performed;

d) who is responsible for monitoring and measuring the effectiveness of the cybersecurity risk-management measures;

e) when the results from monitoring and measurement are to be analysed and evaluated;

f) who has to analyse and evaluate these results.

6 Policies and practices

6.1 Trust Service Practice statement

REQ-6.1-01: The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.

REQ-6.1-02: The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.

In particular:

- **REQ-6.1-03:** The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP.

NOTE 1: The present document makes no requirement as to the structure of the trust service practice statement.

- **REQ-6.1-04:** The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.

- **REQ-6.1-05:** The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy.

NOTE 2: The TSP need not disclose any aspects containing sensitive information in the documentation that is made available to subscribers and relying parties.

- **REQ-6.1-06:** The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.

- **REQ-6.1-07:** The TSP's management shall implement the practices.

- **REQ-6.1-08:** The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement.
- **REQ-6.1-09 [CONDITIONAL]:** When the TSP intends to make changes in its practice statement that might affect the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties.

NOTE 3: The due notice does not need to provide the details of the changes. The due notice can be published on the TSP's repository.

- **REQ-6.1-10:** The TSP shall, following approval as in **REQ-6.1-06** above, make the revised TSP's practice statement immediately available as required under **REQ-6.1-05** above.
- **REQ-6.1-11:** The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).

6.2 Terms and Conditions

REQ-6.2-01: TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.

REQ-6.2-02: The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:

a) the trust service policy being applied;

b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;

EXAMPLE 1: The expected life-time of public key certificates.

c) the subscriber's obligations, if any;

d) information for parties relying on the trust service;

EXAMPLE 2: How to verify the trust service token, any possible limitations on the validity period associated with the trust service token.

e) the period of time during which TSP's event logs are retained;

f) limitations of liability;

g) the applicable legal system;

h) procedures for complaints and dispute settlement;

i) whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;

j) the TSP's contact information; and

k) any undertaking regarding availability.

REQ-6.2-03: Subscribers and parties relying on the trust service shall be informed in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

REQ-6.2-04: Terms and conditions shall be made available through a durable means of communication.

REQ-6.2-05: Terms and conditions shall be available in a readily understandable language.

REQ-6.2-06: Terms and conditions may be transmitted electronically.

6.3 Information and Network Security Policy

REQ-6.3-01: The TSP shall define a policy on the security of network and information systems which is approved by management and which sets out the TSP's approach to managing the security of its network and information systems, that:

a) are appropriate to and complementary with the TSP's business strategy and objectives;

b) sets out network and information security objectives;

c) includes a commitment to continual improvement of the security of network and information systems;

d) includes a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;

e) are communicated to and acknowledged by relevant employees and relevant interested external parties;

f) lays down roles and responsibilities pursuant to clause 7.1;

g) lists the documentation to be kept and the duration of retention of the documentation;

h) lists the topic-specific policies;

i) lays down indicators and measures to monitor its implementation and the current status of the TSP's maturity level of network and information security; and

j) indicates the date of the formal approval by the management bodies of the TSP.

REQ-6.3-02: Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

In particular:

- **REQ-6.3-03:** A TSP's policy on the security of network and information systems shall be:

  a) documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.

  b) reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.

- **REQ-6.3-04:** The TSP shall establish procedures to notify of important changes in the provision of the trust service to the supervisory body, including changes in the provision of trust services and the intention to cease on its provision,. in accordance with business requirements and relevant laws and regulations. The TSP shall notify the supervisory body at least:

  a) one month before implementing any change;

  b) three months before the planned cessation of a trust service provision.

NOTE 1: Trust service providers qualified according to Regulation (EU) 2014/910 [i.1] are required to inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.

- **REQ-6.3-05:** The TSP shall publish and communicate the information security policy to all employees who are impacted by it.

NOTE 2: See clause 5.1 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-6.3-06:** The TSP's policy on the security of network and information systems and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals, at least annually, or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

- **REQ-6.3-07:** Any changes that will impact on the level of security provided shall be approved by the management body referred to in **REQ-6.1-07**.

- **REQ-6.3-08:** The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.
- **REQ-6.3-09:** The maximum interval between two checks shall be documented in the trust service practice statement.

NOTE 3: Further recommendations are given in the CA/Browser Forum network security guide [i.3], item 1.

7 TSP management and operation

7.1 Internal organization

7.1.1 General

REQ-7.1.1-01: The TSP shall lay down responsibilities and authorities for network and information system security and assign them to roles, allocate them according to the TSP's needs, and communicate them to the management bodies.

REQ-7.1.1-02: The TSP shall require all personnel and third parties to apply network and information system security in accordance with the established policy on the security of network and information systems, topic-specific policies and procedures of the TSP.

REQ-7.1.1-03: At least one person shall report directly to the management bodies on matters of network and information system security.

PRO-7.1.1-04: Depending on the size of the TSP, network and information system security shall be covered by dedicated roles or duties carried out in addition to existing roles. This shall be documented in the risk management plan.

REQ-7.1.1-05: The TSP shall review roles, responsibilities and authorities at planned intervals and when significant incidents or changes to operations or risks occur.

7.1.2 Organization reliability

REQ-7.1.2-01: The TSP organization shall be reliable.

In particular:

- **REQ-7.1.2-02:** Trust service practices under which the TSP operates shall be non-discriminatory.
- **REQ-7.1.2-03:** The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.
- **REQ-7.1.2-04:** The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

NOTE: For liability of TSPs operating in EU, see article 13 of the Regulation (EU) No 910/2014 [i.1].

- **REQ-7.1.2-05:** The TSP shall have the financial stability and resources required to operate in conformity with this policy.
- **REQ-7.1.2-06:** The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

7.1.3 Segregation of duties

REQ-7.1.3-01: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.

NOTE: See clause 5.3 of ISO/IEC 27002:2022 [i.11] for guidance.

7.2 Human resources

REQ-7.2-01: The TSP shall ensure that their employees and direct suppliers and service providers understand and commit to their security responsibilities, as appropriate for the offered services and the job and in line with the TSP's policy on the security of network and information systems. The TSP shall, therefore:

a) implement mechanism to ensure that:

- all employees, direct suppliers and service providers, wherever applicable, understand and follow the Information and Network Security Policy and processes that the TSP applies;
- all users with administrative or privileged access are aware of and act in accordance with their roles, responsibilities and authorities;
- members of management bodies understand and act in accordance with their role, responsibilities and authorities regarding network and information system security;
- personnel qualified for the respective roles are hired.

EXAMPLE: Using tools such as reference checks, vetting procedures, validation of certifications, or written tests.

b) review the assignment of personnel to specific roles, as well as their commitment of human resources in that regard, at planned intervals and at least annually. They shall update the assignment where necessary.

NOTE 1: See clause 5.4 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.2-02:** The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding cybersecurity and personal data protection rules as appropriate for the offered services and the job function.
- **REQ-7.2-03:** The TSP shall identify at least one person responsible for network and information security and reporting to top management.
- **REQ-7.2-04:** TSP's personnel in trusted roles, and, if applicable, its subcontractors in trusted roles, shall be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.
- **REQ-7.2-05:** TSP's personnel in trusted roles shall receive regular updates on new threats and current security practices at least every 12 months.

NOTE 2: Personnel employed by a TSP include individual personnel contractually engaged in performing functions in support of the TSP's services. Personnel who can be involved in monitoring the TSP's services need not be TSP's personnel.

- **REQ-7.2-06:** Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures in accordance with an established communicated and maintained disciplinary process for handling violations of network and information system security policies. This process shall:

  a) take into consideration relevant legal, statutory, contractual and business requirements.

  b) be reviewed and, where appropriate, updated at planned intervals, at least annually, and when necessary due to legal changes or significant changes to operations or risks.

NOTE 3: See clause 6.4 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.2-07:** Information security roles and responsibilities, as specified in the TSP's policy on the security of network and information systems, shall be documented in job descriptions or in documents available to all concerned personnel and allocated accordingly.
- **REQ-7.2-08:** Trusted roles, on which the TSP's operation is dependent, shall be clearly identified.

NOTE 4: See clause 5.2 of ISO/IEC 27002:2022 [i.11] for guidance.

NOTE 5: See clause 5.4 of ISO/IEC 27002:2022 [i.11] for further guidance on management responsibilities.

- **REQ-7.2-09:** TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

NOTE 6: See clause 6.1 of ISO/IEC 27002:2022 [i.11] for further guidance on screening, and clause 6.2 for further guidance on terms and conditions on employment.

- **PRO-7.2-10:** Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.

- **REQ-7.2-11:** Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

- **REQ-7.2-12:** Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

- **REQ-7.2-13:** All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.

- **REQ-7.2-14:** Trusted roles shall include roles that involve the following responsibilities:

  a) Security Officers: Overall responsibility for administering the implementation of the security practices.

  b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.

NOTE 7: This includes recovery of the system.

  c) System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.

  d) System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.

NOTE 8: Additional application specific roles can be required for particular trust services.

- **REQ-7.2-15:** TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.

- **REQ-7.2-16:** Trusted roles shall be accepted by the appointed person to fulfil the role.

- **REQ-7.2-17:** Personnel shall not have access to the trusted functions until the necessary checks are completed.

NOTE 9: In some countries it is not possible for TSP to obtain information on past convictions without the collaboration of the candidate employee.

NOTE 10: See clause 6.1 of ISO/IEC 27002:2022 [i.11] for further guidance on screening.

- **REQ-7.2-18 [CONDITIONAL]:** When personnel are working remotely, TSP shall implement cybersecurity measures to protect information accessed, processed or stored outside the TSP's premises.

In particular:

- **REQ-7.2-19 [CONDITIONAL]:** TSPs allowing remote working activities shall issue a topic-specific policy on remote working that defines the relevant cybersecurity conditions and restrictions.

NOTE 11: See clause 6.7 of ISO/IEC 27002:2022 [i.11] for further guidance on remote working.

REQ-7.2-20: The TSP shall ensure to the extent feasible verification of the background of their employees, and where applicable of direct suppliers and service providers, if necessary for their role, responsibilities and authorisations.

REQ-7.2-21: For the purpose of background verification, the TSP shall:

a) put in place criteria, which set out which roles, responsibilities and authorities shall only be exercised by persons whose background has been verified;

b) ensure that verification is performed on these persons before they start exercising these roles, responsibilities and authorities, which shall take into consideration the applicable laws, regulations, and ethics in proportion to the business requirements, the asset classification and the network and information systems to be accessed, and the perceived risks.

REQ-7.2-22: The TSP shall review and, where appropriate, update the background verification policy at planned intervals, at least every two years, and update it where necessary.

REQ-7.2-23: The TSP shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are contractually defined and enforced.

REQ-7.2-24: For the purpose of REQ-7.2-23, the TSP shall include in the individual's terms and conditions of employment, contract or agreement the responsibilities and duties that are still valid after termination of employment or contract, such as confidentiality clauses.

7.3 Asset management

7.3.1 General requirements

REQ-7.3.1-01: The TSP shall ensure an appropriate level of protection of its assets including information assets.

REQ-7.3.1-02: The assets provided through a supply chain shall be protected as specified in clause 7.14.

NOTE: Asset Management is a requirement which is incorporated in all ETSI EN 319 411-1 [i.5] (clause 6.4.1), ETSI EN 319 421 [i.14] (clause 7.4), ETSI TS 119 431-1 [i.9] (clause 6.4.1), ETSI TS 119 441 [i.15] (clause 7.3), ETSI TS 119 461 [i.16] (clause 7.3), ETSI TS 119 511 [i.17] (clause 7.3), ETSI EN 319 521 [i.18] (clause 7.3.1), ETSI EN 319 531 [i.19] (clause 7.3.1).

7.3.2 Assets classification

REQ-7.3.2.01: The TSP shall maintain an accurate inventory of assets as a prerequisite for effective technical vulnerability management.

REQ-7.3.2-02: For asset classification, the TSP shall:

a) lay down a system of classification levels for assets;

b) associate all assets with a classification level, based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value.

REQ-7.3.2-03: The TSP shall assign a classification level to each asset, or group of assets, based on requirements for protecting confidentiality, integrity, authenticity and availability, and in accordance with its risk assessment and business value.

REQ-7.3.2-04: The TSP shall assure that the availability requirements of each asset, or group of assets, classified are aligned with the delivery and recovery objectives as described in the business and disaster recovery plan.

REQ-7.3. 2-05: The TSP shall conduct periodic reviews of the classification levels of the assets and update them, where appropriate.

NOTE 1: See clauses 5.9 and 8.8 of ISO/IEC 27002:2022 [i.11] for guidance.

REQ-7.3.2-06: The TSP shall identify, document and implement rules for the acceptable use of and procedures for handling information and other associated assets.

NOTE 2: See clause 5.10 of ISO/IEC 27002:2022 [i.11] for guidance.

REQ-7.3.2-07: The TSP shall implement and document procedures in case of change or termination process of, internal and external personnel, contractors or other third parties in order to include the return of all previously issued physical and electronic assets owned by or entrusted to the TSP.

NOTE 3: See clause 5.11 of ISO/IEC 27002:2022 [i.11] for guidance.

7.3.3 Storage media and asset handling

REQ-7.3.3-01: The TSP shall establish, implement and apply a policy for the proper handling of assets, including information and storage media management, in accordance with their policy on the security of network and information systems, and shall communicate this policy to anyone who uses or handles assets. The policy shall:

a) cover the entire life cycle of the assets, including acquisition, use, storage, transportation and disposal;

b) cover the removable information and storage media, and its handling by third parties at the TSP's premises or other locations where the removable media is connected to the TSP's network and information systems;

c) provide rules on the safe use, safe storage, safe transport, and the irretrievable deletion and destruction of the assets; and

d) provide that the transfer shall take place in a secure manner, in accordance with the type of asset to be transferred.

REQ-7.3.3-02: Storage media used within the TSP's systems shall be securely handled to protect storage media from damage, theft, unauthorized access and obsolescence.

REQ-7.3.3-03: The TSP shall maintain a storage media management procedure that complies with REQ-7.3.3-02 for the duration of the required records retention period.

NOTE: See clause 7.10 of ISO/IEC 27002:2022 [i.11] for guidance.

REQ-7.3.3-04: The TSP shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

REQ-7.3.3-05: The TSP shall establish, implement and apply a specific policy on removable media that shall:

a) provide for a technical prohibition of the connection of removable media unless there is an organisational reason for their use;

b) provide for disabling self-execution from such media and scanning the media for malicious code before they are used on the TSP's systems;

c) provide measures for controlling and protecting portable storage devices containing data while in transit and in storage;

d) where appropriate, provide measures for the use of cryptographic techniques to protect data on removable storage media.

7.4 Access control

7.4.1 General

REQ-7.4.1-01: The TSP shall establish, document and implement logical and physical access control policies for the access to their network and information systems, based on business requirements as well as network and information system security requirements. The access control policies shall:

a) address access by persons, including staff, visitors, and external entities such as suppliers and service providers;

b) address access by network and information systems;

c) ensure that access is only granted to users that have been adequately authenticated.

REQ-7.4.1-02: The TSP shall administer user access of operators, administrators and other privileged accounts and system auditors applying the principle of "least privileges" when configuring access privileges. In particular:

REQ-7.4.1-03: The TSP shall provide setting up specific accounts to be used for administrative purposes like installation, configuration, management or maintenance.

REQ-7.4.1-04: Privileged accounts shall be used only if the privileges are necessary for the specific activity.

REQ-7.4.1-05: Strong identification, authentication and authorisation procedures shall be used for privileged accounts.

NOTE 1: This generally applies to personnel appointed to trusted roles as per **REQ-7.2-14.**

REQ-7.4.1-06 [CONDITIONAL]: Where appropriate, the TSP shall ensure that users and devices are authenticated by multi-factor or continuous authentication mechanisms, such as secure voice, video and text, before accessing the TSP's network and ITS information systems, depending on the classification of the systems to be accessed.

NOTE 2: See clauses 8.5 of ISO/IEC 27002:2022 [i.11] for guidance.

REQ-7.4.1-07: The TSP shall provide, modify, remove and document access rights to network and information systems in accordance with the access control policy. In addition:

a) The TSP shall review access rights to privileged and administrator accounts at planned intervals, and access rights shall be modified based on organisational changes.

b) The result of the review, including the necessary changes of access rights, shall be documented.

REQ-7.4-1-08: The TSP shall:

a) assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;

b) ensure that access rights are modified accordingly upon termination or change of employment;

c) ensure that access to network and information systems is authorised by the relevant persons;

d) ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in particular by limiting access rights in scope and in duration;

e) maintain a register of access rights granted; and

f) apply logging to the management of access rights.

REQ-7.4-1-09: Access to information and application system functions shall be restricted in accordance with the access control policy.

REQ-7.4.1-10: The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

REQ-7.4-1-11: TSP's personnel shall be identified and authenticated before using critical applications related to the service.

REQ-7.4-1-12: TSP's personnel shall be accountable for their activities.

EXAMPLE: By retaining event logs.

REQ-7.4-1-13: Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or storage media (see clause 7.3.2) being accessible to unauthorized users.

NOTE 3: See clauses 5.15, 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5 and 8.18 of ISO/IEC 27002:2022 [i.11] for guidance.

NOTE 4: Further recommendations regarding authentication are given in the CA/Browser Forum network security guide [i.3], clause 2.

REQ-7.4.1-14: The TSP shall review and, where appropriate, update the access control policies at planned intervals and when significant incidents or significant changes to operations or risks occur.

7.4.2 Privileged and system administration accounts

REQ-7.4.2-01: The TSP shall maintain policies for management of privileged accounts and system administration accounts as part of the access control policy.

REQ-7.4.2-02: The policies for privileged accounts and system administration accounts shall:

a) establish strong identification, authentication such as multi-factor authentication, and authorisation procedures for privileged accounts and system administration accounts;

b) set up specific accounts to be used for system administration operations exclusively, such as installation, configuration, management or maintenance;

c) individualise and restrict system administration privileges to the highest extent possible;

d) provide that system administration accounts are only used to connect to system administration systems.

REQ-7.4.2-03: The TSP shall review and document access rights of privileged and system administration accounts at planned intervals, including the necessary changes of access rights.

7.4.3 Administration systems

REQ-7.4.3-01: The TSP shall restrict and control the use of administration systems.

REQ-7.4.3-02: For system administration systems, the TSP shall:

a) only use system administration systems for system administration purposes, and not for any other operations;

b) separate logically such systems from application software not used for system administrative purposes; and

c) protect access to system administration systems through authentication and encryption.

7.4.4 Identification

REQ-7.4.4-01: The TSP shall manage the full life cycle of identities of network and information systems and their users.

REQ-7.4.4-02: For identity management, the TSP shall:

a) set up unique identities for network and information systems and their users;

b) link the identity of users to a single person;

c) ensure oversight of identities of network and information systems; and

d) apply logging to the management of identities.

REQ-7.4.4-03: The TSP shall only permit identities assigned to multiple persons, such as shared identities, where they are necessary for business or operational reasons and are subject to an explicit approval process and documentation.

REQ-7.4.4-04: The TSP shall take identities assigned to multiple persons into account in the cybersecurity risk management framework.

REQ-7.4.4-05: The TSP shall regularly review the identities for network and information systems and their users and, if no longer needed, deactivate them without delay.

7.4.5 Authentication

REQ-7.4.5-01: The TSP shall implement secure authentication procedures and technologies based on access restrictions and the policy on access control.

REQ-7.4.5-02: For authentication, the TSP shall:

a) ensure the strength of authentication is appropriate to the classification of the asset to be accessed;

b) control the allocation to users and management of secret authentication information by a process that ensures the confidentiality of the information, including advising personnel on appropriate handling of authentication information;

c) require the change of authentication credentials initially, at predefined intervals and upon suspicion that the credentials were compromised;

d) require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts;

e) terminate inactive sessions after a predefined period of inactivity; and

f) require separate credentials to access privileged access or administrative accounts.

REQ-7.4.5-03: The TSP shall to the extent feasible use state-of-the-art authentication methods, in accordance with the associated assessed risk and the classification of the asset to be accessed, and unique authentication information.

REQ-7.4.5-04: The TSP shall review the authentication procedures and technologies at planned intervals.

7.4.6 Multi-factor authentication

REQ-7.4.6-01: The TSP shall ensure that users are authenticated as specified in REQ-7.4.1-06 and REQ-7.4.5-02, a).

7.5 Cryptographic controls

REQ-7.5-01: Appropriate security controls shall be in place for the management of any cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle.

NOTE 1: See clause 8.24 of ISO/IEC 27002:2022 [i.11] for guidance.

REQ-7.5-02: The TSP shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data in line with the TSP's asset classification and the results of the risk assessment.

REQ-7.5-03: The policy and procedures for cryptography shall establish:

a) in accordance with the TSP's classification of assets, the type, strength and quality of the cryptographic measures required to protect the TSP's assets, including data at rest and data in transit;

b) based on point a), the protocols or families of protocols to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices to be approved and required for use by the TSP, following, where appropriate, a cryptographic agility approach; and

c) the TSP's approach to key management, including, where appropriate, methods for the following:

   i) generating different keys for cryptographic systems and applications;

   ii) issuing and obtaining public key certificates;

   iii) distributing keys to intended entities, including how to activate keys when received;

   iv) storing keys, including how authorised users obtain access to keys;

   v) changing or updating keys, including rules on when and how to change keys;

   vi) dealing with compromised keys;

   vii) revoking keys including how to withdraw or deactivate keys;

   viii) recovering lost or corrupted keys;

   ix) backing up or archiving keys;

   x) destroying keys;

xi) logging and auditing of key management-related activities; and

xii) setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the organization's rules on key management.

NOTE 2: For TSPs issuing certificates in accordance with ETSI EN 319 411-1 [i.5] or ETSI EN 319 411-2 [i.7], the key management requirements specified in those standards fulfil this requirement.

REQ-7.5-04: The TSP shall review and, where appropriate, update their cryptography policy and procedures at planned intervals, taking into account the state of the art in cryptography.

REQ-7.5-05: For the purpose of the provision of its trust services, the TSP should select and use suitable cryptographic techniques in accordance with recognized standards such as ETSI TS 119 312 [1]

7.6 Physical and environmental security

REQ-7.6-01: The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services, prevent or reduce the consequences of events originating from physical and environmental threats, and minimize risks related to physical security.

NOTE 1: See clauses 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 and 8.1 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.6-02:** Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals.

NOTE 2: Criticality is identified through risk assessment, or through application security requirements, as requiring a security protection.

- **REQ-7.6-03:** Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.

- **REQ-7.6-04:** Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

- **REQ-7.6-05:** Components that are critical for the secure operation of the trust service shall be located in a physically protected security perimeter, and access control against intrusion and alarms to detect intrusion.

- **REQ-7.6-06:** The TSP shall prevent loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities.

- **PRO-7.6-07 [CONDITIONAL]:** For the protection of supporting utilities, the TSP shall, where appropriate:

  a) protect facilities from power failures and other disruptions caused by failures in supporting utilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning;

  b) consider the use of redundancy in utilities services;

  c) protect utility services for electricity and telecommunications, which transport data or supply network and information systems, against interception and damage;

  d) monitor the utility services referred to in point c) and report to the competent internal or external personnel events outside the minimum and maximum control thresholds affecting the utility services;

  e) conclude contracts for the emergency supply with corresponding services, such as for the fuel for emergency power supply;

  f) ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.

- **REQ-7.6-08:** The TSP shall test, review and, where appropriate, update the protection measures for supporting utilities on a regular basis or following significant incidents or significant changes to operations or risks.

- **REQ-7.6-09:** The TSP shall prevent or reduce the consequences of events originating from physical and environmental threats, such as natural disasters and other intentional or unintentional threats, based on the results of the risk assessment.
- **PRO-7.6-10 [CONDITIONAL]:** For protection against physical and environmental threats, the TSP shall, where appropriate:

  a) design and implement protection measures against physical and environmental threats;

  b) determine minimum and maximum control thresholds for physical and environmental threats;

  c) monitor environmental parameters and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point b).
- **REQ-7.6-11:** The TSP shall test, review and, where appropriate, update the protection measures against physical and environmental threats on a regular basis or following significant incidents or significant changes to operations or risks.
- **REQ-7.6-12:** The TSP shall, on the basis of the risk assessment, lay down and use security perimeters to protect areas where network and information systems and other associated assets are located.
- **REQ-7.6-13:** The TSP shall continuously monitor their premises for unauthorised physical access.
- **REQ-7.6-14:** The TSP shall test, review and, where appropriate, update the physical access control measures on a regular basis or following significant incidents or significant changes to operations or risks.

7.7 Operation security

REQ-7.7-01: The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

In particular:

- **REQ-7.7-02:** An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.
- **REQ-7.7-03:** Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.
- **REQ-7.7-04:** The procedures shall include documentation of the changes.

NOTE 1: See clauses 5.37, 8.6, 8.31 and 8.32 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.7-05:** The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

NOTE 2: See clause 8.7 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.7-06:** Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.
- **REQ-7.7-07:** The TSP shall specify and apply procedures for ensuring that:

  a) security patches are applied within a reasonable time after they come available;

  b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and

  c) the reasons for not applying any security patches are documented.

REQ-7.7-08: The TSP shall establish, document, implement, monitor, and review configurations, including security configurations, of hardware, software, services and networks.

REQ-7.7-09: The TSP shall monitor configurations with a comprehensive set of system management tools.

EXAMPLE: Examples of system management tools are: maintenance utilities, remote support, enterprise management tools, backup and restore software, or change detection mechanisms, such as file integrity monitoring solutions

REQ-7.7.10: The TSP shall review configurations on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed.

NOTE 3: See clause 8.9 of ISO/IEC 27002:2022 [i.11] for guidance.

NOTE 4: Further recommendations are given in the CA/Browser Forum network security guide [i.3], item 1.

REQ-7.7-11: The TSP shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components that are critical for the TSP's security of network and information systems, based on the risk assessment.

REQ-7.7-12: The processes for acquisition of ICT services or ICT products shall include:

a) security requirements to apply to the ICT services or ICT products to be acquired;

b) requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products, or replacement after the end of the support period;

c) information describing the hardware and software components used in the ICT services or ICT products;

d) information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation;

e) assurance that the ICT services or ICT products comply with the security requirements;

f) methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.

REQ-7.7-13: The TSP shall review and, where appropriate, update the processes at planned intervals, at least annually, and when significant incidents occur.

REQ-7.7-14: Before developing a network and information system, including software, the TSP shall lay down rules for the secure development of network and information systems and apply them when developing network and information systems in-house, or when outsourcing the development of network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.

REQ-7.7-15: For secure development, the TSP shall:

a) carry out an analysis of security requirements at the specification and design phases of any development or acquisition project undertaken by the TSP or on behalf of those entities;

b) apply principles for engineering secure systems and secure coding principles to any information system development activities such as promoting cybersecurity-by-design, zero-trust architectures;

c) lay down security requirements regarding development environments;

d) establish and implement security testing processes in the development life cycle;

e) appropriately select, protect and manage security test data;

f) sanitise and anonymise testing data according to the risk assessment.

REQ-7.7-16: For outsourced development of network and information systems, the TSP shall also apply the policies and procedures referred to in relation to suppliers and ICT services or ICT products acquisition.

REQ-7.7-17: The TSP shall review and, where necessary, update their secure development rules at planned intervals.

REQ-7.7-18: The TSP shall apply change management procedures to control changes of network and information systems. Where applicable, the procedures shall be consistent with the TSP's general policies concerning change management.

REQ-7.7-19: The change management procedures shall be applied for releases, modifications and emergency changes of any software and hardware in operation and changes to the configuration. The procedures shall ensure that those changes are documented and, based on the risk assessment, tested and assessed in view of the potential impact before being implemented.

REQ-7.7-20: In the event that the regular change management procedures could not be followed due to an emergency, the TSP shall document the result of the change, and the explanation for why the procedures could not be followed.

REQ-7.7-21: The TSP shall review and, where appropriate, update the change management procedures at planned intervals and when significant incidents or significant changes to operations or risks occur.

REQ-7.7-22: The TSP shall establish, implement and apply a policy and procedures for security testing.

REQ-7.7-23: For security testing, the TSP shall:

a) establish, based on the risk assessment, the need, scope, frequency and type of security tests;

b) carry out security tests according to a documented test methodology, covering the components identified as relevant for secure operation in a risk analysis;

c) document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;

d) apply mitigating actions in case of critical findings.

REQ-7.7-24: The TSP shall review and, where appropriate, update their security testing policies at planned intervals.

REQ-7.7-25: The TSP shall specify and apply procedures, coherent with the change management procedures as well as with vulnerability management, risk management and other relevant management procedures, for ensuring that:

a) security patches are applied within a reasonable time after they become available;

b) security patches are tested before being applied in production systems;

c) security patches come from trusted sources and are checked for integrity;

d) additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied.

PRO-7.7-26 [CONDITIONAL]: The TSP may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The TSP shall duly document and substantiate the reasons for any such decision.

7.8 Network security

REQ-7.8-01: The TSP shall protect its network and systems from attacks.

NOTE 1: See clauses 8.20, 8.21, 8.22 and 8.23 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.8-02:** The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services. The TSP shall segment their systems and networks from third parties' systems and networks.

- **REQ-7.8-03:** The TSP shall apply the same security controls to all systems co-located in the same zone, and grant access to a network or zone based on an assessment of its security requirements.
- **REQ-7.8-04:** The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP for safety, and within zones to those necessary for the operation of the TSP.
- **REQ-7.8-05:** The TSP shall explicitly forbid or deactivate not needed connections and services, and, where appropriate, exclusively allow access to the TSP's network and information systems by devices authorised by the TSP.
- **REQ-7.8-06:** The TSP shall review the established rule set, network segmentation, and protection measures on a regular basis and when significant incidents or significant changes to operations or risks occur.
- **REQ-7.8-07:** The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.5]).
- **REQ-7.8-08:** The TSP shall separate dedicated network for administration of IT systems and TSP's operational network, and segregate network administration channels from other network traffic.
- **REQ-7.8-09:** The TSP shall logically separate administration systems and networks from other information systems and networks, and shall not use systems used for administration of the security policy implementation for other purposes.
- **REQ-7.8-10:** The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems) including backups.
- **REQ-7.8-11:** The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.
- **REQ-7.8-12 [CONDITIONAL]:** If a high level of availability of external access to the trust service is required, the TSP shall:

  a) assure that the external network connection is redundant to ensure availability of the services in case of a single failure; and

  b) deploy a demilitarised zone within their communication networks to ensure secure communication originating from or destined to their networks.

- **REQ-7.8-13:** The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
- **REQ-7.8-14:** The TSP shall perform the vulnerability scan requested by **REQ-7.8-13** at least once per quarter.
- **REQ-7.8-15**: The TSP shall monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers.
- **REQ-7.8-16:** The TSP shall protect its network and information systems against malicious and unauthorised software by means of malware detection and removal software, which is updated at least on a daily basis.

NOTE 2: See clause 8.7 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.8-17:** The TSP shall regularly update its malware detection and repair software.
- **REQ-7.8-18:** The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant addressing, without undue delay, vulnerabilities identified as critical to their operations.
- **REQ-7.8-19:** The penetration test requested by **REQ-7.8-18** shall be conducted as follows:

  a) The test shall be performed at least once per year.

b) For vulnerabilities identified during testing with justified potential impact, the TSP shall either implement a mitigation plan or document and substantiate why remediation is not required.

- **REQ-7.8-20:** The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
- **REQ-7.8-21:** Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.
- **REQ-7.8-22:** The TSP shall configure firewalls to prevent all protocols and accesses not required for the operation of the TSP.
- **REQ-7.8-23:** The TSP shall adopt an implementation plan for:

  a) the full transition towards latest generation network layer communication protocols in a secure, appropriate and gradual way and establish measures to accelerate such transition;

  b) the deployment of internationally agreed and interoperable modern e-mail communications standards to secure e-mail communications to mitigate vulnerabilities linked to e-mail-related threats and establish measures to accelerate such deployment; and

  c) applying best practices for the security of the DNS, and for Internet routing security and routing hygiene of traffic originating from and destined to the network.

- **REQ-7.8-24:** The TSP shall document the architecture of the network in a comprehensible and up to date manner.

7.9 Vulnerabilities and Incident management

7.9.1 Monitoring and logging

REQ-7.9.1-01: The TSP shall establish mechanisms to detect potential security incidents and to respond accordingly by implementing tools and processes to enable continuous monitoring and logging of activities on the entity's network and information systems.

NOTE 1: See clauses 8.16, 5.24, 5.25, 5.26, 5.27, 5.28 and 6.8 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.9.1-02:** Monitoring activities should take account of the sensitivity of any information collected or analysed.
- **REQ-7.9.1-03:** Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.

NOTE 2: Abnormal network system activities can comprise (external) network scans or packet drops.

- **REQ-7.9.1-04:** The TSP shall maintain, document and regularly review logs which shall include:

  a) outbound and inbound network traffic;

  b) creation, modification or deletion of users of the TSP's network and information systems and extension of the permissions;

  c) access to systems and applications;

  d) authentication-related events;

  e) activation, stopping and pausing of the various logs;

  f) activities regarding user administration and permission management, access (including privileged access) to systems and applications;

  g) activities performed with administrator accounts;

h) assess or changes to critical configuration files and backups;

i) security relevant logs, including event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;

j) use and performance of system resources;

k) physical access to facilities, where appropriate;

l) access and use of network equipment and devices; and

m) environmental events, where appropriate.

- **REQ-7.9.1-05:** The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.
- **REQ-7.9.1-06:** The TSP shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.
- **REQ-7.9.1-07:** To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities.
- **REQ-7.9.1-08:** The TSP shall implement their monitoring activities in a way which minimises false positives and false negatives.
- **REQ-7.9.1-09:** The TSP shall establish a list of assets to be subject to logging as per **REQ-7.9.1-04** based on the results of the risk assessment.
- **REQ-7.9.1-10:** The logs shall be regularly reviewed for any unusual or unwanted trends.
- **PRO-7.9.1-11:** The TSP shall lay down appropriate values for alarm thresholds.
- **PRO-7.9.1-12 [CONDITIONAL]:** If the laid down values for alarm threshold are exceeded, an alarm shall be triggered, where appropriate, automatically.
- **PRO-7.9.1-13:** The TSP shall ensure that, in case of an alarm, a qualified and appropriate response is initiated in a timely manner.
- **REQ-7.9.1-14:** The TSP shall maintain and back up logs for a predefined period and shall protect them from unauthorised access or changes.
- **REQ-7.9.1-15:** To the extent feasible, the TSP shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment.
- **REQ-7.9.1-16:** The TSP shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant.
- **REQ-7.9.1-17:** The TSP shall establish a system to monitor the availability of the monitoring and logging systems independent of the systems they are monitoring.
- **REQ-7.9.1-18:** The procedures as well as the list of assets that are being logged shall be reviewed and, where appropriate, updated at regular intervals and after significant incidents.

7.9.2 Incident response

- **REQ-7.9.2-01:** The TSP shall establish and implement an incident handling policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing or responding to, recovering from, documenting and reporting of incidents in a timely manner.

- **REQ-7.9.2-02:** The TSP shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.

EXAMPLE 1: Relevant legislative frameworks such as DORA [i.21], CER [i.22], Regulation (EU) 910/2014 [i.1] in particular its Articles 19a and 24(2)(fb), CRA [i.23], DSA [i.24], DGA [i.25], Directive (EU) 2022/2555 [i.27], etc.

- **REQ-7.9.2-03:** TSPs shall inform stakeholders about incidents according to agreed communication plans.
- **REQ-7.9.2-04:** The TSP shall establish and maintain effective communication plans that include incident categorisation, well-defined escalation procedures, and standardised reporting protocols.
- **REQ-7.9.2-05:** The TSP shall ensure that personnel possess the necessary competencies to proficiently detect and respond to security incidents.
- **REQ-7.9.2-06:** The TSP shall create and maintain comprehensive documentation throughout the incident detection and response process.
- **REQ-7.9.2-07:** The TSP shall establish clear interfaces between the incident handling and business continuity management functions to ensure a coordinated and cohesive response during incidents.
- **REQ-7.9.2-08:** The TSP shall test and review regularly and after incidents roles, responsibilities and appropriate procedures.
- **REQ-7.9.2-09:** The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.
- **REQ-7.9.2-10:** For any vulnerability, given the potential impact, the TSP shall [CHOICE]:
  - create and implement a plan to mitigate the vulnerability; or
  - document the factual basis for the TSP's determination that the vulnerability does not require remediation.

EXAMPLE 2: The TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation.

NOTE 1: Further recommendations are given in the CA/Browser Forum network security guide [i.3] item 4 f).

- **REQ-7.9.2-11:** Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.
- **REQ-7.9.2-12:** The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.
- **REQ-7.9.2-13:** The incident handling policy shall be coherent with the business continuity and disaster recovery plan. The policy shall include:
  a) a categorisation system for incidents that is consistent with the event assessment and classification;
  b) effective communication plans including for escalation and reporting;
  c) assignment of roles to detect and appropriately respond to incidents to competent employees;
  d) documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, contact lists and templates.
- **REQ-7.9.2-14:** The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated at planned intervals and after significant incidents or significant changes to operations or risks.
- **REQ-7.9.2-15:** The TSP shall respond to incidents in accordance with documented procedures and in a timely manner.

- **REQ-7.9.2-16:** The incident response procedures shall include the following stages:

  a) incident containment, to prevent the consequences of the incident from spreading;

  b) eradication, to prevent the incident from continuing or reappearing;

  c) recovery from the incident, where necessary.

- **REQ-7.9.2-17:** The TSP shall establish communication plans and procedures:

  a) with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification;

  b) for communication among staff members of the TSP, and for communication with relevant stakeholders external to the TSP.

- **REQ-7.9.2-18:** The TSP shall log incident response activities in accordance with the monitoring and logging procedures, and record evidence.

- **REQ-7.9.2-19:** The TSP shall test at planned intervals their incident response procedures.

7.9.3 Reporting

- **REQ-7.9.3-01:** The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

NOTE: TSPs operating within the European Union can contact the appropriate supervisory body and/or other competent authorities for further guidance on implementing notification procedures as per Regulation (EU) No 910/2014 [i.1] and Directive (EU) 2022/2555 [i.27].

- **REQ-7.9.3-02:** Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

- **REQ-7.9.3-03:** The TSP shall establish a simple procedure allowing its staff, contractors and customers to report possible network and information security incidents.

- **REQ-7.9.3-04:** The TSP shall communicate the reporting procedure to its contractors and customers and shall train its staff to follow the reporting procedure and to address the appropriate point of contact.

- **REQ-7.9.3-05:** The TSP shall put in place a simple mechanism allowing their employees, suppliers, and customers to report suspicious events.

- **PRO-7.9.3-06 [CONDITIONAL]:** The TSP may communicate the event reporting mechanism to their suppliers and customers, and, in case the mechanism is implemented, shall regularly train their employees on how to use it.

- **REQ-7.9.3-07:** The TSP shall consider an incident to be significant where one or more of the following criteria are fulfilled:

  a) the incident has caused or is capable of causing direct financial loss for the TSP that exceeds EUR 500 000 or 5 % of the TSP's total annual turnover in the preceding financial year, whichever is lower;

  b) the incident has caused or is capable of causing the exfiltration of trade secrets of the TSP;

  c) the incident has caused or is capable of causing the death of a natural person;

  d) the incident has caused or is capable of causing considerable damage to a natural person's health;

  e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred, which is capable of causing severe operational disruption;

  f) the incident meets the criteria of recurring incidents as defined in REQ-7.9.3-10;

g) a trust service is completely unavailable for more than 20 minutes;

h) a trust service is unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis;

i) more than 1 % of the users or relying parties in the Union, or more than 200 000 users or relying parties in the Union, whichever number is smaller, are impacted by limited availability of a trust service;

j) physical access to an area where network and information systems are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is compromised; and

k) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a trust service is compromised with an impact on more than 0,1 % of users or relying parties, or more than 100 of users or relying parties, whichever number is smaller of the trust service in the Union.

- **REQ-7.9.3-08:** Scheduled interruptions of service and planned consequences of scheduled maintenance operations carried out by or on behalf of the TSP shall not be considered to be significant incidents.
- **REQ-7.9.3-09:** When calculating the number of users impacted by an incident, the TSP shall consider:

  a) the number of customers that have a contract with the TSP which grants them access to the TSP's network and information systems or services offered by, or accessible via, those network and information systems; and

  b) the number of natural and legal persons associated with business customers that use the TSP's network and information systems or services offered by, or accessible via, those network and information systems.

- **REQ-7.9.3-10:** The TSP shall consider incidents that individually are not considered a significant incident as collectively one significant incident where they meet all of the following criteria:

  a) they have occurred at least twice within 6 months;

  b) they have the same apparent root cause;

  c) they collectively meet the criteria of causing direct financial loss exceeding the thresholds defined in REQ-7.9.3-07 a).

7.9.4 Event assessment and classification

- **REQ-7.9.4-01:** The TSP shall analyse the reported events and assess their severity.
- **REQ-7.9.4-02:** The TSP shall be capable to reassess and reclassify events based on new inputs.
- **REQ-7.9.4-03:** The TSP shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.
- **REQ-7.9.4-04:** For event assessment, the TSP shall:

  a) carry out the assessment based on predefined criteria laid down in advance, and on a triage to determine prioritisation of incident containment and eradication;

  b) assess the existence of recurring incidents on a quarterly basis;

  c) review the appropriate logs for the purposes of event assessment and classification;

  d) put in place a process for log correlation and analysis;

  e) reassess and reclassify events in case of new information becoming available or after analysis of previously available information.

7.9.5 Post-incident reviews

- **REQ-7.9.5-01:** The TSP shall keep itself informed about technical vulnerabilities of all information systems it uses.
- **REQ-7.9.5-02:** The TSP shall evaluate the TSP's exposure to such vulnerabilities and take appropriate measures.

NOTE: See clause 8.8 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.9.5-03:** The TSP shall identify the root cause of an incident and shall conduct a post-incident review possibly resulting in measures mitigating the risk of the recurrence of similar incidents.
- **REQ-7.9.5-04:** The TSP shall ensure that each past incident led to a post-incident review.
- **PRO-7.9.5-05:** Where appropriate, the TSP may carry out post-incident reviews after recovery from incidents.
- **PRO-7.9.5-06:** The post-incident reviews shall, if carried out, identify, where possible, the root cause of the incident and result in documented lessons learned to reduce the occurrence and consequences of future incidents.
- **REQ-7.9.5-07:** The TSP shall ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures, and to incident handling, detection and response procedures.
- **REQ-7.9.5-08:** The TSP shall review at planned intervals if incidents led to post-incident reviews.

7.10 Collection of evidence

REQ-7.10-01: The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

NOTE 1: See requirement **REQ-7.13-05.**

NOTE 2: See clauses 5.28 and 8.15 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.10-02:** The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.
- **REQ-7.10-03:** Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.
- **REQ-7.10-04:** Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
- **REQ-7.10-05:** The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.
- **REQ-7.10-06:** The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.
- **REQ-7.10-07:** Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.2).
- **REQ-7.10-08:** The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

EXAMPLE: This can be achieved, for example, through the use of write-only media, a record of each removable storage media used and the use of off-site backup or by parallel storage of the information at several (e.g. 2 or 3) independent sites.

7.11 Business continuity management

7.11.1 General

REQ-7.11.1-01: The TSP shall maintain backup copies of data and provide sufficient available resources, including facilities, network and information systems and staff, to ensure an appropriate level of redundancy in accordance with risk assessment and business continuity plan.

REQ-7.11-1-02: In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

NOTE 1: See clauses 8.13, 5.29, 5.29 and 5.30 of ISO/IEC 27002:2022 [i.11] for guidance in the event of a disaster.

NOTE 2: Other disaster situations include failure of critical components of a TSP's trustworthy system, including hardware and software.

REQ-7.11.1-03: Based on the results of the risk assessment and the business continuity plan, the TSP shall ensure sufficient availability of resources by at least partial redundancy of the following:

a) network and information systems;

b) assets, including facilities, equipment and supplies;

c) personnel with the necessary responsibility, authority and competence;

d) appropriate communication channels.

REQ-7.11.1-04: The TSP shall document the results of the tests and, where needed, take corrective action.

7.11.2 Back up

REQ-7.11.2-01: The TSP shall maintain backup plan and update it regularly.

REQ-7.11.2-02: The TSP shall define backup plans taking into account at least the following:

a) recovery times;

b) assurance of the backup copies' completeness and accuracy, including configuration data and information stored in cloud service environment;

c) storage of backup copies at a safe location or locations, which are outside the network of the system backed up and are at sufficient distance to escape any damage from a disaster at the main site;

d) appropriate physical and logical controls for backup copies in accordance with their information classification level; and

e) processes for restoring information from backup copies, including approval processes; and

f) retention periods based on business and regulatory requirements.

REQ-7.11.2-03: The TSP shall perform regular integrity check on the backup copies.

REQ-7.11.2-04: The TSP shall test at planed intervals the recovery of backup copies and redundancies and shall take corrective actions in case of findings. The results of these tests shall be documented.

NOTE: See clauses 8.3 and 8.13 of ISO/IEC 27002:2022 [i.11] for guidance.

PRO-7.11.2-05: Where appropriate, the TSP shall ensure that monitoring and adjustment of resources, including facilities, systems and personnel, is duly informed by backup and redundancy requirements.

REQ-7.11.2-06: The TSP shall carry out regular testing of the recovery of backup copies and redundancies to ensure that, in recovery conditions, they can be relied upon and cover the copies, processes and knowledge to perform an effective recovery.

7.11.3 Crisis management

REQ-7.11.3-01: The TSP shall establish processes for crisis management addressing at least:

a) roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in crisis situations, including specific steps to follow;

b) appropriate communication means between the TSP and relevant competent authorities, including both obligatory communications, such as incident reports and related timelines, and non-obligatory communications; and

c) application of appropriate controls to maintain network and information system security in crisis situations.

REQ-7.11.3-02: The TSP shall implement a process for managing and making use of information received from National CSIRT or, where applicable, competent authorities, concerning incidents, vulnerabilities, threats or possible mitigation measures.

REQ-7.11.3-03: The TSP shall test and review its crisis management plan at planned intervals.

REQ-7.11.3-04: Additionally, the TSP shall update the crisis management plan, where appropriate, following significant incidents or significant changes to operations or risks.

7.12 TSP termination and termination plans

REQ-7.12-01: Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

In particular:

- **REQ-7.12-02:** The TSP shall have an up-to-date termination plan.

Before the TSP terminates its services at least the following procedures apply:

- **REQ-7.12-03:** Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.

- **REQ-7.12-04:** Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.

- **REQ-7.12-05:** Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.

- **REQ-7.12-06:** Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.

- **REQ-7.12-07:** Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

- **REQ-7.12-08:** Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.

- **REQ-7.12-09:** The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

- **REQ-7.12-10:** The TSP shall state in its practices the provisions made for termination of service. This shall include:

  a) notification of affected entities; and

b) where applicable, transferring the TSP's obligations to other parties.

- **REQ-7.12-11:** The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

7.13 Compliance

REQ-7.13-01: The TSP shall ensure that it operates in a legal and trustworthy manner.

In particular:

- **REQ-7.13-02:** The TSP shall provide evidence on how it meets the applicable legal requirements.
- **REQ-7.13-03:** Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.
- **REQ-7.13-04:** Applicable standards on accessibility such as ETSI EN 301 549 [i.6] should be taken into account.
- **REQ-7.13-05:** Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

NOTE 1: TSPs operating in Europe are required to ensure that personal data is processed in accordance with Regulation (EU) 2016/679 [i.8]. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online.

NOTE 2: See ISO/IEC 27701:2019 [i.10] for requirements and guidance on the extension to ISO/IEC 27002:2022 [i.11] for privacy information management.

NOTE 3: See clauses 5.31, 5.32, 5.33, 5.34 and 5.35 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.13-06:** The TSP shall put in place an effective compliance reporting system:

  a) appropriate to their structures, operating environments and threat landscapes.

  b) capable to provide to the management bodies an informed view of the current state of the TSP's management of risks.

7.14 Supply chain

7.14.1 Supply chain policy

REQ-7.14.1-01: The TSP shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the TSP shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

REQ-7.14.1-02: The TSP shall define, document and implement processes and procedures to manage the information security risks associated with the use of supplier's products or services, including criteria to select and contract suppliers and service providers.

In particular:

- **REQ-7.14.1-03:** The supply chain policy shall identify and communicate the TSP's role in the supply chain.
- **REQ-7.14.1-04:** The supply chain policy shall define criteria for selecting and contracting suppliers or service providers. Criteria shall include:

  a) the cybersecurity practices of the suppliers and service providers, including their secure development procedures;

b) the ability of the supplier or service provider to meet the cybersecurity specifications, risks and classification levels of the TSP's services, systems or products delivered by the supplier or service provider;

c) the overall quality and resilience of ICT products and ICT services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the ICT products and ICT services;

d) the ability of the TSP to diversify sources of supply and to limit vendor lock-in; and

e) the results of the coordinated security risk assessments of critical supply chains.

- **REQ-7.14.1-05:** The TSP shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.
- **REQ-7.14.1-06:** For monitoring changes in cybersecurity practices, the TSP shall:

  a) regularly monitor reports on the implementation of the service level agreements, where applicable;

  b) review incidents related to ICT products and ICT services from suppliers and service providers;

  c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

  d) analyse the risks presented by changes related to ICT products and ICT services from suppliers and service providers and, where appropriate, take mitigating measures in a timely manner.

7.14.2 Supply chain procedures and processes

REQ-7.14.2-01: Processes and procedures shall be defined and implemented to manage information security risks associated with the information and communication technologies products and services supply chain.

In particular:

- **REQ-7.14.2-02:** TSP shall define information security requirements to apply to ICT product or service acquisition.
- **REQ-7.14.2-03:** TSP shall require that ICT services suppliers propagate the TSP's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the TSP.
- **REQ-7.14.2-04:** TSP shall require that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities.
- **REQ-7.14.2-05:** TSP shall request that ICT products suppliers provide information describing the software components used in products.
- **REQ-7.14.2-06:** TSP shall request that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation.
- **REQ-7.14.2-07:** TSP shall implement a monitoring process and acceptable methods for validating ICT products and services conform to stated cybersecurity requirements.
- **REQ-7.14.2-08:** TSP shall implement a process for identifying and documenting product or service components that are critical for maintaining functionality.
- **REQ-7.14.2-09:** TSP shall obtain assurance that critical components and their origin can be traced throughout the supply chain.
- **REQ-7.14.2-10:** TSP shall obtain assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features.
- **REQ-7.14.2-11:** TSP shall implement processes to ensure that components from suppliers are genuine and unaltered from their specification.

- **REQ-7.14.2-12:** TSP shall define rules for sharing of information regarding the supply chain and any potential issues and compromises among the TSP and its suppliers.

- **REQ-7.14.2-13:** TSP shall implement specific processes for managing ICT component life cycle and availability and associated security risks.

NOTE 1: See clause 5.21 of ISO/IEC 27002:2022 [i.11] for guidance on managing information security in the ICT supply chain.

REQ-7.14.2-14: TSP shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

NOTE 2: See clause 5.22 of ISO/IEC 27002:2022 [i.11] for guidance on Monitoring, review and change management of supplier services.

REQ-7.14.2-15: The TSP shall define, implement and communicate to all relevant interested parties topic-specific policies on the use of cloud services and on how the TSP intends to manage information security risks associated with them.

NOTE 3: See clause 5.23 of ISO/IEC 27002:2022 [i.11] for guidance on Information security for use of cloud services.

NOTE 4: The use of cloud services involves, as per contract, shared responsibility for information security and collaborative effort between the cloud service provider and the TSP acting as the cloud service provider customer. It is essential that the responsibilities for both the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately.

7.14.3 Responsibility, third parties agreements and SLA

REQ-7.14.3-01 [CONDITIONAL]: When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it shall maintain overall responsibility for conformance with the supply chain policy, its information security policy and the requirements defined in the trust service policy.

REQ-7.14.3-02: The TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.

In particular:

- **REQ-7.14.3-03:** These processes and procedures shall include:

  a) those to be implemented by the TSP;

  b) those the TSP requires the supplier to implement for the commencement of use of a supplier's products or services; and

  c) those the TSP requires the supplier to implement for the termination of use of a supplier's products and services.

NOTE 1: This applies to TSP's use of resources of cloud service providers.

NOTE 2: See clause 5.19 of ISO/IEC 27002:2022 [i.11] for guidance on information security in supplier relationships.

REQ-7.14.3-04: The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements to ensure that there is clear understanding between the TSP and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

REQ-7.14.3-05 [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.

REQ-7.14.3-06 [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component meet the appropriate requirements of the applicable policy and practices.

REQ-7.14.3-07: The TSP shall include in their services agreements "Service level agreements" and/or auditing mechanisms ensuring that direct suppliers and service providers, including cloud computing providers, take appropriate security measures addressing the TSP's security requirements aligned with the TSP's risk assessment.

In particular:

- **REQ-7.14.3-08:** Compliance with TSPs security policies and requirements shall be considered in the selection process of any direct supplier or service provider as part of the procurement process.
- **REQ-7.14.3-09:** Applicable TSPs security policies and requirements and shall be included in contracts with direct suppliers or service providers.

REQ-7.14.3-10: The TSP shall review the supply chain policy and monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals, at least annually, or after an incident related to the provision of services from direct suppliers or service providers.

NOTE 3: See clauses 5.19 to 5.23 of ISO/IEC 27002:2022 [i.11] for guidance on supplier relationships.

REQ-7.14.3-11: The TSP shall establish and maintain a register of suppliers and their agreements to track where the TSP information is managed and/or archived.

EXAMPLE: This can help identify where information is exchanged.

NOTE 4: This registry could be integrated with other compliance registries maintained by the TSP, such as those required under GDPR for data processing activities, provided all required information is captured and readily accessible.

REQ-7.14.3-12: The TSP shall regularly review, validate and update its registry of suppliers and their agreements to ensure that they are still valid, fit for purpose, and include the relevant information security clauses.

NOTE 5: See clause 5.20 of ISO/IEC 27002:2022 [i.11] for guidance on addressing information security within supplier agreements.

REQ-7.14.3-13: Based on the supply chain security policy and taking into account the results of the risk assessment, the TSP shall ensure that their contracts with the suppliers and service providers specify, where appropriate through service level agreements, the following, where appropriate:

a) cybersecurity requirements for the suppliers or service providers, including requirements regarding the security in acquisition of ICT services or ICT products;

b) requirements regarding awareness, skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees;

c) requirements regarding the verification of the background of the suppliers' and service providers' employees;

d) an obligation on suppliers and service providers to notify, without undue delay, the TSP of incidents that present a risk to the security of the network and information systems of the TSP;

e) the right to audit or right to receive audit reports;

f) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the TSP;

g) requirements regarding subcontracting and, where the TSP allows subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point a);

h) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.

REQ-7.14.3-14: The TSP shall maintain and keep up to date a registry of their direct suppliers and service providers, including:

a) contact points for each direct supplier and service provider;

b) a list of ICT products, ICT services, and ICT processes provided by the direct supplier or service provider to the TSP.

Annex A (informative): Mapping ETSI EN 319 401 requirements with DORA Regulation

A.1 Introduction

The Digital Operational Resilience Act (DORA) establishes a comprehensive framework for ensuring the digital operational resilience of financial entities within the European Union. DORA requires financial entities to implement robust ICT risk management frameworks and to properly oversee their ICT third-party service providers.

Trust Service Providers (TSPs), particularly Qualified Trust Service Providers (QTSPs), are subject to a rigorous regulatory framework under the eIDAS Regulation and the implementing standards developed by ETSI. This regulatory regime already includes stringent requirements for security, reliability, and operational resilience that significantly overlap with DORA's requirements for ICT third-party service providers (Article 30).

By recognizing the rigorous auditing and certification regime that QTSPs undergo, financial entities can streamline their due diligence processes, potentially reducing questionnaires and duplicate assessments. The eIDAS certification, which includes fulfilment of requirements from the NIS2 directive, can serve as a primary verification mechanism for many DORA requirements.

Financial entities subject to DORA can efficiently verify compliance by consulting publicly available mandatory information such as the Trust Service Practice Statement (TSPS), reviewing the TSP's presence on the EU Trust List, and requesting relevant documentation from the QTSP as needed.

This approach not only simplifies compliance requirements for financial entities but also recognizes the unique position of QTSPs as fully externally certified suppliers within the digital financial ecosystem.

A.2 Purpose

The purpose of this annex is to demonstrate how the requirements imposed on Trust Service Providers by the present document and related standards correspond to the requirements in Article 30 of DORA, which details contractual arrangements between financial entities and ICT third-party service providers. This mapping may be used by financial entities to streamline their due diligence and oversight processes when engaging QTSPs as ICT service providers.

A.3 How to use this mapping

The following table maps the requirements of DORA Article 30 (paragraphs 2 and 3) to corresponding requirements in ETSI standards. For each DORA requirement, the table provides references to the relevant controls in the present document and related standards that demonstrate compliance.

Where a DORA requirement is fully covered by ETSI standards, this is indicated by the relevant requirement references. Where partial coverage exists, this is explicitly noted. Financial entities may use this mapping to identify where existing ETSI certification and compliance activities can be leveraged to satisfy DORA oversight requirements, potentially reducing duplication of effort and streamlining the contracting process.

DORA Article 30 requirements	Corresponding ETSI EN 319 401 requirements
Article 30(2)(a) A clear and complete description of all functions and services to be provided	• **REQ-6.1-03:** Helps comply by requiring a statement of practices and procedures addressing all requirements of the applicable trust service policy. • **REQ-6.1-04:** Supports compliance by requiring identification of obligations of external organizations supporting the TSP's services. • **REQ-6.2-01:** Contributes by requiring the TSP to make terms and conditions available to subscribers and relying parties. • **REQ-6.2-02:** Helps fulfil the requirement by specifying minimum content of terms and conditions, including applied policies and contact information. • **REQ-7.14.1-02:** Assists compliance by requiring documented processes for supplier management including selection criteria. • **REQ-7.14.3-04:** Directly supports by requiring documented contractual relationships for subcontracting arrangements. • **REQ-7.14.3-11:** Enhances compliance through the requirement to maintain a register of suppliers and their agreements.
Article 30(2)(b) The locations where the contracted functions and ICT services are to be provided and where data is to be processed, including storage location, and requirement for notification of changes to these locations	• **REQ-6.3-04:** Supports compliance by establishing procedures to notify of important changes in the provision of the trust service to appropriate parties, including changes in service provision locations. • **REQ-7.14.2-05:** Helps fulfil this requirement by specifying that TSPs should request information describing software components used in products, which could include location information. • **REQ-7.14.3-07:** Contributes to compliance by requiring service level agreements that would typically include location information. • **REQ-7.14.3-11:** Assists compliance through the requirement to maintain a register of suppliers and their agreements, which would document service locations. • **REQ-7.14.3-12:** Enhances compliance by requiring regular review and updates of the supplier registry to ensure it contains current location information. • **REQ-7.14.3-13:** Directly supports compliance by requiring contracts with suppliers to specify required information, which would include service locations.
Article 30(2)(c) Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data	• **REQ-5-02:** Contributes to compliance by requiring risk treatment measures that ensure security level is commensurate to the degree of risk. • **REQ-6.2-02:** Supports compliance by requiring terms and conditions to include limitations on the use of services and liability information. • **REQ-7.3.2-02:** Helps meet the requirement by requiring asset classification based on confidentiality, integrity, authenticity and availability requirements. • **REQ-7.5-01:** Directly supports by requiring a policy on cryptography to ensure confidentiality, authenticity and integrity of data. • **REQ-7.9.1-01:** Assists compliance by requiring tools and processes for continuous monitoring and detection of security incidents. • **REQ-7.10-01:** Contributes by requiring records to be kept accessible for providing evidence while maintaining integrity and confidentiality. • **REQ-7.13-05:** Directly addresses the requirement by requiring appropriate technical and organizational measures against unauthorized processing of personal data and protection against loss or damage. • **REQ-7.14.3-07:** Enhances compliance by requiring service level agreements with direct suppliers addressing security measures.

DORA Article 30 requirements	Corresponding ETSI EN 319 401 requirements
Article 30(2)(d) Provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of insolvency, resolution or discontinuation	• **REQ-7.10-01:** Supports compliance by requiring all relevant information to be recorded and kept accessible, even after the activities of the TSP have ceased. • **REQ-7.11.2-01:** Contributes by requiring maintenance of backup copies of data to ensure an appropriate level of redundancy. • **REQ-7.12-01:** Directly supports by requiring the minimization of disruptions to subscribers and relying parties as a result of cessation of services. • **REQ-7.12-06:** Helps meet the requirement by requiring transfer of obligations to a reliable party for maintaining information after cessation of services. • **REQ-7.12-11:** Assists compliance by requiring maintenance or transfer of obligations to make available public keys or trust service tokens to relying parties. • **REQ-7.14.3-13:** Enhances compliance by requiring contracts with suppliers to specify obligations at termination of contract, including retrieval and disposal of information.
Article 30(2)(e) Service level descriptions, including updates and revisions thereof	• **REQ-6.1-05:** Supports compliance by requiring the TSP to make available practice statements and relevant documentation to demonstrate conformance. • **REQ-6.1-08:** Contributes by requiring a defined review process for practices, including responsibilities for maintaining the practice statement. • **REQ-6.1-09:** Directly supports by requiring due notice of changes to be given when the TSP intends to make changes that might affect acceptance of the service. • **REQ-6.1-10:** Helps meet the requirement by requiring revised practice statements to be made immediately available. • **REQ-6.3-02:** Assists compliance by requiring changes to information security policy to be communicated to relevant third parties. • **REQ-7.14.3-07:** Enhances compliance by requiring service level agreements that address security measures. • **REQ-7.14.3-13:** Directly supports by requiring contracts with suppliers to specify service level agreements.
Article 30(2)(f) The obligation of the ICT third-party service provider to provide assistance at no additional cost or at a cost determined ex-ante when an ICT incident occurs	• **REQ-7.9.2-01:** Supports compliance by requiring establishment of incident handling policy with roles, responsibilities, and procedures for responding to incidents. • **REQ-7.9.2-05:** Contributes by requiring personnel to possess necessary competencies to proficiently detect and respond to security incidents. • **REQ-7.9.2-06:** Helps meet the requirement by requiring comprehensive documentation throughout the incident detection and response process. • **REQ-7.9.2-15:** Directly supports by requiring the TSP to respond to incidents in accordance with documented procedures and in a timely manner. • **REQ-7.9.2-17:** Assists compliance by establishing communication plans and procedures for communication among staff members and with external stakeholders. • **REQ-7.14.3-13:** Enhances compliance by requiring contracts to specify obligations for handling incidents that present a risk to security.

DORA Article 30 requirements	Corresponding ETSI EN 319 401 requirements
Article 30(2)(g) The obligation to fully cooperate with the competent authorities and the resolution authorities	• **REQ-7.9.2-02:** Supports compliance by requiring the TSP to comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including to supervisory authorities. • **REQ-7.9.2-07:** Contributes by requiring clear interfaces between incident handling and business continuity management functions. • **REQ-7.9.2-17:** Helps meet the requirement by establishing communication plans with Computer Security Incident Response Teams (CSIRTs) or competent authorities. • **REQ-7.11.3-02:** Assists compliance by requiring implementation of a process for managing information received from National CSIRT or competent authorities. • **REQ-7.13-02:** Enhances compliance by requiring the TSP to provide evidence on how it meets applicable legal requirements. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify obligations for notification and cooperation with authorities.
Article 30(2)(h) Termination rights and related minimum notice periods	• **REQ-6.2-02:** Supports compliance by requiring terms and conditions to specify limitations on liability and legal information. • **REQ-7.12-01:** Contributes by requiring potential disruptions to subscribers and relying parties to be minimized as a result of cessation of services. • **REQ-7.12-02:** Helps meet the requirement by requiring an up-to-date termination plan. • **REQ-7.12-03:** Directly supports by requiring the TSP to inform all subscribers, entities with agreements, and relevant authorities about termination before it happens. • **REQ-7.12-08:** Assists compliance by requiring arrangements to transfer services to another TSP where possible. • **REQ-7.12-10:** Enhances compliance by requiring the TSP to state provisions for termination of service in its practices. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify obligations at termination of contract.
Article 30(2)(i) The conditions for the participation in ICT security awareness programmes and digital operational resilience training	• **REQ-7.2-02:** Supports compliance by requiring staff and contractors to possess necessary expertise, reliability, experience, and qualifications with training regarding cybersecurity. • **REQ-7.2-05:** Contributes by requiring regular updates on new threats and current security practices. • **REQ-7.2-07:** Helps meet the requirement by requiring information security roles and responsibilities to be documented. • **REQ-7.2-21:** Assists compliance by requiring verification of background of employees and service providers, which would include verifying training. • **REQ-7.9.2-05:** Enhances compliance by ensuring personnel possess necessary competencies to detect and respond to security incidents. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify requirements regarding awareness, skills and training required from the suppliers' or service providers' employees.
Article 30(3)(a) Full service level descriptions with precise performance targets	• **REQ-6.1-05:** Supports by requiring documentation demonstrating conformance to policy. • **REQ-6.2-02:** Contributes by requiring detailed terms and conditions. • **REQ-6.2-05:** Helps by requiring terms to be in understandable language. • **REQ-7.14.3-07:** Directly supports by requiring service level agreements with appropriate security measures. • **REQ-7.14.3-13:** Enhances compliance by requiring contracts to specify service levels.

DORA Article 30 requirements	Corresponding ETSI EN 319 401 requirements
Article 30(3)(b) Notice periods and reporting obligations of the ICT third-party service provider to the financial entity	• **REQ-6.3-04:** Supports by requiring procedures to notify of important changes. • **REQ-7.9.2-03:** Contributes by requiring TSPs to inform stakeholders about incidents. • **REQ-7.9.3-02**: Helps by requiring notification to affected persons of security breaches. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify notification obligations.
Article 30(3)(c) Requirements for the ICT third-party service provider to implement and test business contingency plans and to have ICT security measures, tools and policies	• **REQ-7.11.1-01:** Supports by requiring backup data and resources for redundancy. • **REQ-7.11.1-02:** Contributes by requiring restoration of operations after disaster. • **REQ-7.11.3-01:** Helps by requiring processes for crisis management. • **REQ-7.14.3-07:** Assists by requiring security measures in service agreements. • **REQ-7.14.3-13:** Enhances compliance by requiring contracts to address cybersecurity requirements.
Article 30(3)(d) The obligation to participate and fully cooperate in the financial entity's TLPT	• **REQ-7.8-13:** Supports by requiring regular vulnerability scanning. • **REQ-7.8-18:** Contributes by requiring penetration testing after significant changes. • **REQ-7.8-20:** Helps by requiring evidence of qualified penetration testing. • **REQ-7.9.2-08:** Assists by requiring regular testing of incident response procedures. • **REQ-7.11.2-06:** Enhances compliance by requiring testing of recovery processes.
Article 30(3)(e)(i) Unrestricted rights of access, inspection and audit	• **REQ-7.9.3-06:** Supports by requiring mechanisms for reporting security incidents. • **REQ-7.10-01:** Contributes by requiring records to be kept accessible for legal evidence. • **REQ-7.10-03:** Helps by requiring records to be available for providing evidence. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify the right to audit or receive audit reports. • **REQ-7.13-06:** Includes the TSP obligation to put in place an effective compliance reporting system
Article 30(3)(e)(ii) The right to agree on alternative assurance levels if other clients' rights are affected	• **REQ-7.14.1-02:** Supports by requiring criteria for selecting and contracting suppliers. • **REQ-7.14.2-07:** Contributes by requiring monitoring processes for validating ICT products and services. • **REQ-7.14.3-06:** Helps by ensuring flexibility in service component requirements.
Article 30(3)(e)(iii) The obligation to fully cooperate during onsite inspections	• **REQ-7.9.2-07:** Supports by requiring interfaces between incident handling and business continuity. • **REQ-7.13-02:** Contributes by requiring evidence of meeting legal requirements. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify cooperation with authorities.
Article 30(3)(e)(iv) The obligation to provide details on the scope, procedures to be followed and frequency of inspections and audits	• **REQ-7.14.3-07:** Supports by requiring service level agreements addressing security. • **REQ-7.14.2-12:** Contributes by requiring rules for sharing information. • **REQ-7.14.3-13:** Helps by requiring specific obligations in contracts.
Article 30(3)(f)(i) Exit strategies during transition period for service continuity	• **REQ-7.12-01:** Supports by requiring minimization of disruptions during cessation. • **REQ-7.12-06:** Contributes by requiring transfer of obligations to a reliable party. • **REQ-7.12-08:** Directly supports by requiring arrangements for service transfer. • **REQ-7.12-10:** Helps by requiring provisions for termination in TSP practices.

DORA Article 30 requirements	Corresponding ETSI EN 319 401 requirements
Article 30(3)(f)(ii) Exit strategies for allowing migration to another provider or in-house solutions	• **REQ-7.12-08:** Supports by requiring arrangements to transfer provision of services. • **REQ-7.12-11:** Contributes by requiring maintenance of obligations for a reasonable period. • **REQ-7.14.3-13:** Directly supports by requiring contracts to specify obligations at termination.
DORA derogation regarding **"microenterprises delegating rights of access, inspection and audit to independent third parties"**	• **REQ-7.14.3-01:** Supports by allowing the TSP to maintain overall responsibility while using other parties through subcontracting arrangements. • **REQ-7.14.3-02:** Contributes by requiring the TSP to define outsourcers' liability and ensure implementation of required controls. • **REQ-7.14.3-04:** Helps by requiring documented agreements for third-party arrangements to ensure clear understanding of obligations. • **REQ-7.14.3-07:** Assists compliance by allowing auditing mechanisms through service agreements. • **REQ-7.14.3-13:** Enhances compliance by requiring contracts to specify rights to audit or receive audit reports, which could include delegated audit arrangements. • **REQ-7.14.2-07:** Directly supports by allowing for acceptable methods for validating ICT products and services, which could include third-party validation.

Annex B (informative): Mapping ETSI EN 319 401 requirements with eIDAS Regulation

Regulation (EU) No 910/2014 [i.1]	ETSI EN 319 401
Regulation article 13.2 Liability and burden of proof	**EU qualified certificate policy reference**
"13 2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations."	REQ-6.2-02 items f) and g)
Regulation article 15 Accessibility for persons with disabilities	**EU qualified certificate policy reference**
"The provision of electronic identification means, trust services and end-user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies."	REQ-7.13-03 and REQ-7.13-04
Security requirements applicable to trust service providers (Article 20 e IDAS [i.1] and article 21 NIS2 Directive [i.13])	**EU qualified certificate policy reference** Clauses 5, 6, 7
Regulation article 24 **Requirements for qualified trust service providers**	**EU qualified certificate policy reference**
24.2.(a) "inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities;"	REQ-6.3-04
24.2 (b) "employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;"	Clause 7.2
24.2 (c) "with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;"	REQ-7.1.1-04
24.2 (d) "before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use";	Clause 6.2
24.2 (e) "use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including suitable cryptographic techniques."	REQ-7.8-21 and REQ-7.8-22 Clauses 7.5 to 7.8, especially 7.5-02
24.2 (f) "use trustworthy systems to store data provided to them, in a verifiable form so that: *(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,* *(ii) only authorised persons can make entries and changes to the stored data,* *(iii) the data can be checked for authenticity."*	REQ-7.8-21 and REQ-7.8-22 Clauses 7.5 to 7.8
24.2 (g) "take appropriate measures against forgery and theft of data;"	Clauses 5, 6.3, 7.2 to 7.12 REQ-7.8-21 and REQ-7.8-22
24.2 (h) "record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;"	Clause 7.12 REQ-7.3.3-02
24.2 (i) "have an up-to-date termination plan to ensure the continuity of service in accordance with provisions that are verified by the supervisory body pursuant to Article 46b(4), point (i)."	Clause 7.12

Annex C (informative): Mapping ETSI EN 319 401 requirements with Commission Implementing Regulation (EU) 2024/2690 (NIS2)

C.1 Introduction

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 [i.27] lays down rules for the application of Directive (EU) 2022/2555 (NIS2) as regards technical and methodological requirements of cybersecurity risk-management measures. This implementing regulation applies specifically to trust service providers, among other entities, establishing detailed requirements to ensure a high common level of cybersecurity across the Union.

The present document already incorporates the fundamental cybersecurity principles and requirements established in the NIS2 Directive [i.13] and its implementing regulation, providing a comprehensive framework for security management and operational resilience of trust service providers. The requirements in the present document not only meet the demands of the implementing regulation but in many cases provide more detailed and specific specifications for the trust services context, demonstrating comprehensive coverage and contributing to achieving a high common level of cybersecurity in the European Union.

This annex demonstrates the correspondence and facilitates trust service providers' understanding of how compliance with the present document contributes to meeting the obligations established in the NIS2 implementing regulation [i.27].

C.2 Purpose

This mapping allows trust service providers to:

- Identify the present document's requirements that contribute to compliance with the NIS2 Implementing Regulation
- Understand the comprehensive coverage that the present document provides for cybersecurity requirements
- Facilitate assessment and audit processes by demonstrating regulatory correspondence
- Optimize implementation of cybersecurity measures by avoiding duplication

C.3 Mapping table

The following table maps the articles and sections of Commission Implementing Regulation (EU) 2024/2690 [i.27] with the corresponding requirements in the present document.

Commission Implementing Regulation (EU) 2024/2690	**Corresponding ETSI EN 319 401 requirements**
Article 1 - Subject matter	The entirety of ETSI EN 319 401 addresses the subject matter of the regulation for trust service providers
Article 2 - Technical and methodological requirements	Clauses 5, 6 and 7 of ETSI EN 319 401
Article 2(2)	REQ-4.2.01 to REQ-4.2.06 regarding proportionality in applying technical and methodological requirements
Article 3 - Significant incidents	REQ-7.9.3-07 to REQ-7.9.3-10 (significant incident criteria)
Article 4 - Recurring incidents	REQ-7.9.3-10 (recurring incidents)
Article 14 - Significant incidents with regard to trust service providers	REQ-7.9.3-07 (specific criteria for TSP) REQ-7.9.3-08 and REQ-7.9.3-09 (calculation of impacted users)
ANNEX - Section 1: Policy on the security of network and information systems	
1.1 - Policy on the security of network and information systems	REQ-6.3-01 to REQ-6.3-09 (Information and Network Security Policy)

Commission Implementing Regulation (EU) 2024/2690	Corresponding ETSI EN 319 401 requirements
1.2 - Roles, responsibilities and authorities	REQ-7.1.1-01 to REQ-7.1.1-05 (Internal organization) REQ-7.1.2-01 to REQ-7.1.2-06 (Organization reliability) REQ-7.1.3-01 (Segregation of duties)
ANNEX - Section 2: Risk management policy	
2.1 - Risk management framework	REQ-5-01 to REQ-5-08 (Risk Management Framework and Risk Assessment)
2.2 - Compliance monitoring	REQ-7.13-06 (Compliance reporting system) REQ-5-08 (Procedures to assess effectiveness)
2.3 - Independent review of information and network security	REQ-7.13-01 to REQ-7.13-06 (Compliance)
ANNEX - Section 3: Incident handling	
3.1 - Incident handling policy	REQ-7.9.2-01 to REQ-7.9.2-19 (Incident response)
3.2 - Monitoring and logging	REQ-7.9.1-01 to REQ-7.9.1-18 (Monitoring and logging)
3.3 - Event reporting	REQ-7.9.3-03 to REQ-7.9.3-06 (Reporting)
3.4 - Event assessment and classification	REQ-7.9.4-01 to REQ-7.9.4-04 (Event assessment and classification)
3.5 - Incident response	REQ-7.9.2-15 to REQ-7.9.2-19 (Incident response)
3.6 - Post-incident reviews	REQ-7.9.5-01 to REQ-7.9.5-08 (Post-incident reviews)
ANNEX - Section 4: Business continuity and crisis management	
4.1 - Business continuity and disaster recovery plan	REQ-7.11.1-01 to REQ-7.11.1-04 (Business continuity management)
4.2 - Backup and redundancy management	REQ-7.11.2-01 to REQ-7.11.2-06 (Back up)
4.3 - Crisis management	REQ-7.11.3-01 to REQ-7.11.3-04 (Crisis management)
ANNEX - Section 5: Supply chain security	
5.1 - Supply chain security policy	REQ-7.14.1-01 to REQ-7.14.1-06; REQ-7.14.2-01 to REQ-7.14.2-15; REQ-7.14.3-01 to REQ-7.14.3-12 (Supply chain security policy)
5.2 - Directory of suppliers and service providers	REQ-7.14.3-11 to REQ-7.14.3-14 (Registry of suppliers)
ANNEX - Section 6: Security in network and information systems acquisition, development and maintenance	
6.1 - Security in acquisition of ICT services or ICT products	REQ-7.7-11 to REQ-7.7-13 (Acquisition processes) REQ-7.14.2-01 to REQ-7.14.2-15 (Security in acquisition)
6.2 - Secure development life cycle	REQ-7.7-14 to REQ-7.7-17 (Secure development)
6.3 - Configuration management	REQ-7.7-08 to REQ-7.7-10 (Configuration management)
6.4 - Change management, repairs and maintenance	REQ-7.7-18 to REQ-7.7-21 (Change management)
6.5 - Security testing	REQ-7.7-22 to REQ-7.7-24 (Security testing) REQ-7.8-13, REQ-7.8-18 to REQ-7.8-20 (Penetration testing)
6.6 - Security patch management	REQ-7.7-07, REQ-7.7-25, PRO-7.7-26 (Security patch management)
6.7 - Network security	REQ-7.8-01 to REQ-7.8-23 (Network security)
6.8 - Network segmentation	REQ-7.8-02 to REQ-7.8-12 (Network segmentation)
6.9 - Protection against malicious and unauthorised software	REQ-7.7-05, REQ-7.8-16 to REQ-7.8-17 (Protection against malware)
6.10 - Vulnerability handling and disclosure	REQ-7.9.2-09 to REQ-7.9.2-10, REQ-7.9.5-01 to REQ-7.9.5-02 (Vulnerability management)
ANNEX - Section 7: Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	
7.1 to 7.3	REQ-5-08 (Assessment of effectiveness of measures) REQ-7.13-06 (Compliance reporting system)
ANNEX - Section 8: Basic cyber hygiene practices and security training	
8.1 - Awareness raising and basic cyber hygiene practices	REQ-7.2-02, REQ-7.2-05 (Personnel training)
8.2 - Security training	REQ-7.2-02 to REQ-7.2-05, REQ-7.2-12 (Specialized training)
ANNEX - Section 9: Cryptography	
9.1 to 9.3	REQ-7.5-01 to REQ-7.5-05 (Cryptographic controls)
ANNEX - Section 10: Human resources security	
10.1 - Human resources security	REQ-7.2-01 to REQ-7.2-24 (Human resources)
10.2 - Verification of background	REQ-7.2-20 to REQ-7.2-22 (Background verification)
10.3 - Termination or change of employment procedures	REQ-7.2-23 to REQ-7.2-24 (Termination procedures)
10.4 - Disciplinary process	REQ-7.2-06 (Disciplinary sanctions)
ANNEX - Section 11: Access control	
11.1 - Access control policy	REQ-7.4.1-01 to REQ-7.4.1-14 (Access control general)
11.2 - Management of access rights	REQ-7.4.1-07 to REQ-7.4.1-08 (Management of access rights)

Commission Implementing Regulation (EU) 2024/2690	Corresponding ETSI EN 319 401 requirements
11.3 - Privileged accounts and system administration accounts	REQ-7.4.2-01 to REQ-7.4.2-04 (Privileged accounts)
11.4 - Administration systems	REQ-7.4.3-01 to REQ-7.4.3-02 (Administration systems)
11.5 - Identification	REQ-7.4.4-01 to REQ-7.4.4-05 (Identification)
11.6 - Authentication	REQ-7.4.5-01 to REQ-7.4.5-04 (Authentication)
11.7 - Multi-factor authentication	REQ-7.4.6-01 (Multi-factor authentication)
ANNEX - Section 12: Asset management	
12.1 - Asset classification	REQ-7.3.2-01 to REQ-7.3.2-07 (Assets classification)
12.2 - Handling of assets	REQ-7.3.1-01 to REQ-7.3.1-02 (General requirements for asset management) REQ-7.3.3-04 (asset handling policies and their review)
12.3 - Removable media policy	REQ-7.3.3-05 (Removable media policy)
12.4 - Asset inventory	REQ-7.3.2-01 (Asset inventory)
12.5 - Deposit, return or deletion of assets upon termination of employment	REQ-7.3.2-07 (Return of assets)
ANNEX - Section 13: Environmental and physical security	
13.1 - Supporting utilities	REQ-7.6-06 (Supporting utilities) PRO-7.6-07 (Protection of supporting utilities) REQ-7.6-08 (Testing of protection measures)
13.2 - Protection against physical and environmental threats	REQ-7.6-09 to REQ-7.6-11 (Protection against physical and environmental threats) PRO-7.6-10 (Protection measures)
13.3 - Perimeter and physical access control	REQ-7.6-01 to REQ-7.6-05 (Physical and environmental security) REQ-7.6-12 to REQ-7.6-14 (Physical access control)

Annex D (informative): Change history

Date	Version	Information about changes
February 2016	2.1.1	Publication.
June 2017	2.2.0	All requirements numbered as per clause 3.3. **REQ-7.1.1-04:** "national law" replaced with "applicable law". Clause 7.8: several requirement rephrased to use active verbal form, with no technical change. **REQ-7.9-1:** reformulated. **REQ-7.12-10:** "where applicable" added before "transferring the TSP obligations to other parties". **REQ-7.13-03:** "where feasible" added at the end of the sentence. Clause 7.13: note updated to include Regulation (EU) 2016/679. **REQ-7.9-11:** the text "*the TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation*" is turned into a note.
January 2018	2.2.1	Following ENAP public enquiry, the following changes were made: • Deletion of REQ-6.1-03 that was replicated. • Deletion of REQ-6.2-02 g) that was replicated. • Addition of REQ-6.3-10 to document the maximum interval between two checks. • Correction of requirement numbering in clause 7.8 (REQ-7.8-04 was used twice).
September 2020	2.2.2	CR#1 Trust service policy definition and use in clauses 6.1-03. CR#2 Policy for separate components provided by third parties in clause 7.1.1. CR#3 Deviation between the note 2 in OVR 5.2-05 in 319 411-1 and REQ-6.1-05 - REQ-6.1-03 in ETSI EN 319 401. CR#4 Editorial cleaning on Void items. CR#5 Explain "notify notice of changes" in REQ-6.1-09. CR#6 REQ-7.2-08 duplicates REQ-7.2-16. CR#7 Redundant requirement REQ-7.2-09 covered by REQ-7.2-16. CR#8 Use of least privilege in clause 7.2.16. CR#9 Move requirements in clauses 7.4 & 7.7 to 7.8. CR#10 REQ-7.8-11 overcautious. CR#11 Time period in REQ-7.8-13. CR#12 Time period in REQ-7.8-14. CR#13 General correct use of term TSP or Trust service component provider. CR#14 REQ-7.13-05 reference ISO/IEC 27701:2019 for guidance.
May 2021	2.3.1	Publication.
April 2023	2.3.2	Updates to take into account NIS2 Directive. Updates to take into account revision to ISO/IEC 27002:2022.
December 2023		Renumbered all new, changed or moved requirements. Removing "void" requirements.
June 2024	3.1.1	Major revision to align with requirements of NIS2 Directive [i.13] prior to finalisation supporting implementing regulation.
June 2025	3.2.0	Publication for ENAP. Alignment with NIS2 Directive and published Implementing regulation [i.27].
November 2025	3.2.1	Publication for VOTE.

History

Document history				
V1.1.1	January 2013	Publication		
V2.0.1	July 2015	Publication as ETSI TS 119 401 (withdrawn)		
V2.1.1	February 2016	Publication		
V2.2.1	April 2018	Publication		
V2.3.1	May 2021	Publication		
V3.1.1	June 2024	Publication		
V3.2.0	June 2025	ENAP process	AP 20250914:	2025-06-16 to 2025-09-15
V3.2.1	November 2025	ENAP process	V 20260103:	2025-11-04 to 2026-01-05