centro criptológico nacional

ICT Security Guide
CCN-STIC 862

Applicability Criteria for ENS Security Measures against the Quantum Threat



November 2026

Courtesy translation

Courtesy translation

Edit:

centro criptológico nacional

Firmado digitalmente por CCN
Fecha: 2026.11.20 10:08:40 +01'00'

© National Cryptologic Centre (CCN), 2026

Publication date: November 2026

LIMITATION OF LIABILITY

This document is provided in accordance with the terms set out herein, expressly disclaiming any implied warranty that may be associated with it. Under no circumstances may the National Cryptologic Centre be held liable for any direct, indirect, incidental or special damage arising from the use of the information and software referred to herein, even when advised of the possibility of such damage.

LEGAL NOTICE

The partial or total reproduction of this document by any means or process, including reprography and computer processing, and the distribution of copies thereof through public rental or lending, are strictly prohibited without the written authorization of the National Cryptologic Centre, subject to the penalties established by law.

INDEX

1 INTRODUCTION 4
2 PURPOSE, SCOPE AND INTENDED AUDIENCE 4
2.1 Purpose 4
2.2 Scope 5
2.3 Audience 5
3 CONCEPTS 5
4 GENERAL APPLICABILITY CRITERIA 7
4.1 Applicability criteria for ENS measures 7
4.1.1 [org.3] – Security procedures 8
4.1.2 [op.pl.1] – Risk analysis 8
4.1.3 [op.pl.2] – Security architecture 9
4.1.4 [op.pl.3] – Acquisition of new components 9
4.1.5 [op.pl.5] – Certified components 10
4.1.6 [op.acc.5] – Authentication mechanism (external users) 10
4.1.7 [op.acc.6] – Authentication mechanism (organization users) 10
4.1.8 [op.exp.1] – Asset inventory 11
4.1.9 [op.exp.2] – Security configuration 11
4.1.10 [op.exp.7] – Incident management 12
4.1.11 [op.exp.8] – Recording of the activity 12
4.1.12 [op.exp.10] – Cryptographic key protection 13
4.1.13 [op.ext.1] – Contracting and service level agreements 13
4.1.14 [op.ext.3] – Protection of the supply chain 13
4.1.15 [op.cont.1] – Impact analysis 14
4.1.16 [op.cont.2] – Continuity plan 14
4.1.17 [op.cont.3] – Periodic tests 15
4.1.18 [mp.per.3] – Awareness 15
4.1.19 [mp.per.4] – Training 15
4.1.20 [mp.com.2] – Protection of confidentiality 16
4.1.21 [mp.com.3] – Protection of integrity and authenticity 16
4.1.22 [mp.si.2] – Cryptography 17
4.1.23 [mp.sw.1] – IT applications development 17
4.1.24 [mp.sw.2] – Acceptance and commissioning 18
4.1.25 [mp.info.3] – Electronic signature 18
4.1.26 [mp.info.4] – Time stamps 19
4.2 Matrix of scenarios and related measures 19
5 PRIORITIZATION OF ACTIONS 21
6 DOCUMENTATION, MONITORING AND REVIEW 21

Courtesy translation

1 INTRODUCTION

The National Security Framework (*Esquema Nacional de Seguridad*, ENS), regulated by Royal Decree 311/2022, establishes the basic principles, minimum requirements and security measures intended to adequately protect the information processed and the services provided by the systems within its scope of application. Its application is based on risk management; prevention, detection, response and conservation; lines of defence; continuous monitoring; and periodic re-evaluation.

Advances in quantum computing make it necessary to prepare the transition of potentially affected cryptographic mechanisms towards solutions suitable for a post-quantum scenario. This need particularly affects certain public-key cryptographic mechanisms used for key establishment, authentication and digital signatures, and requires the risk associated with the harvesting of encrypted information for potential future decryption to be considered from now on.

The response to this risk should not be limited to replacing cryptographic algorithms. The post-quantum transition is a progressive process of risk management and system transformation, encompassing the identification of cryptographic uses and dependencies, the assessment of their exposure, the determination of action priorities, the planning and implementation of migration, the management of coexistence between mechanisms and the incorporation of crypto-agility capabilities enabling an orderly response to future cryptographic changes.

Many of the risks associated with this transition can be addressed through the measures set out in Annex II of the ENS by adapting their interpretation, procedures and technical capabilities. Preparing for the quantum threat requires, in particular, maintaining an appropriate cryptographic inventory, incorporating the threat into the risk analysis, establishing a transition plan and developing capabilities that enable cryptographic mechanisms to be replaced or updated in a controlled manner.

This guide links the post-quantum transition to the ENS measures. For each measure considered relevant, it establishes criteria for determining when and how the quantum threat should be considered, without thereby modifying either the catalogue of measures or the enforceability regime established in the ENS.

Recommendations on specific cryptographic mechanisms and parameters, their authorization, transition timelines and technical implementation shall be established in the corresponding guidelines and recommendations issued by the National Cryptologic Centre (CCN).

In this context, second additional provision of Royal Decree 311/2022 provides for the National Cryptologic Centre (CCN) to develop and disseminate information and communication technology security guidelines to facilitate compliance with its provisions. This guide falls within that technical guidance function.

2 PURPOSE, SCOPE AND INTENDED AUDIENCE

2.1 Purpose

This guide aims to establish **criteria for the application and adaptation of the ENS security measures** relevant to addressing the quantum threat through the preparation, planning, implementation and monitoring of the post-quantum transition of information systems, in a consistent, proportionate, verifiable and risk-based manner.

Courtesy translation

For the purposes of this guide, addressing the quantum threat requires identifying cryptographic uses and dependencies, assessing exposure, prioritizing actions, planning and implementing the migration to suitable mechanisms and incorporating crypto-agility capabilities that make it possible to respond to developments in cryptographic mechanisms, standards and recommendations.

The criteria set out in this guide **neither replace nor exempt from the categorization of information systems** in accordance with the ENS, nor from carrying out the corresponding risk analysis and risk management. The enforceability of security measures shall be determined by the system category, the security dimensions, the corresponding levels and, where appropriate, the risk analysis. The criteria set out in this guide make it possible to determine when the implementation of an applicable measure must specifically consider the risks and needs associated with the quantum threat.

2.2 Scope

The applicability criteria have a **specific and complementary scope**, limited to providing guidance on the applicability, adaptation or, where appropriate, reinforcement of certain security measures affected by the risks arising from quantum computing.

The assessment shall consider the required protection horizon for information and evidence, the expected lifetime of the cryptographic mechanisms and the time required to replace them. Particular attention shall be paid to situations where **the required protection horizon, combined with the estimated migration time, may exceed the period during which it is reasonable to rely on the cryptographic mechanism in use**.

2.3 Audience

This guide is intended for **entities and organizations within the scope of application of the ENS,** as well as for those involved in risk analysis and management and for the implementation, operation and supervision of security measures.

The ENS applies not only to public sector information systems, but also to those of **private-sector** entities that, under a contractual relationship, provide services to public sector entities for the exercise of their competences, as established in Article 2.3 of Royal Decree 311/2022. Furthermore, any organization may choose to apply the ENS voluntarily as a reference framework for improving the security of its information systems.

3 CONCEPTS

To ensure a consistent interpretation of the applicability criteria, the terms set out in the following table shall, for the purpose of this guide, have the meaning specified therein, without prejudice to the definitions established in the ENS and its implementing regulations.

Concept	Operational definition
Quantum threat	Risk to the security of information, communications and electronic evidence arising from the development of quantum computing capabilities capable of reducing or compromising the security provided by certain cryptographic mechanisms.
Post-quantum cryptography	Set of cryptographic mechanisms designed to provide security against adversaries with access to both classical and quantum computing capabilities, in accordance with the standards,

Courtesy translation

Concept	Operational definition
	authorized mechanisms and guidelines established by the competent bodies.
Post-quantum transition	Planned process for identifying, assessing, prioritizing, adapting and replacing cryptographic mechanisms and dependencies affected by the quantum threat, including the preparation, testing, coexistence, migration, decommissioning and monitoring of the mechanisms in use.
Crypto-agility	Ability of a system, product, service or organization to replace or update cryptographic algorithms, protocols, parameters, keys, certificates, libraries or components in a controlled manner and with an acceptable impact on the security, interoperability, continuity and operation of the system.
Cryptographic inventory	Structured and up-to-date record of the uses of cryptography in the system, including algorithms, protocols, libraries, modules, certificates, services, products, interfaces and cryptographic dependencies, together with the information needed to determine their purpose, location, owner, lifecycle and transition requirement, without including any secret cryptographic material.
Protection horizon	Period during which the required security properties must be maintained for the information, communications or evidence protected by cryptographic mechanisms.
Harvest now, decrypt later	Acquisition and retention of encrypted information with the intention of attempting to decrypt it later, when sufficient cryptanalytic or quantum computing capabilities become available.
Cryptographic dependency	Direct or indirect dependency on cryptographic algorithms, protocols, libraries, modules, certificates, keys, products, services or infrastructures required for the operation or security of a system.
Cryptographic migration	Set of technical and organizational activities through which one cryptographic mechanism is replaced by another, including the preparation, testing, coexistence, deployment, decommissioning and verification phases.
Hybrid mode	Combined use of classical and post-quantum cryptographic mechanisms during specific phases of transition, where required by the applicable guidelines, in order to facilitate migration and manage security and interoperability risks.
Applicability criterion	Guideline indicating when and how to apply, adapt or strengthen an Annex II ENS measure or reinforcement against offensive AI, without modifying the catalogue of measures or its enforceability regime.
Compensatory measure	Alternative or interim safeguard that reduces risk until the intended measure can be implemented.
Statement of Applicability	List of the Annex II ENS security measures selected for an information system, in accordance with its category and the risk analysis.

transition

4 GENERAL APPLICABILITY CRITERIA

The applicability criteria provide a framework for determining, **in a proportionate and risk-based manner**, when it is necessary to apply, adapt or reinforce the ENS measures affected by the quantum threat, taking into account the characteristics of the system, the information and services being protected, their exposure, the protection horizon and the evolution of technological and cryptographic capabilities. The aim is to facilitate a consistent and verifiable application of the ENS, while preserving its **stability and technological neutrality**.

This guidance shall be applied **throughout the entire lifecycle of the affected system and services**, from planning, design, development, acquisition and procurement to operation, monitoring, updating, continuity, replacement or decommissioning.

The mere availability or standardization of post-quantum mechanisms shall not, in itself, determine their implementation. The selection and use of cryptographic mechanisms shall take into account the guidelines of the National Cryptologic Centre (CCN), their authorization for the relevant use case, technical maturity, interoperability, performance, the system category and the identified risks.

The post-quantum transition shall rely, in particular, on **four cross-cutting capabilities**:

1. **Cryptographic inventory**, providing visibility into the cryptographic mechanisms and dependencies in place and where they are used.
2. **Cryptographic and quantum risk assessment**, enabling their exposure and treatment priority.
3. **Transition planning**, establishing the roadmap, owners, resources, dependencies, milestones and migration conditions.
4. **Crypto-agility**, enabling cryptographic mechanisms to be replaced or updated in a controlled manner and with an acceptable impact.

Implementation shall prioritise, among others, essential services, information requiring long-term confidentiality, public key infrastructures, identity and electronic signature services, and assets exposed to the risk of Harvest now, Decrypt later.

The proposed applicability criteria determine when the implementation of an applicable security measure should specifically consider the risks and needs arising from the quantum threat.

4.1 Applicability criteria for ENS measures

For each security measure, the **specific applicability criteria for addressing the quantum threat** and their rationale are provided. The selection of security measures included in this guide is not exhaustive: measures not included shall remain applicable where appropriate in accordance with the ENS.

The criteria set out in this guide do not, by themselves, determine whether an ENS measure is required. This shall be determined by the system category, the security dimensions, the corresponding levels and, where appropriate, the risk analysis.

The selection is not exhaustive: measures not included shall remain applicable where appropriate in accordance with the ENS. **It should not be assumed that the quantum threat affects all mechanisms uniformly.**

Courtesy translation

4.1.1 [org.3] – Security procedures

Code	ENS measure
[org.3]	Security procedures

Applicability criterion
Security procedures shall address the identification, replacement, renewal or revocation of algorithms, protocols, keys and certificates affected by the quantum threat, as well as the coexistence of classical and post-quantum mechanisms. They shall be kept up to date, be consistent with the security policy, the risk analysis and the architecture, and comply with the guidelines issued by the competent bodies and with the transition roadmap. Security procedures shall incorporate governance of the cryptographic transition: responsibilities, coordination, change approval, exception management, temporary coexistence of classical and quantum-resistant mechanisms, secure rollback and emergency migration.

Rationale
The cryptographic transition requires repeatable, coordinated and auditable activities. Keeping procedures up to date prevents incomplete or incompatible changes and the reintroduction of configurations that are no longer secure.

4.1.2 [op.pl.1] – Risk analysis

Code	ENS measure
[op.pl.1]	Risk analysis

Applicability criterion
Where the security of cryptographic uses or dependencies may be compromised during the protection period of the information or evidence, the risk analysis shall include the relevant assets and use cases, as well as an inventory of internal and external dependencies. The required confidentiality and validity periods of the information and evidence, the expected lifetime of the cryptographic mechanisms, the risk of Harvest now, Decrypt later and the time required for migration shall be assessed. The transition shall be **a particular priority** where the sum of the required protection period and the migration time may exceed the period during which it is reasonable to rely on the security of the cryptographic mechanism in use. The analysis shall enable the definition of priorities, milestones, resources, compensatory measures and criteria for accelerating the transition. Acceptance of cryptographic mechanisms with insufficient resistance shall be explicit, duly justified, temporary and subject to review.

Rationale
The quantum threat requires preparation activities to begin before cryptographically relevant quantum capabilities become available. In particular, encrypted information captured today may be retained in order to attempt to decrypt it later.

Courtesy translation

Jointly assessing the protection horizon, the expected lifetime of cryptographic mechanisms and the time required to carry out the migration makes it possible to identify cases where the transition needs to begin in advance and to establish priorities proportionate to the risk.

4.1.3 [op.pl.2] – Security architecture

Code	ENS measure
[op.pl.2]	**Security architecture**

Applicability criterion
Where the security architecture includes cryptographic mechanisms or trust relationships that may be affected by the quantum threat, their components, interfaces and dependencies shall be identified, and crypto-agility shall be incorporated into the design. The transition architecture shall provide for post-quantum or hybrid mechanisms where appropriate, in accordance with the guidelines issued by the competent bodies. It shall address interoperability, performance, key and certificate management and temporary coexistence, and shall prevent downgrade to unauthorized mechanisms. Recovery alternatives shall avoid reintroducing configurations that are no longer secure.

Rationale
Documenting the architecture makes it possible to identify protection mechanisms and trust relationships and link them to the risk analysis. Where public-key cryptography is used across applications, communications, authentication and trust infrastructures, its coordinated replacement prevents partial migrations that could leave vulnerable points or disrupt services.

4.1.4 [op.pl.3] – Acquisition of new components

Code	ENS measure
[op.pl.3]	**Acquisition of new components**

Applicability criterion
When acquiring components with cryptographic mechanisms or dependencies that may be affected during their expected lifetime, requirements shall be defined for crypto-agility, cryptographic updates, dependencies documentation, interoperability and migration support, in accordance with the risk analysis and the architecture. Post-quantum or hybrid mechanisms shall be included where appropriate. Technical, contractual, training and financial aspects shall be planned jointly, in accordance with the transition milestones.

Rationale
New acquisitions may introduce dependencies on algorithms or components that are difficult to replace, thereby hindering migration. Planning their evolution and support throughout their service life helps to avoid such dependencies and to coordinate the resources for the transition.

Courtesy translation

4.1.5 [op.pl.5] – Certified components

Code	ENS measure
[op.pl.5]	Certified components

Applicability criterion
The selection of security products and services shall take into account the qualification requirements applicable under the ENS and the CCN guidelines. Where the post-quantum transition is relevant to the use case, the product or service shall be assessed in terms of its ability to incorporate authorized cryptographic mechanisms, its crypto-agility, its update support and the manufacturers or supplier's roadmap.

Rationale
The qualification of a product or service provides assurance regarding its security but does not in itself demonstrate that its cryptographic mechanisms are resistant to the quantum threat. Prioritising qualified components that also use quantum-resistant mechanisms, in accordance with CCN guidelines, reduces the risk of acquiring components that need to be replaced during their service life and facilitates an orderly transition.

4.1.6 [op.acc.5] – Authentication mechanism (external users)

Code	ENS measure
[op.acc.5]	Authentication mechanism (external users)

Applicability criterion
Where the authentication of external users relies on digital certificates or other public-key mechanisms potentially affected by the quantum threat, the certificates, protocols and trust chains involved shall be identified, and their replacement shall be planned according to the system category and the risk analysis. The migration shall preserve interoperability and prevent downgrade to unauthorized mechanisms. Authentication methods not based on public-key cryptography shall continue to be handled in accordance with the standard requirements.

Rationale
The weakening of algorithms used to verify the identity of external users may compromise authentication and facilitate impersonation. A coordinated migration preserves confidence and interoperability of access mechanism.

4.1.7 [op.acc.6] – Authentication mechanism (organization users)

Code	ENS measure
[op.acc.6]	Authentication mechanism (organization users)

Applicability criterion

Courtesy translation

Transition planning shall include the authentication of organization users, including remote access. Certificates, public keys, protocols and trust chains affected by the quantum threat shall be identified, and their replacement shall be scheduled without disrupting service.

Where reinforcement **[op.acc.6.r9.2]** applies, remote access traffic shall be encrypted, and its adaptation shall incorporate post-quantum cryptography capabilities.

The transition of authentication mechanisms for devices, services and processes shall be planned in coordination with the architecture, communications and key management, without being automatically included in this measure. Their certificates, keys, protocols and trust chains shall be reviewed to distinguish affected methods from those that retain an adequate level of resistance.

Rationale

Authentication relies on confidence in credentials and access mechanisms. Public-key dependencies, which are also common in APIs, system-to-system communications and workloads, may be numerous and difficult to replace. Maintaining an inventory of these dependencies and providing crypto-agility enables their transition to be coordinated.

4.1.8 [op.exp.1] – Asset inventory

Code	ENS measure
[op.exp.1]	**Asset inventory**

Applicability criterion

Where system assets include cryptographic uses or dependencies that need to be assessed for the transition, the inventory shall include the relevant cryptographic assets and a map of their dependencies. It shall indicate their purpose, version, location and supplier, without including any secret information that could compromise them.

Where **reinforcement R4 – Software components List** applies, the formal list of software components and deployment services shall complement the inventory.

Rationale

Knowledge of cryptographic uses and dependencies is necessary to assess exposure, prioritize systems and plan a comprehensive transition, preventing affected components from remaining unidentified.

A comprehensive cryptographic transition cannot be assessed or planned without knowing where and for what purpose cryptography is used. A structured inventory makes it possible to identify direct and indirect dependencies, prioritize actions and prevent vulnerable or outdated mechanisms from remaining in use because they were not identified during planning.

4.1.9 [op.exp.2] – Security configuration

Code	ENS measure
[op.exp.2]	**Security configuration**

Applicability criterion

Security configurations shall specify the authorized mechanisms, parameters and protocols, disable obsolete options and prevent security downgrades. Changes shall be controlled and documented to ensure traceability, in accordance with the transition plan.

Courtesy translation

Where the configuration allows protocols, suites, algorithms or cryptographic mechanisms scheduled for decommissioning under the transition plan, they shall be removed or disabled in coordination with interoperability and continuity testing.

Rationale
Consistent configurations prevent the use of vulnerable algorithms, reduce exposure and facilitate coordinated deployment. Decommissioning of legacy mechanisms in a coordinated manner limits that exposure and facilitates migration to configurations resistant to the quantum threat, without compromising interoperability or service continuity.

4.1.10 [op.exp.7] – Incident management

Code	ENS measure
[op.exp.7]	**Incident management**

Applicability criterion
Incident management shall address any loss of cryptographic confidence that may affect algorithms, keys, certificates, signatures, communications and confidence infrastructures or services. Procedures shall distinguish between the planned transition and emergency migration and shall provide for revocation, urgent replacement, preservation of evidence and coordination with third parties. In coordination with continuity capabilities, an accelerated migration shall be prepared and rehearsed, with activation and recovery criteria that prevent the restoration of vulnerable configurations.

Rationale
A cryptanalytic breakthrough or a change in applicable guidelines may undermine confidence in cryptographic mechanisms and require urgent and simultaneous action across multiple services, components and third parties. Incident management enables this response to be coordinated and complements, without replacing, the planned migration.

4.1.11 [op.exp.8] – Recording of the activity

Code	ENS measure
[op.exp.8]	**Recording of the activity**

Applicability criterion
To monitor and provide evidence of the the transition and the lifecycle of cryptographic keys, certificates and mechanisms, sufficient evidence of their generation, use, renewal, revocation, replacement and configuration shall be retained, and linked to the related changes, approvals, tests and results. Retention periods shall be consistent with the applicable obligations and the evidentiary value of the information.

Rationale

Courtesy translation

Accountability makes it possible to demonstrate which mechanism protected each operation, to investigate failures and to show that the roadmap has been executed.

4.1.12 [op.exp.10] – Cryptographic key protection

Code	ENS measure
[op.exp.10]	Cryptographic key protection

Applicability criterion
Where the system manages keys associated with cryptographic mechanisms whose security needs to be reviewed considering the quantum threat, their entire lifecycle shall be assessed. Their rotation, invalidation, orderly replacement, backup and recovery shall be planned in accordance with the transition and the authorized mechanisms. Key establishment, digital signatures, symmetric encryption and hash functions shall be assessed separately, taking into account their dependencies, parameters, interoperability requirements and acceptance criteria. In accordance with CCN guidelines, the authorization of the mechanism, the suitability of the product and the compliance of its implementation shall be verified. Hybrid solutions shall be assessed as a whole.

Rationale
Proper key custody does not compensate for the loss of security of the associated algorithm. Each function has different dependencies and acceptance criteria.

4.1.13 [op.ext.1] – Contracting and service level agreements

Code	ENS measure
[op.ext.1]	Contracting and service level agreements

Applicability criterion
Where changes to the cryptographic components, platforms or dependencies of contracted services require provider involvement, contracts and agreements shall define the service, responsibilities, minimum service levels and the consequences of non-compliance.. They shall include commitments regarding c maintenance, evolution and cryptographic update, support, interoperability, vulnerability notification, certificate renewal and replacement, algorithm replacement, end of cryptographic support, and cooperation in testing and migrations activities. These obligations shall extend to subcontractors and essential dependencies.

Rationale
The entity depends on its suppliers to modify platforms, products and services. Defining their obligations before migration becomes urgent enables responsibilities to be coordinated and ensures that the necessary support is available to carry out the Migration.

4.1.14 [op.ext.3] – Protection of the supply chain

Code	ENS measure
[op.ext.3]	Protection of the supply chain

Courtesy translation

Applicability criterion
Where the supply chain includes libraries, cryptographic modules, PKIs, HSMs, firmware, devices or external services potentially affected by the quantum threat, the providers and the provenance, support and replaceability of these components and services shall be assessed, together with subcontracting dependencies, the transition roadmap, and migration commitments and timelines.

Rationale
An unidentified dependency or a supplier without an upgrade path may prevent or delay completion of the transition.

4.1.15 [op.cont.1] – Impact analysis

Code	ENS measure
[op.cont.1]	Impact analysis

Applicability criterion
Where cryptographic obsolescence, loss of confidence in cryptographic mechanisms or an urgent migration may affect service availability, the impact analysis shall assess potential disruptions, including those affecting services dependent on PKI and certificates. Critical elements, common dependencies, maximum tolerable downtime and operational alternatives shall be identified.

Rationale
Loss of confidence in a shared mechanism may simultaneously affect multiple critical services.

4.1.16 [op.cont.2] – Continuity plan

Code	ENS measure
[op.cont.2]	Continuity plan

Applicability criterion
Where the cryptographic transition or the loss of confidence in its mechanisms may affect the continuity or recovery of critical services, the continuity plan shall include the urgent replacement of keys and certificates, alternative mechanisms, emergency migration and integrity verification. Activation criteria for an accelerated migration shall be defined, together with recovery procedures that avoid restoring vulnerable configurations. These procedures shall be coordinated with technical teams, PKI managers, suppliers and service owners, and shall be rehearsed with the third parties involved.

Rationale
An unplanned transition may cause unavailability or reintroduce mechanisms whose security has been lost.

Courtesy translation

4.1.17 [op.cont.3] – Periodic tests

Code	ENS measure
[op.cont.3]	Periodic tests

Applicability criterion
Where the continuity plan addresses the cryptographic transition or the loss of confidence in algorithms or infrastructures, migration, mass renewal, revocation, coexistence, accelerated migration, recovery and secure rollback shall be rehearsed. Tests shall verify the activation criteria for accelerated migration, coordination with third parties and recovery without restoring vulnerable configurations. Their results shall be used to update the inventory, risk analysis, procedures, continuity plan and roadmap.

Rationale
Testing makes it possible to detect hidden or unrecorded dependencies, incompatibilities and unrealistic transition or recovery timelines, and to correct shortcomings in the plan before the transition is carried out.

4.1.18 [mp.per.3] – Awareness

Code	ENS measure
[mp.per.3]	Awareness

Applicability criterion
Where responsible personnel or users are required to implement cryptographic transition decisions or manage cryptography or long-lived information, awareness activities shall address the need to renew keys, credentials, certificates and evidence, the risks associated with delaying such actions, and the channels for reporting anomalies or migration instructions.

Rationale
Transition affects non-technical users and managers and requires an understanding of the decisions and timescales involved.

4.1.19 [mp.per.4] – Training

Code	ENS measure
[mp.per.4]	Training

Applicability criterion
Where personnel functions require specific competencies to prepare, implement or verify the cryptographic transition, training shall be tailored to those responsible for PKI, electronic signatures, architecture, development, systems, procurement, continuity, preservation and auditing. Training shall cover cryptographic inventory, crypto-agility, migration, testing, preservation and emergency response. Its effectiveness shall be verified through exercises, tests and evidence of implementation.

Courtesy translation

Rationale
The technical and organizational complexity of the transition requires specialized competencies and coordination across teams.

4.1.20 [mp.com.2] – Protection of confidentiality

Code	ENS measure
[mp.com.2]	Protection of confidentiality

Applicability criterion
where the confidentiality of information in transit relies on mechanisms potentially vulnerable to the quantum threat, the affected communications and categories of information, their sensitivity, historical exposure and protection period shall be identified. Migration to authorised quantum-resistant mechanisms shall be prioritised, particularly for information requiring long-term confidentiality and exposed to the risk of Harvest now, Decrypt later. Any information potentially captured in the pass shall be treated separately. The decision shall be documented according to the type of information, its exposure and protection period, taking into account the relevant security dimensions and levels and, where appropriate, the system category. The protection of stored information shall be coordinated with the security measures concerning storage media and cryptographic keys.

Rationale
Encrypted information may be captured today for decryption in the future. Migration becomes a higher priority where confidentiality must be maintained beyond the expected lifetime of the cryptographic mechanism. Migration reduces future exposure, but does not, by itself, eliminate the risk associated with information that has already been intercepted, which requires separate treatment.

4.1.21 [mp.com.3] – Protection of integrity and authenticity

Code	ENS measure
[mp.com.3]	Protection of integrity and authenticity

Applicability criterion
Where the protection of the origin, integrity or authenticity of communications relies on digital signatures or public-key mechanisms potentially affected by the quantum threat, they shall be inventoried and their future verifiability shall be assessed. Their replacement shall be planned in coordination with PKI and key management and with those responsible for electronic signatures, time stamping and preservation of evidence.

Rationale
The quantum threat may weaken signature and authentication algorithms and undermine confidence in information and communications.

Courtesy translation

These mechanisms shall remain fit for purpose throughout the period during which the origin, integrity and authenticity of the information need to be verified.

4.1.22 [mp.si.2] – Cryptography

Code	ENS measure
[mp.si.2]	Cryptography

Applicability criterion
Where the cryptographic protection of information stored on media needs to be reviewed in light of the quantum threat, the encryption in use, public-key dependencies, key management and recovery, and the protection horizon shall be identified. The assessment shall take into account both the applicability conditions and the system category. The selection of algorithms and parameters shall be based on the inventory and shall follow the recommendations of the competent bodies, taking into account prioritization, crypto-agility and the review of symmetric parameters and hash functions. Post-quantum or hybrid mechanisms shall only be considered where appropriate and authorized. Actions shall be coordinated with the relevant security measures concerning communications, digital signatures and key protection.

Rationale
The standardization of a cryptographic mechanism does not guarantee that it is authorized, or that the product or its implementation is compliant for a specific use under the ENS. Stored information may need to remain protected for longer than the cryptographic mechanisms protecting it can be expected to remain secure. The transition shall therefore be prepared before relevant quantum capability become available, with particular attention to public-key dependencies in encryption, key exchange and digital signatures.

4.1.23 [mp.sw.1] – IT applications development

Code	ENS measure
[mp.sw.1]	IT applications development

Applicability criterion
Where IT applications use cryptographic mechanisms or dependencies that require adaptation to the quantum threat, their development shall incorporate security by design and component control. Cryptographic primitives shall be separated from business logic to enable libraries, algorithms, parameters, keys and certificates to be replaced without redesigning the application. Cryptographic dependencies shall be documented and controlled throughout the development lifecycle, avoiding rigid or undocumented dependencies. Cryptographic policies shall be centralized wherever possible.

Rationale
Designing IT applications without rigid cryptographic dependencies facilitates the replacement of their mechanisms and reduces migration costs, time and risk.

Courtesy translation

Incorporating crypto-agility from the development stage enables applications to adapt to new recommendations or to the loss of security of certain cryptographic mechanisms without requiring a complete redesign.

4.1.24 [mp.sw.2] – Acceptance and commissioning

Code	ENS measure
[mp.sw.2]	Acceptance and commissioning

Applicability criterion
Before solutions or changes involving cryptographic mechanisms affected by the transition are put into production, the mechanisms, algorithms and parameters used, the absence of obsolete dependencies and the update capability shall be verified. Interoperability, performance, compatibility, coexistence, rollback and continuity testing shall be carried out in controlled and isolated environments. Testing shall include hybrid configurations where appropriate, and the corresponding evidence shall be retained.

Rationale
Post-quantum mechanisms may affect data sizes, latency, memory consumption, protocols and trust chain. Prior to deployment, acceptance shall demonstrate that the solution meets the security criteria and supports the introduction of changes without disrupting services or degrading confidentiality, authenticity or integrity.

4.1.25 [mp.info.3] – Electronic signature

Code	ENS measure
[mp.info.3]	Electronic signature

Applicability criterion
Where electronic signatures are generated or retained using mechanisms whose security may be compromised during the required verification period, a distinction shall be made between the generation of new signatures and the preservation of historical ones. For historical signatures, validation data, trust chains, time references and any renewals performed shall be retained and documented. Renewal or re-timestamping shall be planned, and its timeliness and effectiveness shall be assessed before confidence in the underlying mechanism is lost, in accordance with the applicable technical and legal conditions.

Rationale
Electronic signatures protect authenticity, integrity of the signed information and the identity of the signatory, and these guarantees must remain verifiable throughout the entire retention period. Late renewal or re-timestamping does not restore evidence whose authenticity or integrity can no longer be demonstrated.

Courtesy translation

4.1.26 [mp.info.4] – Time stamps

Code	ENS measure
[mp.info.4]	Time stamps

Applicability criterion
Where time stamps are generated or retained and their cryptographic mechanisms may no longer provide adequate security during the required verification period, their algorithms, keys and trust chains shall be assessed.. A distinction shall be made between the generation of new time stamps and the preservation of historical evidence. Validation data, the trust chain, the time reference and any renewals performed shall be documented. Renewal or re-timestamping procedures shall be defined to maintain the continuity of evidence throughout the required period, and their timeliness and effectiveness shall be assessed before confidence in the underlying mechanism is lost, in accordance with the applicable technical and legal conditions.

Rationale
Time stamps provide a time reference for verifying evidence and preserving its evidential value, but they also rely on public-key mechanisms. Their preservation requires these guarantees to be maintained: renewal or re-timestamping does not, by itself, restore the integrity or authenticity of evidence that can no longer be demonstrated.

4.2 Matrix of scenarios and related measures

The following matrix provides a proposed mapping traceability between risk scenarios and security measures. **It does not replace the risk analysis**, **nor does it constitute an exhaustive list.**

Scenario	Description	Related measures
Harvest now, Decrypt later	Interception and retention of encrypted information for decryption when sufficient quantum computing capabilities become available.	[op.pl.1] Risk analysis [op.exp.1] Asset inventory [mp.com.2] Protection of confidentiality [mp.si.2] Cryptography
Authentication and signatures compromise	Loss of confidence in certificates, digital signatures or authentication mechanisms based on vulnerable algorithms.	[op.acc.5] Authentication mechanism (external users) [op.acc.6] Authentication mechanism (organization users) [mp.com.3] Protection of integrity and authenticity [mp.info.3] Electronic signature [mp.info.4] Time stamps
Unknown cryptographic dependencies	Use of unidentified cryptographic mechanisms, libraries, certificates or protocols that prevent the transition from being planned.	[op.exp.1] Asset inventory [op.pl.1] Risk analysis [op.pl.2] Security architecture [mp.per.4] Training [op.ext.3] Protection of the supply chain

Courtesy translation

Scenario	Description	Related measures
Lack of crypto-agility	Inability to replace cryptographic mechanisms without redesigning systems, applications or integrations.	[op.pl.2] Security architecture [op.pl.3] Acquisition of new components [op.pl.5] Certified components [mp.sw.1] IT applications development [mp.sw.2] Acceptance and commissioning [mp.si.2] Cryptography
Incomplete or inconsistent migration	Uncontrolled coexistence of classical and post-quantum mechanisms, leading to downgrades or fallback to weaker mechanisms.	[org.3] Security procedures [op.exp.2] Security configuration [mp.sw.1] IT applications development [mp.sw.2] Acceptance and commissioning [mp.per.3] Awareness [mp.per.4] Training
Keys or certificate compromise	Exposure or mismanagement of keys and certificates during renewal, replacement or revocation.	[op.exp.8] Recording of the activity [op.exp.10] Cryptographic key protection [mp.per.3] Awareness [op.exp.7] Incident management
Loss of evidence validity	Future deterioration of the authenticity or evidential value of preserved documents, records, electronic signatures and time stamps.	[mp.info.3] Electronic signature [mp.info.4] Time stamps [mp.com.3] Protection of integrity and authenticity [op.exp.8] Recording of the activity
Vendor or product Lock-in	Dependency on components for which support, updates or a migration path are unavailable.	[op.ext.1] Contracting and service level agreements [op.ext.3] Protection of the supply chain [op.pl.3] Acquisition of new components
Performance and availability impact	Increased data sizes, latency, memory requirements or resource consumption when deploying post-quantum mechanisms.	[mp.sw.2] Acceptance and commissioning [op.cont.1] Impact analysis [op.cont.2] Continuity plan [op.cont.3] Periodic tests
Insufficient interoperability	Failures between systems adopting different standards, parameters or transition timelines.	[op.pl.2] Security architecture [mp.sw.2] Acceptance and commissioning [mp.com.2] Protection of confidentiality [mp.com.3] Protection of integrity and authenticity [op.exp.2] Security configuration
Emergency cryptographic migration	Need for accelerated replacement due to loss of confidence or an urgent change in applicable guidelines.	[op.exp.7] Incident management [op.cont.2] Continuity plan [op.cont.3] Periodic tests [mp.per.4] Training

Courtesy translation

5 PRIORITIZATION OF ACTIONS

Once applicability has been determined, the entity shall prioritize the post-quantum transition actions needed to address the quantum threat, taking into account the risk reduction they provide and the need to carry out the migration sufficiently in advance.

To this end, a **five-step procedure** shall be followed:

1. **Identify cryptographic uses and dependencies:** inventory the affected mechanisms, protocols, certificates and components, as well as their internal and external dependencies.
2. **Assess exposure and the protection horizon:** determine how long the information or evidence needs to be protected and its exposure to the risk Harvest now, Decrypt later.
3. **Determine the need for and urgency of the transition:** compare the protection horizon with the expected effective lifetime of the cryptographic mechanism and the migration time.
4. **Prioritize systems and use cases:** rank them according to their criticality, replacement complexity, dependencies and crypto-agility.
5. **Plan and execute the migration and verify the residual risk:** define and implement the required actions and subsequently assess the residual risk, applying compensatory measures where appropriate.

6 DOCUMENTATION, MONITORING AND REVIEW

Decisions on applicability, adaptation, prioritisation and acceptance shall be duly justified in the risk analysis and where appropriate, reflected, in the **Statement of Applicability, the risk treatment plans and the cryptographic transition plan.** Responsibilities, resources, deadlines, dependencies, milestones, testing, acceptance criteria, exceptions, compensatory measures and residual risk shall be documented.

Acceptance of risk arising from vulnerable mechanisms shall be explicit, duly justified, temporary and subject to review. Monitoring shall use verifiable indicators and shall be reviewed at least annually and whenever significant changes occur in the threat, standards, authorized mechanisms, suppliers, architecture, incidents or test results.

Evidence shall include inventories, procedures, architectures, configurations, contracts, logs, test reports, acceptance decisions and exercise results. Implementation and testing results shall feed back into the inventory, the risk analysis and the transition plan.

Courtesy translation