Q-DAY READINESS ASSESSMENT FRAMEWORK

Assessing Crypto-Agility and PQC Readiness

Version 1.0
March 2026

Inés Atug
ines@nointernet.de

Created with the assistance of AI-powered tools.

Table of Contents

1 Introduction

1.1 The Threat of Q-Day

The term **Q-Day** refers to the point in time at which a cryptographically relevant quantum computer (*Cryptographically Relevant Quantum Computer, CRQC*) will become available, capable of breaking the asymmetric encryption algorithms that are widely used today. Experts estimate this will occur sometime between 2030 and 2040, with projections continually shifting forward due to ongoing technological advances.

The mathematical foundation of this threat is **Shor's Algorithm**, which on a sufficiently powerful quantum computer enables the factorization of large numbers and the computation of discrete logarithms in polynomial time. This would render RSA, ECC (Elliptic Curve Cryptography), and Diffie-Hellman (DH) – which today form the backbone of nearly all digital communications – compromisable within a short period. Symmetric algorithms such as AES may also be affected: **Grover's Algorithm** halves the effective key length, meaning AES-128 would offer only 64-bit security. The recommendation is therefore to use at least AES-256.

In response to this threat, the National Institute of Standards and Technology (NIST) finalized the first post-quantum cryptography standards in August 2024[1]: **FIPS 203 (ML-KEM)** for key encapsulation based on the CRYSTALS-Kyber algorithm, **FIPS 204 (ML-DSA)** for digital signatures based on CRYSTALS-Dilithium, and **FIPS 205 (SLH-DSA)** for stateless hash-based signatures (SPHINCS+). These standards form the foundation for the migration to quantum-safe cryptography.

The BSI (German Federal Office for Information Security) recommends, in a joint statement with the French ANSSI and the Dutch NLNCSA, the use of hybrid solutions[2], in which classical and post-quantum-safe algorithms are combined. This approach provides protection against both current and future attacks.

The EU published a coordinated PQC roadmap in June 2025[3], defining three central milestones: By **31.12.2026**, national roadmaps are to be established, cryptographic inventories built, and awareness programs launched. By **31.12.2030**, all highly critical use cases are to be migrated. By **31.12.2035**, the complete migration of all remaining systems is to be finalized.

Of particular urgency is the so-called **HNDL threat (Harvest Now, Decrypt Later)**: attackers – in particular state-level actors – are already intercepting encrypted data today and storing it, in order to decrypt it once a CRQC becomes available. This means that confidential data transmitted today is already at risk if its retention period extends beyond the expected Q-Day.

The **HNDL Exposure Window** is calculated as: data retention period minus time until a CRQC becomes available. If this value is greater than zero, the data in question is potentially at risk. For

[1] National Institute of Standards and Technology (NIST), *Post-Quantum Cryptography: FIPS Approved*, 2024, https://csrc.nist.gov/projects/post-quantum-cryptography

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), Joint Statement on the Transition to Post-Quantum Cryptography, 2025, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf

[3] Europäische Kommission, *Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, 2024, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

organizations working with long-lived secrets – such as health records, state secrets, intellectual property, or long-term contracts – there is therefore an immediate need for action.

1.2 Why Crypto-Agility?

Crypto-agility (*Crypto-Agility*) refers, as defined by NIST, to the ability of an organization to efficiently replace or update cryptographic algorithms, protocols, keys, and certificates without significant operational disruption[4]. It is explicitly not a one-time migration project, but rather a **permanent organizational capability**, that enables timely responses to new threats, vulnerabilities, or regulatory requirements.

NIST Cybersecurity White Paper 39 (CSWP 39) from December 2025 elevates crypto-agility to a fundamental design principle[4]. The document defines six core capabilities that a crypto-agile organization must possess:

1. Automated Discovery: Automated detection and inventory of all cryptographic assets across the entire infrastructure.

2. Risk-Based Prioritization: Risk-based prioritization of identified cryptographic dependencies for targeted resource allocation.

3. Continuous Measurement: Continuous measurement and monitoring of the cryptographic security posture using defined metrics and KPIs.

4. Agility Testing: Regular testing of the ability to replace cryptographic components and carry out migrations.

5. Executive Reporting: Structured reporting to executive management on cryptographic security status and migration progress.

6. Machine-Readable Policies: Machine-readable policies that enable automated enforcement of cryptographic standards.

The urgency of PQC migration underscores that crypto-agility is not an optional future investment, but a fundamental prerequisite for sustainable IT security. Organizations that do not invest in crypto-agility today will face significantly higher costs and risks later.

1.3 Regulatory Context

The requirements for cryptographic security and PQC readiness are shaped by an increasingly dense web of regulatory provisions. For European organizations, the following regulatory frameworks are particularly relevant:

NIS2 Directive (EU) 2022/2555: Article 21(2)(h) obligates essential and important entities to implement policies and procedures for the use of cryptography[5]. The associated EU Implementing Regulation 2024/2690 specifies this requirement in concrete terms and explicitly mandates that cryptography policies must be based on the principle of crypto-agility[6].

[4] National Institute of Standards and Technology (NIST), *NIST CSWP 39: Considerations for Achieving Cryptographic Agility*, Dezember 2025, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf

[5] Europäische Union, *Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2)*, Artikel 21(2)(h)

[6] Europäische Kommission, Durchführungsverordnung (EU) 2024/2690, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2690

EU PQC Roadmap (June 2025): The NIS Cooperation Group has published a coordinated implementation roadmap for the transition to post-quantum cryptography[7]. This defines three binding milestones: inventory and roadmap development by 31 December 2026, migration of highly critical systems by 31 December 2030, and complete migration by 31 December 2035.

DORA (Digital Operational Resilience Act): For the financial sector, DORA links requirements for operational resilience with cryptographic security[8]. Financial institutions must ensure that their ICT systems are protected against emerging threats – including quantum attacks.

Cyber Resilience Act (CRA): The CRA requires that digital products with digital elements take into account the state of the art with regard to cryptographic measures[9]. From 2027 onwards, quantum-safe cryptography will increasingly be regarded as the state of the art.

GDPR "State of the Art": Article 32 of the GDPR[10] requires technical and organizational measures taking into account the state of the art. Once PQC standards are considered the state of the art, organizations that continue to rely exclusively on quantum-vulnerable algorithms will be in breach of their compliance obligations.

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography (2025): The joint statement by 21 European security agencies recommends hybrid solutions and calls for protection against HNDL attacks no later than the end of 2030[11]. Detailed transition plans for PKI infrastructures are to be in place within the same timeframe.

CNSA 2.0 (USA): The NSA has established binding timelines for US government agencies and their suppliers with the Commercial National Security Algorithm Suite 2.0[12]: PQC for software signatures from 2025, for VPNs and routers from 2026, phase-out of legacy systems by 2030, and fully quantum-resistant National Security Systems by 2035.

UK NCSC Roadmap (2025): The UK's National Cyber Security Centre has published a three-phase roadmap[13]: Discovery & Plan through 2028, Prioritize & Pilot from 2028 to 2031, and Complete Adoption from 2031 to 2035.

1.4 Objectives of the Framework

The Q-Day Readiness Assessment Framework presented here aims to provide organizations – in particular small and medium-sized enterprises (SMEs) – with a practical tool for systematic self-assessment of their crypto-agility and PQC readiness.

---

[7] Europäische Kommission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 2024, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[8] Europäische Union, Digital Operational Resilience Act (DORA), Verordnung (EU) 2022/2554, https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[9] Europäische Union, Cyber Resilience Act (CRA), Verordnung (EU) 2024/2847, https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[10] Europäische Union, Datenschutz-Grundverordnung (DSGVO), Artikel 32, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI), Quantentechnologien und quantensichere Kryptografie – Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, 2024, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien/quantentechnologien_node.html

[12] National Security Agency (NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2024, https://media.defense.gov/2022/Sep/07/2003074170/-1/-1/0/CSI-CNSA-2.0-FACT-SHEET.PDF

[13] UK National Cyber Security Centre (NCSC), Timelines for Migration to Post-Quantum Cryptography, 2025, https://www.ncsc.gov.uk/whitepaper/timelines-for-migration-to-post-quantum-cryptography

The framework is based on the following core principles:

Six Dimensions: The assessment model encompasses the dimensions Inventory, Substitutability, Configurability, Automation, Monitoring, and Governance. These dimensions cover both technical and organizational aspects of cryptographic maturity.

Five Maturity Levels: Each dimension is assessed using a five-level maturity model (Level 1 to 5) that describes progressively building capabilities.

SME Suitability: The framework is designed so that it can be applied without extensive cryptography expertise. The questions are formulated in practical terms and relate to concrete, verifiable facts.

Clear Positioning: The result of the assessment provides a clear positioning on the maturity scale and identifies areas requiring action.

Prioritized Measures: The integrated measures catalog (Chapter 4) and the roadmap (Chapter 5) translate the assessment results into concrete, actionable recommendations.

Regulatory Alignment: The maturity levels and the roadmap are aligned with the milestones of the EU PQC Roadmap (2026/2030/2035), enabling organizations to measure their progress against regulatory timelines.

2 Methodological Foundations

The Q-Day Readiness Assessment Framework combines proven methods from three established frameworks into an integrated assessment approach. The methodological foundations are explained below.

2.1 The BSI HV-Benchmark Compact

The BSI (German Federal Office for Information Security) has developed the HV-Benchmark compact as an instrument for assessing the high availability of IT infrastructures[14]. The methodology is characterized by the following features, which have been adapted for the present framework:

Level-Based Assessment: The HV-Benchmark uses a level model in which each level builds on the previous one. A higher level requires the fulfillment of all requirements of the levels below it. This principle ensures a consistent and transparent assessment.

Weakest-Link Principle: The overall assessment is determined by the weakest link[15]. If an organization achieves Level 4 in five dimensions but only Level 2 in one dimension, the overall maturity level is 2. This principle prevents weaknesses in individual areas from being offset by strengths in others.

Indicator-Based: The assessment is carried out using concrete, verifiable indicators (questions), not subjective judgments. Each question can be answered Yes, Partially, or No.

Transparency and Comparability: The standardized methodology ensures that results are transparent and allow comparisons over time as well as between organizations.

2.2 The CAMM Maturity Model

The **Crypto-Agility Maturity Model (CAMM)** by Näther et al. is the first scientifically grounded maturity model specifically for crypto-agility[16]. It defines five maturity levels (Level 0 to 4) and structures requirements into three categories:

Knowledge (K): Knowledge-based requirements relating to the understanding and documentation of cryptographic dependencies (e.g., inventory, algorithm IDs, performance awareness, security assessment).

Process (P): Process-based requirements relating to organizational workflows and procedures (e.g., updatability, reversibility, policies, testing, automation, scalability).

System Property (S): System properties that must be anchored in architecture and implementation (e.g., extensibility, cryptographic modularity, algorithm exclusion, hardware modularity).

The five CAMM levels build on each other: **Level 0 (Initial)** describes systems in which cryptographic agility is not possible. **Level 1 (Possible)** means that the basic prerequisites for agility are in place. **Level 2 (Prepared)** requires modular architecture and negotiation capability. **Level 3 (Practiced)** demands proven processes and policies. **Level 4 (Sophisticated)** represents fully automated, scalable crypto-agility.

[14]BSI, HV-Benchmark kompakt, 2024, https://www.bsi.bund.de
[15]BSI, HV-Benchmark: Bewertungsmethodik, 2024, https://www.bsi.bund.de
[16] Näther, K., et al., CAMM – Crypto-Agility Maturity Model, 2023, https://arxiv.org/html/2202.07645v3

Why CAMM alone is not sufficient: A key reason for the development of the present framework lies in the deliberate scope limitation of CAMM. The CAMM was designed to assess the crypto-agility of an individual software system or a specific IT landscape – the authors explicitly state: "a maturity model for determining the state of crypto-agility of a given software or IT system". The requirements and maturity levels refer to technical system properties such as modularity, extensibility, and algorithm negotiation at the product level. Organizational dimensions – such as governance structures, organization-wide policies, regulatory compliance, supply chain management, or the ability to coordinate a PQC migration across hundreds of heterogeneous systems – fall outside the CAMM scope. An organization may well operate individual systems with a high CAMM level and yet, as a whole, be unable to respond in a timely manner to a new cryptographic threat, due to a lack of central control, monitoring, automation, or governance. The Q-Day Readiness Assessment Framework closes this gap by supplementing the technical aspects of CAMM with the organizational dimensions of Monitoring, Automation, and Governance, thereby enabling a holistic positioning assessment at the enterprise level – with a particular focus on the requirements of SMEs.

2.3 NIST CSWP 39 Maturity Model

NIST Cybersecurity White Paper 39 (CSWP 39) from December 2025[17] defines a four-tier maturity model for crypto-agility, which serves as a complementary reference for the present framework:

Tier	Description
Tier 1 – Reactive	No formal ownership of cryptographic security. Ad-hoc awareness, no inventory. Reactive action only in response to incidents.
Tier 2 – Managed	CISO awareness present, partial inventory established. Initial documentation and basic processes in place.
Tier 3 – Standardized	Automated discovery, continuous monitoring, executive KPIs defined. Minimum for regulatory compliance.
Tier 4 – Adaptive	Continuous optimization, demonstrated agility through regular testing, integration into Enterprise Risk Management.

2.4 Mapping to the Q-Day Readiness Framework

The present framework combines the strengths of the three described methods: the level-based, indicator-driven assessment methodology of the BSI HV-Benchmark, the six crypto-agility-specific dimensions and the scientific foundation of the CAMM model, as well as the practice-oriented requirements and the compliance perspective of NIST CSWP 39.

The following table defines the five maturity levels of the Q-Day Readiness Framework:

Level	Designation	Description

[17] National Institute of Standards and Technology (NIST), *NIST CSWP 39: Considerations for Achieving Cryptographic Agility*, Dezember 2025, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf

1	**Initial**	No or only rudimentary awareness of cryptographic dependencies. No inventory, no documented processes, no dedicated accountability. Cryptography is taken for granted and not actively managed.
2	**Aware**	Basic awareness of the quantum threat present. Initial inventory measures initiated, critical systems identified. Responsibilities have been assigned, initial documentation exists. The path to crypto-agility has been recognized as a need.
3	**Systematic**	Complete cryptographic inventory in place. Formal processes and policies established. Systematic assessment and prioritized migration strategy. Hybrid implementations in critical systems. Regular monitoring and reporting. This is the critical threshold for regulatory compliance.
4	**Advanced**	Largely automated cryptographic processes. Continuous discovery and compliance monitoring. Algorithm replacement without operational disruption possible. Integration into Enterprise Risk Management and supply chain management.
5	**Excellent**	Fully orchestrated, self-optimizing crypto-agility. Proactive evaluation of new algorithms and threats. Predictive analytics. Demonstrated ability to respond to zero-day vulnerabilities within defined time windows across the organization. Crypto-agility as an integral part of organizational culture.

Level 3 (Systematic) represents the **critical threshold**: organizations that reach this level possess the basic capabilities required for regulatory compliance and are able to carry out an orderly PQC migration. Level 3 corresponds to CAMM Level 2–3 and NIST Tier 3 (Standardized).

2.5 Conducting the Assessment

The assessment is conducted dimension by dimension using the questions defined in Chapter 3. For each dimension, the achieved maturity level is determined by verifying whether the requirements of the respective level are met. The **weakest-link principle**: a level is only considered achieved if all questions for that level can be answered predominantly with “Yes”. Individual questions that are only partially fulfilled may be tolerated, provided the overall picture of the level is consistent.

The **Overall Maturity Level** of the organization corresponds to the lowest individual value across all six dimensions. This principle ensures that no critical gaps are overlooked.

Practical guidance for conducting the assessment:

Participants: The assessment should be conducted with the involvement of IT management, the CISO or IT security officer, system administration, software development (if applicable), and executive management. External facilitation can enhance objectivity.

Time required: For the initial assessment, 4 to 8 hours should be planned, spread across one to two workshops. Follow-up assessments are typically completable in 2 to 4 hours.

3 The Six Dimensions of Crypto-Agility

The dimension model is based on the CAMM framework by Näther et al.[18] and has been adapted for practical application in organizations. The six dimensions cover both technical aspects (Inventory, Substitutability, Configurability, Automation, Monitoring) and organizational aspects (Governance) of crypto-agility. Together they form a holistic picture of an organization's ability to manage cryptographic change.

For each dimension, the purpose, scope, and typical challenges are described first. The maturity table then enables concrete assessment based on verifiable questions. The Answer column can be filled with "Yes", "Partially", or "No"; the Comments column serves to document evidence and measures.

3.1 Dimension 1 – Inventory

The Dimension **Inventory** captures the extent to which an organization maintains a complete and current overview of its cryptographic assets. This includes algorithms in use, protocols, keys, certificates, and their dependencies.

A cryptographic inventory is the indispensable foundation of any PQC migration. Without knowing where and how cryptography is deployed, a systematic migration is impossible. The EU PQC Roadmap identifies the creation of cryptographic inventories as the first milestone by end of 2026.

Typical challenges for SMEs: Shadow IT and undocumented systems complicate inventorying. Legacy systems frequently use older cryptographic methods whose dependencies are not transparent. Cloud services and SaaS applications shift cryptography to third-party responsibility without the specific methods in use being known. Embedded systems and IoT devices often employ hardcoded cryptographic implementations that resist straightforward inventorying.

Level	Question / Indicator	Answer	Comments
1	**Initial**		
1	Does an overview exist of the key systems that use cryptography (e.g. VPN, email, web servers, database encryption)?		
1	Is it known which cryptographic methods (algorithms, protocols, key lengths) are in use within the organization?		
1	Is it known which certificates and keys are in use and when they expire?		
2	**Aware**		

2	Has a systematic stocktaking of cryptographic assets been initiated?		
2	Are critical systems and their cryptographic dependencies being documented?		
2	Has a responsible person been designated for cryptographic inventorying?		
2	Are discovery tools being evaluated or deployed to identify cryptographic assets?		
3	**Systematic**		
3	Does a complete cryptographic inventory exist across all layers (infrastructure, applications, cloud)?		
3	Are dependencies between systems and cryptographic components systematically captured (dependency mapping)?		
3	Are quantum-vulnerable algorithms (RSA, ECC, DH) flagged in the inventory and prioritized by risk?		
3	Is the inventory updated regularly (at least quarterly)?		
3	Does a CBOM (Cryptographic Bill of Materials) exist for key systems?		
4	**Advanced**		
4	Are automated continuous-discovery tools deployed?		
4	Is the cryptographic inventory integrated into CMDB / asset management?		
4	Are supply chains and third-party vendors included in the inventory?		
4	Are SBOMs enriched with cryptographic components?		
5	**Excellent**		
5	Does a cryptographic digital twin exist for scenario analyses and migration simulations?		
5	Is the inventory synchronized in real time across all environments?		

5	Can you produce a complete report on your cryptographic exposure within 24 hours?		

3.2 Dimension 2 – Substitutability

The Dimension **Substitutability** assesses the ability to replace cryptographic algorithms, libraries, and protocols with alternative or newer methods. This is the core of crypto-agility: the technical and organizational capacity to perform an algorithm swap.

Substitutability is determined by several factors: the architecture of the systems (modular vs. monolithic), the APIs and abstraction layers used, the availability of PQC-capable libraries, and the existence of testing and rollback mechanisms.

Typical challenges for SMEs: Many older applications use hardcoded cryptographic methods without an abstraction layer. Proprietary systems often provide no way to replace cryptographic components independently. The lack of test environments complicates the safe evaluation of new algorithms. Moreover, developers are frequently not trained in crypto-agile design principles.

Level	Question / Indicator	Answer	Comments
1	**Initial**		
1	Is it known in which systems cryptography is hardcoded?		
1	Can cryptographic libraries be updated in principle?		
1	Is the substitutability of cryptographic methods a criterion when procuring new systems?		
2	**Aware**		
2	Are modular crypto architectures defined as a requirement for new systems?		
2	Are algorithm-independent APIs and abstraction layers being evaluated (e.g. PKCS#11, JCA/JCE)?		
2	Is PQC substitutability anchored in procurement policies?		
2	Are developers being trained in crypto-agile design principles?		
3	**Systematic**		
3	Can critical systems swap algorithms without code changes?		

3	Are hybrid implementations (classical + PQC) deployed in key systems?		
3	Are PQC-capable libraries in use (e.g. liboqs, BouncyCastle with PQC support)?		
3	Do rollback mechanisms exist for failed migrations?		
3	Is a test environment available for algorithm migrations?		
4	**Advanced**		
4	Can all production systems swap algorithms without operational interruption?		
4	Does a validation pipeline exist for algorithm migrations before going live?		
4	Are vendor dependencies for cryptographic libraries managed systematically?		
4	Is substitutability ensured across the entire supply chain?		
5	**Excellent**		
5	Is a fully automated algorithm swap across the entire infrastructure implemented?		
5	Are new PQC algorithms proactively evaluated in pilot environments?		
5	Can you respond organization-wide to a zero-day vulnerability within 72 hours?		
5	Is crypto-agile by design enforced as the standard architectural principle?		

3.3 Dimension 3 – Configurability

The Dimension **Configurability** assesses the extent to which cryptographic parameters and settings can be adjusted without code changes. Configurability enables rapid responses to new threats or regulatory requirements without having to go through lengthy development and release cycles.

Configurable parameters include, among others, permitted cipher suites, key lengths, protocol versions, certificate validation rules, and algorithm preferences. High configurability is a prerequisite for agile adaptation to changing requirements.

Typical challenges for SMEs: Many standard applications offer only limited configuration options for cryptography. The variety of different systems and platforms makes uniform configuration difficult. The absence of centralized control leads to inconsistent configurations. Changes are frequently made without formal change management, which increases risk.

Level	Question / Indicator	Answer	Comments
1	**Initial**		
1	Is it known which cryptographic parameters are configurable?		
1	Can cipher suites be adjusted / swapped in the most important systems?		
1	Does documentation of the current cryptographic configurations exist?		
2	**Aware**		
2	Are cryptographic parameters managed centrally via configuration files?		
2	Is a decommissioning plan for deprecated cipher suites in place?		
2	Is cipher suite negotiation defined as a requirement for new systems?		
2	Are the current cryptographic configurations documented?		
3	**Systematic**		
3	Does a central policy exist for permitted cipher suites and algorithms?		
3	Has formal change management been introduced for configuration changes?		
3	Are PQC-capable cipher suites configured (e.g. hybrid TLS 1.3)?		
3	Can all critical systems be configured without code changes?		
3	Are configuration standards documented and communicated?		

4	**Advanced**		
4	Is policy-as-code implemented for cryptographic configuration policies?		
4	Is continuous validation of configuration compliance in place?		
4	Are configuration deviations automatically detected and escalated?		
4	Is policy-driven algorithm selection implemented infrastructure-wide?		
5	**Excellent**		
5	Is dynamic, context-dependent configuration adjustment in place?		
5	Is organization-wide automated cipher suite optimization implemented?		
5	Can new configuration requirements be implemented within defined time windows?		
5	Are configurations continuously optimized for performance and security?		

3.4 Dimension 4 – Automation

The Dimension **Automation** assesses the degree of automation of cryptographic processes, particularly in the area of certificate and key lifecycle management. Manual processes are error-prone, difficult to scale, and too slow to respond to dynamic threat scenarios.

Automation encompasses the provisioning, rotation, renewal, and revocation of keys and certificates, as well as the automated monitoring of compliance with cryptographic policies and integration into DevOps processes.

Typical challenges for SMEs: Limited budgets hinder investment in certificate lifecycle management platforms. Manual certificate management regularly leads to outages caused by expired certificates. Missing integration between different systems prevents end-to-end automation. The transition from manual to automated processes requires initial investment in tooling and skill development.

Level	Question / Indicator	Answer	Comments
1	**Initial**		
1	Does an overview of all certificate expiry dates exist?		

1	Are keys and certificates managed manually?		
1	Is it known who is responsible for certificate renewal?		
2	**Aware**		
2	Does basic automation exist for certificate management?		
2	Are automated notifications set up for expiring certificates?		
2	Is scheduled key rotation implemented for critical systems?		
2	Are certificate lifecycle management platforms being evaluated?		
3	**Systematic**		
3	Is a central certificate lifecycle management (CLM) system implemented?		
3	Is key rotation automated according to defined policies?		
3	Are automated compliance checks performed for cryptographic policies?		
3	Are HSMs or cloud KMS deployed for secure key management?		
3	Does process documentation exist for cryptographic operations?		
4	**Advanced**		
4	Is end-to-end automation (provisioning, rotation, renewal, revocation) implemented?		
4	Is cryptographic automation integrated into CI/CD pipelines?		
4	Are errors automatically detected, logged, and escalated?		
4	Are automated rollback mechanisms implemented?		

5	**Excellent**		
5	Does a fully orchestrated, self-healing lifecycle management system exist?		
5	Are algorithm migrations (e.g. RSA→ML-KEM) performed automatically organization-wide?		
5	Is AI/ML-assisted anomaly detection integrated for cryptographic operations?		
5	Is continuous optimization performed based on performance and security metrics?		

3.5 Dimension 5 – Monitoring

The Dimension **Monitoring** assesses an organization's ability to continuously monitor the cryptographic state of its systems, detect deviations, and respond to them. Monitoring is the prerequisite for detecting vulnerabilities, measuring migration progress, and fulfilling regulatory requirements.

Cryptographic monitoring includes oversight of algorithms and protocol versions in use, detection of deprecated or insecure configurations, measurement of key strengths and certificate validity, and tracking of PQC migration progress.

Typical challenges for SMEs: Cryptographic events are often not separately captured or evaluated in standard log systems. Integrating cryptographic findings into existing SIEM systems requires additional configuration. The absence of metrics and KPIs makes it difficult to measure progress and report to management.

Level	Question / Indicator	Answer	Comments
1	**Initial**		
1	Are cryptographic events (TLS errors, certificate errors) captured in log systems?		
1	Does a basic awareness of cryptographic risks exist?		
1	Are responsibilities for cryptographic monitoring defined?		
2	**Aware**		
2	Are regular scans performed for deprecated cryptographic configurations?		

2	Are monitoring results included in security reports?		
2	Does a baseline exist for current cryptographic usage?		
2	Are cryptographic findings included in security reviews?		
3	**Systematic**		
3	Is dedicated cryptographic monitoring implemented (algorithm usage, key strengths, protocol versions)?		
3	Are cryptographic findings integrated into SIEM/SOC?		
3	Are compliance deviations automatically detected and reported?		
3	Is PQC migration progress measured using defined metrics?		
3	Does a dashboard exist for cryptographic status?		
4	**Advanced**		
4	Is real-time detection of cryptographic anomalies in place with automatic escalation?		
4	Are KPIs for cryptographic security defined and reported at management level?		
4	Are third-party vendors and supply chains included in monitoring?		
4	Does a complete cryptographic audit trail exist?		
5	**Excellent**		
5	Is Continuous Cryptographic Assurance established as a process?		
5	Are predictive analyses deployed for cryptographic risks?		
5	Is the effectiveness of monitoring itself measured and improved?		
5	Can you determine the organization-wide exposure level within hours when a new vulnerability emerges?		

3.6 Dimension 6 – Governance

The Dimension **Governance** assesses the organizational framework for cryptographic security: policies, responsibilities, training, regulatory compliance, and the strategic embedding of the topic within the organization. Without adequate governance, technical measures remain isolated solutions without lasting effect.

Governance creates the organizational framework within which technical measures become effective: clear responsibilities, documented policies, training programs, escalation paths, and the integration of cryptographic security into corporate management.

Typical challenges for SMEs: Cryptography is often regarded as a purely technical matter requiring no governance structures. The quantum threat is unknown to many decision-makers or is perceived as too abstract. Limited human resources make it difficult to establish dedicated roles and committees. Integration into existing management systems (e.g. ISMS) requires additional effort.

Level	Question / Indicator	Answer	Comments
1	**Initial**		
1	Does a basic cryptography policy exist?		
1	Are roles and responsibilities for cryptographic security defined?		
1	Are regulatory requirements for cryptography being tracked?		
2	**Aware**		
2	Has a RACI matrix been created for cryptographic responsibilities?		
2	Does an exception documentation process exist for cryptographic deviations?		
2	Are basic awareness training sessions on the quantum threat being conducted?		
2	Are regulatory requirements (NIS2, GDPR, sector-specific) actively tracked?		
3	**Systematic**		
3	Does an organization-wide policy framework for cryptography exist?		
3	Has an executive sponsor been designated for the quantum readiness program?		

3	Are vendor requirements for PQC readiness defined in procurement?		
3	Is crypto governance integrated into the ISMS (e.g. ISO 27001)?		
3	Are escalation paths defined for critical cryptographic findings?		
4	**Advanced**		
4	Does a cross-functional quantum readiness team exist?		
4	Are third-party vendor risks systematically assessed?		
4	Is risk-based prioritization for PQC migration implemented?		
4	Are KPIs for crypto-agility defined at management level?		
5	**Excellent**		
5	Is crypto governance embedded in the enterprise-wide risk strategy?		
5	Are policies automatically enforced (policy-as-code)?		
5	Is continuous compliance in place with automated attestation?		
5	Is proactive adaptation to new regulatory requirements taking place?		
5	Is the effectiveness of governance measured and continuously improved?		

4 Action Catalog: From Level to Level

The following Action Catalog describes concrete, actionable activities for each of the six dimensions that move an organization from one maturity level to the next. The measures are prioritized and formulated in a way that is comprehensible and actionable even for SMEs with limited resources. Each transition comprises four to six measures to be worked through in the order given.

4.1 Dimension 1 – Inventory

Inventorying forms the foundation of any PQC migration. Without a complete and current inventory of cryptographic assets, risk-based prioritization is not possible.

Transition	Measures
1 → 2	1. Designate a responsible person for cryptographic inventorying. 2. Conduct workshops with IT teams to identify cryptographic systems. 3. Document critical systems and their cryptographic dependencies in a table. 4. Evaluate discovery tools. 5. Consolidate initial findings in a central document.
2 → 3	1. Create a complete cryptographic inventory across all layers (infrastructure, applications, cloud). 2. Introduce dependency mapping to make dependencies between systems visible. 3. Define regular update cycles (at least quarterly). 4. Flag quantum-vulnerable algorithms (RSA, ECC, DH) in the inventory and prioritize by risk. 5. Create a CBOM (Cryptographic Bill of Materials) for key systems.
3 → 4	1. Implement automated continuous-discovery tools. 2. Enrich Software Bill of Materials (SBOM) with cryptographic components. 3. Implement risk-based prioritization (high-value assets first). 4. Include supply chains and third-party vendors in the inventory. 5. Integrate the inventory into CMDB/asset management.
4 → 5	1. Build a cryptographic digital twin for scenario analyses and migration simulations. 2. Ensure real-time synchronization across all environments (on-premises, cloud, hybrid). 3. Implement automatic linking of inventory changes with risk assessments. 4. Build the capability to produce a complete report on cryptographic exposure within 24 hours.

4.2 Dimension 2 – Substitutability

The substitutability of cryptographic components is the technical core of crypto-agility. Investments in modular architectures and abstraction layers pay dividends with every future cryptographic change.

Transition	Measures

1 → 2	1. Conduct an analysis of where cryptography is hardcoded. 2. Define modular architectures as a requirement for new systems. 3. Evaluate algorithm-independent APIs and abstraction layers (e.g. PKCS#11, JCA/JCE). 4. Include PQC substitutability in procurement policies. 5. Train developers in crypto-agile design principles.
2 → 3	1. Rebuild critical systems to support algorithm swap without code changes. 2. Introduce hybrid implementations (classical + PQC) in key systems. 3. Deploy PQC-capable libraries (e.g. liboqs, BouncyCastle with PQC support). 4. Implement rollback mechanisms for failed migrations. 5. Build a test environment for algorithm migrations.
3 → 4	1. Enable algorithm swap in all production systems without operational interruption. 2. Establish a validation pipeline for algorithm migrations before going live. 3. Systematically manage vendor dependencies for cryptographic libraries. 4. Ensure substitutability across the entire supply chain.
4 → 5	1. Implement fully automated algorithm swap across the entire infrastructure. 2. Proactive evaluation of new PQC algorithms in pilot environments. 3. Ensure the ability to respond to a zero-day vulnerability within 72 hours. 4. Enforce crypto-agile by design as the standard architectural principle.

4.3 Dimension 3 – Configurability

Configurability enables rapid responses to new threats or regulatory requirements. Centralized control and policy-as-code are key elements for efficient cryptographic configuration.

Transition	Measures
1 → 2	1. Conduct a stocktake of configurable cryptographic parameters. 2. Introduce centralized control via configuration files for critical systems. 3. Define cipher suite negotiation as a requirement for new systems. 4. Identify deprecated cipher suites and create a decommissioning plan. 5. Document current cryptographic configurations.
2 → 3	1. Define and implement a central policy for permitted cipher suites and algorithms. 2. Introduce formal change management for configuration changes. 3. Configure PQC-capable cipher suites (e.g. hybrid TLS 1.3). 4. Migrate all critical systems to configuration without code changes. 5. Document and communicate configuration standards.
3 → 4	1. Implement policy-as-code for cryptographic configuration policies. 2. Continuous validation of configuration compliance (compliance scans). 3. Automatic detection and escalation of configuration deviations. 4. Implement policy-driven algorithm selection infrastructure-wide.
4 → 5	1. Dynamic, context-dependent configuration adjustment (based on risk/threat landscape). 2. Organization-wide automated cipher suite optimization.

	3. Build the capability to implement new configuration requirements within defined time windows. 4. Continuous performance and security optimization of configurations.

4.4 Dimension 4 – Automation

Automation of cryptographic processes reduces sources of error, increases response speed, and enables scalability. Central certificate lifecycle management is the most important milestone on the path to full automation.

Transition	Measures
1 → 2	1. Consolidate an overview of all certificate expiry dates. 2. Introduce a first automation solution for certificate management (e.g. ACME, Let's Encrypt). 3. Set up automated notifications for expiring certificates. 4. Implement scheduled key rotation for critical systems. 5. Begin evaluation of CLM platforms.
2 → 3	1. Implement central certificate lifecycle management (CLM). 2. Automated key rotation according to defined policies. 3. Automated compliance checks for cryptographic policies. 4. Deploy HSMs or cloud KMS for secure key management. 5. Create process documentation for cryptographic operations.
3 → 4	1. End-to-end automation (provisioning, rotation, renewal, revocation). 2. Integration into CI/CD pipelines and DevOps processes. 3. Automatic error detection, logging, and escalation. 4. Implement automated rollback mechanisms. 5. Integrate cryptographic automation into cloud environments.
4 → 5	1. Fully orchestrated and self-healing lifecycle management. 2. Continuous optimization based on performance and security metrics. 3. Automated algorithm migrations (e.g. RSA→ML-KEM) organization-wide without manual intervention. 4. Integrate AI/ML-assisted anomaly detection and predictive analytics.

4.5 Dimension 5 – Monitoring

Monitoring provides the data basis for informed decisions, compliance evidence, and measuring migration progress. Without continuous monitoring, the cryptographic security posture remains opaque.

Transition	Measures
1 → 2	1. Capture cryptographic events in log systems (TLS errors, certificate errors, handshake issues). 2. Perform regular scans for deprecated cryptographic configurations. 3. Include monitoring results in security reports. 4. Establish a baseline for current cryptographic usage.

	5. Define responsibilities for cryptographic monitoring.
2 → 3	1. Implement dedicated cryptographic monitoring (algorithm usage, key strengths, protocol versions). 2. Integrate cryptographic findings into SIEM/SOC. 3. Automatic detection and reporting of compliance deviations. 4. Measure PQC migration progress using defined metrics. 5. Create a dashboard for cryptographic status.
3 → 4	1. Real-time detection of cryptographic anomalies with automatic escalation. 2. Define and report KPIs for cryptographic security at management level. 3. Include third-party vendors and supply chains in monitoring. 4. Maintain a complete cryptographic audit trail for all operations.
4 → 5	1. Establish Continuous Cryptographic Assurance as a process. 2. Deploy predictive analytics for cryptographic risks. 3. Measure and improve the effectiveness of monitoring itself. 4. Build the capability to determine the organization-wide exposure level within hours when a new vulnerability emerges.

4.6 Dimension 6 – Governance

Governance creates the organizational framework without which technical measures cannot be sustainably effective. Executive sponsorship, clear responsibilities, and integration into existing management systems are decisive success factors.

Transition	Measures
1 → 2	1. Document a cryptography policy. 2. Create a RACI matrix for roles and responsibilities. 3. Track regulatory requirements (NIS2, GDPR, sector-specific). 4. Introduce an exception documentation process. 5. Conduct basic awareness training sessions.
2 → 3	1. Establish and communicate an organization-wide policy framework. 2. Secure an executive sponsor for the quantum readiness program. 3. Define vendor requirements for PQC readiness in procurement. 4. Integrate crypto governance into the ISMS (ISO 27001). 5. Define escalation paths for critical cryptographic findings.
3 → 4	1. Establish a cross-functional quantum readiness team. 2. Systematically assess third-party vendor risks. 3. Implement risk-based prioritization for PQC migration. 4. Define KPIs for crypto-agility at management level. 5. Centralized management of deviations and exceptions.
4 → 5	1. Embed crypto governance into the enterprise-wide risk strategy. 2. Automatically enforce policies (policy-as-code). 3. Continuous compliance with automated attestation. 4. Proactive adaptation to new regulatory requirements.

	5. Measure and improve the effectiveness of governance.

5 PQC Readiness Roadmap

The following roadmap translates the results of the maturity assessment into a time-structured implementation plan. The four phases correspond to the transitions between maturity levels and are aligned with the milestones of the EU PQC Roadmap[19]. The timeframes are intended as reference values for mid-sized organizations and may vary depending on the starting position and available resources.

5.1 Phase 1: Building Foundations (Level 1 → 2, Timeframe: 3–6 months)

The first phase lays the organizational and knowledge-related foundations for the PQC migration. The focus is on awareness building, an initial inventory, and establishing basic responsibilities. This phase is also feasible with limited resources and should be started without delay.

Core measures:

Building awareness and establishing executive awareness: Senior management must understand the relevance of the quantum threat. Short briefings and decision papers help put the topic on the agenda.

Designating a Quantum Champion: A person or role is defined as the central point of contact for PQC readiness. This person drives the initiative forward and coordinates activities.

Foundational awareness training: IT staff and decision-makers are informed about the quantum threat, HNDL risks, and the fundamentals of PQC migration.

Initial cryptographic inventory: In workshops with IT teams, the most important cryptographic systems and dependencies are identified and documented.

Documenting the quantum threat baseline: The current cryptographic exposure is recorded, particularly with regard to quantum-vulnerable algorithms and HNDL risks.

Reviewing regulatory requirements: The regulatory requirements relevant to the organization (NIS2, GDPR, sector-specific requirements) are identified and documented.

Regulatory Alignment: *This phase should be completed by at the latest* ***31.12.2026****, in order to meet the first milestone of the EU PQC Roadmap.*

5.2 Phase 2: Systematization (Level 2 → 3, Timeframe: 6–18 months)

The second phase converts the foundations established in Phase 1 into systematic, documented processes. The focus is on completing the cryptographic inventory, establishing formal governance structures, and initial technical pilot projects. Reaching Level 3 represents the critical threshold for regulatory compliance.

Core measures:

Complete cryptographic inventory: The inventory begun in Phase 1 is completed across all layers (infrastructure, applications, cloud). Dependency mapping makes dependencies visible.

Securing an executive sponsor: A member of senior management assumes sponsorship of the PQC program and provides the necessary resources.

Establishing a formal PQC program: Objectives, milestones, budget, and responsibilities are defined and documented in a formal program.

Launching hybrid TLS pilots: Hybrid TLS configurations (classical + PQC) are implemented as a pilot in selected systems to gather experience and test compatibility.

Implementing CLM: A central Certificate Lifecycle Management system is introduced to enable automated management of certificates and keys.

Integrating crypto governance into the ISMS: Cryptographic policies and processes are integrated into the existing information security management system (e.g., ISO 27001).

Regulatory Alignment: *This phase should be completed by at the latest **31.12.2028** completed. The EU PQC Roadmap requires only inventory, risk analysis, and planning ("First Steps") by the end of 2026, not the achievement of systematic maturity. The UK NCSC also allows until 2028 for the discovery phase. Reaching Level 3 creates a sound foundation for meeting the regulatory requirements under NIS2 and the EU PQC Roadmap – however, the concrete compliance assessment must always be performed on an organization-specific basis.*

5.3 Phase 3: Operational Maturity (Level 3 → 4, Timeframe: 12–24 months)

The third phase builds on the systematic foundations and advances the organization to an advanced maturity level. The focus is on automation, integration into operational management, and the inclusion of the supply chain. In this phase, PQC migrations are carried out in production systems.

Core measures:

Automated inventory and compliance: Continuous discovery tools replace manual inventory processes. Automated compliance checks monitor adherence to cryptographic policies.

PQC pilot deployments in production: Selected production systems are migrated to PQC algorithms, starting with the most critical use cases.

Quantitative KPIs and management reporting: Measurable metrics for the cryptographic security posture and migration progress are defined and reported to management on a regular basis.

Supply chain integration: Third-party providers and suppliers are included in the PQC readiness assessment. Requirements for cryptographic security are anchored in contracts and procurement processes.

Risk-based migration prioritization: Migration is prioritized according to HNDL risk: systems handling long-lived secrets with high protection requirements are migrated first.

5.4 Phase 4: Excellence (Level 4 → 5, Timeframe: 24–36 months)

The fourth phase brings the organization to the highest maturity level. The focus is on full automation, proactive threat analysis, and the embedding of crypto-agility as a core organizational competency. This phase addresses the long-term EU milestone of 2035.

Core measures:

Full automation and orchestration: All cryptographic processes – from inventory through configuration to migration – are fully automated and orchestrated.

Crypto-agile by design as a principle: Crypto-agility is established as a standard architectural principle. All new systems are designed to be crypto-agile from the outset.

Predictive analytics: AI/ML-supported tools enable predictive risk analyses and the early detection of cryptographic trends and threats.

Continuous Cryptographic Assurance: The cryptographic security posture is continuously and automatically verified. Attestations are generated automatically.

Digital twin for migration simulations: A cryptographic digital twin enables the simulation of migration scenarios and the analysis of impacts before changes are deployed to production.

6 Overall Assessment

The following table summarizes the assessment results across all six dimensions. Enter the maturity level achieved for each dimension. The Overall Maturity Level corresponds – in accordance with the weakest-link principle – to the lowest individual value.

Dimension	Level Achieved	Target Level
1 – Inventory		
2 – Substitutability		
3 – Configurability		
4 – Automation		
5 – Monitoring		
6 – Governance		
Overall Maturity Level		

Recommendation: ***Level 3 (Systematic)*** should be pursued as the **minimum target**, in order to meet the regulatory requirements under NIS2, the EU PQC Roadmap, and the BSI Joint Statement. Achieving Level 3 corresponds to NIST CSWP 39 Tier 3 (Standardized), which is defined as the minimum for regulatory compliance.

Organizations currently below Level 3 should use the **Roadmap (Section 5)** and the **Measures Catalog (Section 4)** as a guide to incrementally reach the minimum level. Alignment with the EU milestones (2026/2030/2035) provides the temporal orientation framework.

7 Recommendations for SMEs

Small and medium-sized enterprises face particular challenges in PQC migration: limited budgets, scarce personnel resources, and often a lack of specialist knowledge in the field of cryptography. The following recommendations address these challenges and outline pragmatic paths toward improving crypto-agility.

7.1 Pragmatic Start: Level 1 → 2 is Achievable

The transition from Level 1 to Level 2 requires no major investment. The essential measures – awareness building, an initial inventory, designating a responsible person – can be implemented with existing resources. The most important step is simply to begin. Even an incomplete inventory is better than none, as it creates the foundation for all further measures.

7.2 Commodity IT: PQC Migration via Vendor Updates

A significant portion of the cryptographic migration will happen automatically for SMEs through vendor updates. Browsers, operating systems, and cloud services are migrating to PQC standards without the end user needing to intervene. Google Chrome and Mozilla Firefox already support hybrid TLS with ML-KEM. Microsoft and AWS are integrating PQC into their cloud platforms. For standard IT infrastructure, this means: regular updates and patches are the simplest and most cost-effective migration strategy.

7.3 Focus on Custom Software and Specialized Systems

The greatest need for action lies in custom-developed software, embedded systems, legacy applications, and specialized industry solutions. These systems may not receive automatic PQC updates and must be actively migrated. Here, early inventory and risk analysis is especially important in order to realistically estimate migration effort and plan ahead in a timely manner.

7.4 Cost-Benefit: Weighing HNDL Risk Against Migration Costs

Not all data and systems are equally worthy of protection. SMEs should prioritize the migration sequence according to HNDL risk: systems that process long-lived secrets (e.g., customer data, intellectual property, contracts) should be migrated first. Systems with short-lived data and low protection requirements can be addressed later. This prioritization enables efficient allocation of limited resources.

7.5 Leveraging External Support

SMEs do not have to manage the PQC migration on their own. Numerous resources are available: the BSI provides recommendations and guidelines for cryptographic security. Industry associations and chambers of commerce offer information and networking. Managed Security Service Providers (MSSPs) can support operational implementation. Funding programs at the federal and EU level can reduce financial barriers.

7.6 Identifying Quick Wins

Some measures offer immediate security gains with minimal effort: update TLS configurations and disable insecure cipher suites. Automate certificate management and introduce key rotation for critical systems. Keep software and operating systems up to date to benefit from vendors' PQC updates. These quick wins improve the security posture immediately and create momentum for further measures.

8 References

[1] National Institute of Standards and Technology (NIST), Post Quantum Cryptography: FIPS Approved, 2024, https://csrc.nist.gov/projects/post-quantum-cryptography

[2] Federal Office for Information Security (BSI), Joint Statement on the Transition to Post-Quantum Cryptography, 2025, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf

[3] European Commission, Coordinated Implementation Roadmap for the Transition to Post Quantum Cryptography, 2024, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[4] National Institute of Standards and Technology (NIST), NIST CSWP 39: Considerations for Achieving Cryptographic Agility, December 2025, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf

[5] European Union, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2), Article 21(2)(h)

[6] European Commission, Implementing Regulation (EU) 2024/2690, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2690

[7] European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 2024, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[8] European Union, Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[9] European Union, Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[10] European Union, General Data Protection Regulation (GDPR), Article 32, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[11] Federal Office for Information Security (BSI), Quantentechnologien und quantensichere Kryptografie – Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, 2024, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien/quantentechnologien_node.html

[12] National Security Agency (NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2024, https://media.defense.gov/2022/Sep/07/2003074170/-1/-1/0/CSI-CNSA-2.0-FACT-SHEET.PDF

[13] UK National Cyber Security Centre (NCSC), Timelines for Migration to Post-Quantum Cryptography, 2025, https://www.ncsc.gov.uk/whitepaper/timelines-for-migration-to-post-quantum-cryptography

[14] BSI, HV-Benchmark kompakt, 2024, https://www.bsi.bund.de

[15] BSI, HV-Benchmark: Bewertungsmethodik, 2024, https://www.bsi.bund.de

[16] Näther, K., et al., CAMM – Crypto-Agility Maturity Model, 2023, https://arxiv.org/html/2202.07645v3

[17] National Institute of Standards and Technology (NIST), NIST CSWP 39: Considerations for Achieving Cryptographic Agility, December 2025, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf