Q-DAY READINESS ASSESSMENT FRAMEWORK

Standortbestimmung zur Krypto-Agilität und PQC-Readiness

Version 1.0
März 2026

Inés Atug
ines@nointernet.de

Erstellt unter Zuhilfenahme KI-gestützter Werkzeuge.

Inhaltsverzeichnis

1 EINLEITUNG 3

1.1 Die Bedrohung durch den Q-Day 3

1.2 Warum Krypto-Agilität? 4

1.3 Regulatorischer Kontext 4

1.4 Zielsetzung des Frameworks 6

2 METHODISCHE GRUNDLAGEN 7

2.1 Der HV-Benchmark kompakt des BSI 7

2.2 Das CAMM-Reifegradmodell 7

2.3 NIST CSWP 39 Maturity Model 8

2.4 Übertragung auf das Q-Day Readiness Framework 8

2.5 Durchführung der Bewertung 9

3 DIE SECHS DIMENSIONEN DER KRYPTO-AGILITÄT 11

3.1 Dimension 1 – Inventory 11

3.2 Dimension 2 – Substitutability 13

3.3 Dimension 3 – Configurability 15

3.4 Dimension 4 – Automation 16

3.5 Dimension 5 – Monitoring 18

3.6 Dimension 6 – Governance 20

4 MAßNAHMENKATALOG: VON STUFE ZU STUFE 23

4.1 Dimension 1 – Inventory 23

4.2 Dimension 2 – Substitutability 24

4.3 Dimension 3 – Configurability 24

4.4 Dimension 4 – Automation 25

4.5 Dimension 5 – Monitoring 26

4.6 Dimension 6 – Governance 26

5 ROADMAP ZUR PQC-READINESS 28

5.1 5.1 Phase 1: Grundlagen schaffen (Stufe 1 → 2, Zeitrahmen: 3–6 Monate) 28

5.2 Phase 2: Systematisierung (Stufe 2 → 3, Zeitrahmen: 6–12 Monate) 28

5.3 Phase 3: Operative Reife (Stufe 3 → 4, Zeitrahmen: 12–24 Monate) 29

5.4 Phase 4: Exzellenz (Stufe 4 → 5, Zeitrahmen: 24–36 Monate) 30

6 GESAMTBEWERTUNG 31

7 EMPFEHLUNGEN FÜR KMU 32

7.1 Pragmatischer Einstieg: Stufe 1 → 2 ist machbar 32

7.2 Commodity-IT: PQC-Migration durch Vendor-Updates 32

7.3 Fokus auf Custom-Software und spezielle Systeme 32

7.4 Kosten-Nutzen: HNDL-Risiko gegen Migrationskosten abwägen 32

7.5 Externe Unterstützung nutzen 32

7.6 Quick Wins identifizieren 32

8 QUELLENVERZEICHNIS 34

1 Einleitung

1.1 Die Bedrohung durch den Q-Day

Der Begriff **Q-Day** bezeichnet den Zeitpunkt, an dem ein kryptografisch relevanter Quantencomputer (*engl. Cryptographically Relevant Quantum Computer, CRQC*) verfügbar sein wird, der in der Lage ist, die heute weit verbreiteten asymmetrischen Verschlüsselungsverfahren zu brechen. Experten schätzen diesen Zeitpunkt auf den Zeitraum zwischen 2030 und 2040, wobei sich die Prognosen durch technologische Fortschritte stetig nach vorne verschieben.

Die mathematische Grundlage dieser Bedrohung bildet **Shor's Algorithmus**, der auf einem hinreichend leistungsfähigen Quantencomputer die Faktorisierung großer Zahlen und die Berechnung diskreter Logarithmen in polynomieller Zeit ermöglicht. Damit wären die Verfahren RSA, ECC (Elliptic Curve Cryptography) und Diffie-Hellman (DH), die heute das Rückgrat nahezu aller digitalen Kommunikation bilden, innerhalb kurzer Zeit kompromittierbar. Symmetrische Verfahren wie AES können ebenfalls betroffen sein: **Grover's Algorithmus** halbiert die effektive Schlüssellänge, sodass AES-128 nur noch die Sicherheit von 64 Bit bieten würde. Die Empfehlung lautet daher, mindestens AES-256 einzusetzen.

Als Reaktion auf diese Bedrohung hat das National Institute of Standards and Technology (NIST) im August 2024 die ersten Post-Quantum-Kryptografie-Standards finalisiert[1]: **FIPS 203 (ML-KEM)** für den Schlüsselaustausch basierend auf dem CRYSTALS-Kyber-Algorithmus, **FIPS 204 (ML-DSA)** für digitale Signaturen basierend auf CRYSTALS-Dilithium sowie **FIPS 205 (SLH-DSA)** für zustandslose hashbasierte Signaturen (SPHINCS+). Diese Standards bilden die Grundlage für die Migration zu quantensicherer Kryptografie.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt in einem gemeinsamen Statement mit der französischen ANSSI und der niederländischen NLNCSA den Einsatz hybrider Lösungen[2], bei denen klassische und post-quantensichere Verfahren kombiniert werden. Dieser Ansatz bietet Schutz sowohl gegen heutige als auch gegen zukünftige Angriffe.

Die EU hat im Juni 2025 eine koordinierte PQC-Roadmap veröffentlicht[3], die drei zentrale Meilensteine definiert: Bis **31.12.2026** sollen nationale Roadmaps erstellt, kryptografische Inventare aufgebaut und Awareness-Programme gestartet werden. Bis **31.12.2030** sollen alle hochkritischen Anwendungsfälle migriert sein. Bis **31.12.2035** soll die vollständige Migration aller verbleibenden Systeme abgeschlossen sein.

Von besonderer Dringlichkeit ist die sogenannte **HNDL-Bedrohung (Harvest Now, Decrypt Later)**: Angreifer – insbesondere staatliche Akteure – fangen bereits heute verschlüsselte Daten ab und speichern diese, um sie zu entschlüsseln, sobald ein CRQC verfügbar ist. Das bedeutet: Vertrauliche Daten, die heute übertragen werden, sind bereits jetzt gefährdet, wenn ihre Aufbewahrungsdauer über den erwarteten Q-Day hinausreicht.

---

[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

Das **HNDL Exposure Window** berechnet sich als: Datenaufbewahrungsdauer minus Zeit bis zum Verfügbarwerden eines CRQC. Ist dieser Wert größer als null, sind die betreffenden Daten potenziell gefährdet. Für Organisationen, die mit langlebigen Geheimnissen arbeiten – etwa Gesundheitsdaten, Staatsgeheimnisse, geistiges Eigentum oder langfristige Verträge – besteht daher unmittelbarer Handlungsbedarf.

1.2 Warum Krypto-Agilität?

Krypto-Agilität (*engl. Crypto-Agility*) bezeichnet nach NIST-Definition die Fähigkeit einer Organisation, kryptografische Algorithmen, Protokolle, Schlüssel und Zertifikate effizient und ohne wesentliche Betriebsunterbrechungen auszutauschen oder zu aktualisieren[4]. Es handelt sich dabei ausdrücklich nicht um ein einmaliges Migrationsprojekt, sondern um eine **dauerhafte organisatorische Fähigkeit**, die es ermöglicht, auf neue Bedrohungen, Schwachstellen oder regulatorische Anforderungen zeitnah zu reagieren.

Das NIST Cybersecurity White Paper 39 (CSWP 39) vom Dezember 2025 erhebt Krypto-Agilität zum fundamentalen Design-Prinzip[4]. Das Dokument definiert sechs Kernfähigkeiten, die eine krypto-agile Organisation aufweisen muss:

1. Automated Discovery: Automatisierte Erkennung und Inventarisierung aller kryptografischen Assets über die gesamte Infrastruktur hinweg.

2. Risk-Based Prioritization: Risikobasierte Priorisierung der identifizierten kryptografischen Abhängigkeiten zur gezielten Ressourcenallokation.

3. Continuous Measurement: Kontinuierliche Messung und Überwachung der kryptografischen Sicherheitslage mittels definierter Metriken und KPIs.

4. Agility Testing: Regelmäßige Tests der Fähigkeit, kryptografische Komponenten auszutauschen und Migrationen durchzuführen.

5. Executive Reporting: Strukturierte Berichterstattung an die Geschäftsleitung über den kryptografischen Sicherheitsstatus und Migrationsfortschritt.

6. Machine-Readable Policies: Maschinenlesbare Richtlinien, die eine automatisierte Durchsetzung kryptografischer Standards ermöglichen.

Die Dringlichkeit der PQC-Migration unterstreicht, dass Krypto-Agilität keine optionale Zukunftsinvestition ist, sondern eine grundlegende Voraussetzung für nachhaltige IT-Sicherheit. Organisationen, die heute nicht in Krypto-Agilität investieren, werden später mit deutlich höheren Kosten und Risiken konfrontiert sein.

1.3 Regulatorischer Kontext

Die Anforderungen an kryptografische Sicherheit und PQC-Readiness werden durch ein zunehmend dichtes Geflecht regulatorischer Vorgaben geprägt. Für europäische Organisationen sind insbesondere folgende Regelwerke relevant:

NIS2-Richtlinie (EU) 2022/2555: Artikel 21(2)(h) verpflichtet wesentliche und wichtige Einrichtungen, Richtlinien und Verfahren für den Einsatz von Kryptografie zu implementieren[5]. Die zugehörige EU Implementing Regulation 2024/2690 konkretisiert diese Anforderung und

[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)

verlangt explizit, dass Kryptografie-Richtlinien auf dem Prinzip der Krypto-Agilität basieren müssen[6].

EU PQC Roadmap (Juni 2025): Die NIS Cooperation Group hat eine koordinierte Implementierungs-Roadmap für den Übergang zu Post-Quantum-Kryptografie veröffentlicht[7]. Diese definiert drei verbindliche Meilensteine: Bis 31.12.2026 Inventarisierung und Roadmap-Erstellung, bis 31.12.2030 Migration hochkritischer Systeme, bis 31.12.2035 vollständige Migration.

DORA (Digital Operational Resilience Act): Für den Finanzsektor verschränkt DORA die Anforderungen an die operationale Resilienz mit kryptografischer Sicherheit[8]. Finanzinstitute müssen sicherstellen, dass ihre IKT-Systeme gegen aufkommende Bedrohungen – einschließlich Quantenangriffe – geschützt sind.

Cyber Resilience Act (CRA): Der CRA fordert für digitale Produkte mit digitalen Elementen die Berücksichtigung des Stands der Technik bei kryptografischen Maßnahmen[9]. Ab 2027 wird quantum-sichere Kryptografie zunehmend als Stand der Technik gelten.

DSGVO „Stand der Technik“: Artikel 32 der DSGVO[10] verlangt technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik. Sobald PQC-Standards als Stand der Technik gelten, werden Organisationen, die weiterhin ausschließlich auf quantenanfällige Verfahren setzen, ihre Compliance-Pflichten verletzen.

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography (2025): Das gemeinsame Statement von 21 europäischen Sicherheitsbehörden empfiehlt hybride Lösungen und fordert Schutz gegen HNDL-Angriffe spätestens bis Ende 2030[11]. Detaillierte Transitionspläne für PKI-Infrastrukturen sollen im gleichen Zeitrahmen vorliegen.

CNSA 2.0 (USA): Die NSA hat mit der Commercial National Security Algorithm Suite 2.0 verbindliche Zeitlinien für US-Regierungsbehörden und deren Zulieferer definiert[12]: Ab 2025 PQC für Software-Signaturen, ab 2026 für VPNs und Router, bis 2030 Auslaufen von Legacy-Systemen und bis 2035 vollständig quantenresistente National Security Systems.

---

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

[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

UK NCSC Roadmap (2025): Das britische National Cyber Security Centre hat eine dreistufige Roadmap veröffentlicht[13]: Discovery & Plan bis 2028, Prioritize & Pilot von 2028 bis 2031 und Complete Adoption von 2031 bis 2035.

1.4 Zielsetzung des Frameworks

Das vorliegende Q-Day Readiness Assessment Framework verfolgt das Ziel, Organisationen – insbesondere kleinen und mittleren Unternehmen (KMU) – ein praxistaugliches Werkzeug zur systematischen Selbstbewertung ihrer Krypto-Agilität und PQC-Readiness bereitzustellen.

Das Framework basiert auf folgenden Grundprinzipien:

Sechs Dimensionen: Das Bewertungsmodell umfasst die Dimensionen Inventory, Substitutability, Configurability, Automation, Monitoring und Governance. Diese Dimensionen decken sowohl technische als auch organisatorische Aspekte der kryptografischen Reife ab.

Fünf Reifegradstufen: Jede Dimension wird anhand eines fünfstufigen Reifegradmodells (Stufe 1 bis 5) bewertet, das aufeinander aufbauende Fähigkeiten beschreibt.

KMU-Tauglichkeit: Das Framework ist so gestaltet, dass es auch ohne umfangreiche Kryptografie-Expertise angewendet werden kann. Die Fragen sind praxisnah formuliert und beziehen sich auf konkrete, überprüfbare Sachverhalte.

Klare Standortbestimmung: Das Ergebnis der Bewertung liefert eine klare Positionsbestimmung auf der Reifegrad-Skala und identifiziert Handlungsbedarfe.

Priorisierte Maßnahmen: Der integrierte Maßnahmenkatalog (Kapitel 4) und die Roadmap (Kapitel 5) überführen die Bewertungsergebnisse in konkrete, umsetzbare Handlungsempfehlungen.

Regulatorisches Alignment: Die Reifegradstufen und die Roadmap sind an den Meilensteinen der EU PQC Roadmap (2026/2030/2035) ausgerichtet, sodass Organisationen ihre Fortschritte an den regulatorischen Zeitlinien messen können.

[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

2 Methodische Grundlagen

Das Q-Day Readiness Assessment Framework kombiniert bewährte Methoden aus drei etablierten Frameworks zu einem integrierten Bewertungsansatz. Die methodischen Grundlagen werden im Folgenden erläutert.

2.1 Der HV-Benchmark kompakt des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem HV-Benchmark kompakt ein Instrument zur Bewertung der Hochverfügbarkeit von IT-Infrastrukturen entwickelt[14]. Die Methodik zeichnet sich durch folgende Merkmale aus, die für das vorliegende Framework adaptiert wurden:

Stufenbasierte Bewertung: Der HV-Benchmark verwendet ein Stufenmodell, bei dem jede Stufe auf der vorherigen aufbaut. Eine höhere Stufe setzt die Erfüllung aller Anforderungen der darunter liegenden Stufen voraus. Dieses Prinzip gewährleistet eine konsistente und nachvollziehbare Bewertung.

Prinzip der schwächsten Kette: Die Gesamtbewertung wird durch das schwächste Glied bestimmt[15]. Wenn eine Organisation in fünf Dimensionen Stufe 4 erreicht, aber in einer Dimension nur Stufe 2, beträgt der Gesamtreifegrad 2. Dieses Prinzip verhindert, dass Schwächen in einzelnen Bereichen durch Stärken in anderen kompensiert werden.

Indikatoren-basiert: Die Bewertung erfolgt anhand konkreter, überprüfbarer Indikatoren (Fragen), nicht anhand subjektiver Einschätzungen. Jede Frage ist mit Ja, Teilweise oder Nein beantwortbar.

Transparenz und Vergleichbarkeit: Durch die standardisierte Methodik sind die Ergebnisse transparent und ermöglichen Vergleiche über die Zeit sowie zwischen Organisationen.

2.2 Das CAMM-Reifegradmodell

Das **Crypto-Agility Maturity Model (CAMM)** von Näther et al. ist das erste wissenschaftlich fundierte Reifegradmodell speziell für Krypto-Agilität[16]. Es definiert fünf Reifegrade (Level 0 bis 4) und strukturiert die Anforderungen in drei Kategorien:

Knowledge (K): Wissensbasierte Anforderungen, die das Verständnis und die Dokumentation kryptografischer Abhängigkeiten betreffen (z. B. Inventarisierung, Algorithmus-IDs, Performance-Bewusstsein, Sicherheitsbewertung).

Process (P): Prozessbasierte Anforderungen, die organisatorische Abläufe und Verfahren betreffen (z. B. Aktualisierbarkeit, Reversibilität, Richtlinien, Tests, Automatisierung, Skalierbarkeit).

System Property (S): Systemeigenschaften, die in der Architektur und Implementierung verankert sein müssen (z. B. Erweiterbarkeit, kryptografische Modularität, Algorithmus-Ausschluss, Hardware-Modularität).

Die fünf CAMM-Level bauen aufeinander auf: **Level 0 (Initial)** beschreibt Systeme, in denen kryptografische Agilität nicht möglich ist. **Level 1 (Possible)** bedeutet, dass grundlegende Voraussetzungen für Agilität gegeben sind. **Level 2 (Prepared)** setzt modulare Architektur und

[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

Verhandlungsfähigkeit voraus. **Level 3 (Practiced)** erfordert erprobte Prozesse und Richtlinien. **Level 4 (Sophisticated)** repräsentiert vollautomatisierte, skalierbare Krypto-Agilität.

Warum CAMM allein nicht ausreicht: Ein wesentlicher Grund für die Entwicklung des vorliegenden Frameworks liegt in der bewussten Scope-Begrenzung des CAMM. Das CAMM wurde konzipiert, um die Krypto-Agilität eines einzelnen Software-Systems oder einer bestimmten IT-Landschaft zu bewerten – die Autoren formulieren explizit: „a maturity model for determining the state of crypto-agility of a given software or IT system". Die Anforderungen und Reifegrade beziehen sich auf technische Systemeigenschaften wie Modularität, Erweiterbarkeit und Algorithmus-Verhandlung auf Produktebene. Organisatorische Dimensionen – etwa Governance-Strukturen, unternehmensweite Richtlinien, regulatorische Compliance, Lieferkettenmanagement oder die Fähigkeit, eine PQC-Migration über Hunderte heterogener Systeme hinweg zu koordinieren – liegen außerhalb des CAMM-Scope. Eine Organisation kann durchaus einzelne Systeme mit hohem CAMM-Level betreiben und dennoch als Ganzes nicht in der Lage sein, auf eine neue kryptografische Bedrohung zeitnah zu reagieren, weil es an zentraler Steuerung, Überwachung, Automatisierung oder Governance fehlt. Das Q-Day Readiness Assessment Framework schließt diese Lücke, indem es die technischen Aspekte des CAMM um die organisatorischen Dimensionen Monitoring, Automation und Governance ergänzt und damit eine ganzheitliche Standortbestimmung auf Unternehmensebene ermöglicht – mit besonderem Fokus auf die Anforderungen von KMU.

2.3 NIST CSWP 39 Maturity Model

Das NIST Cybersecurity White Paper 39 (CSWP 39) vom Dezember 2025[17] definiert ein vierstufiges Reifegradmodell für Krypto-Agilität, das als ergänzende Referenz für das vorliegende Framework dient:

Tier	Beschreibung
Tier 1 – Reactive	Kein formales Ownership für kryptografische Sicherheit. Ad-hoc-Bewusstsein, kein Inventar. Reaktives Handeln nur bei Vorfällen.
Tier 2 – Managed	CISO-Bewusstsein vorhanden, teilweises Inventar erstellt. Erste Dokumentation und grundlegende Prozesse etabliert.
Tier 3 – Standardized	Automatisierte Discovery, kontinuierliches Monitoring, Executive-KPIs definiert. Minimum für regulatorische Compliance.
Tier 4 – Adaptive	Kontinuierliche Optimierung, nachgewiesene Agilität durch regelmäßige Tests, Integration in Enterprise Risk Management.

2.4 Übertragung auf das Q-Day Readiness Framework

Das vorliegende Framework kombiniert die Stärken der drei beschriebenen Methoden: die stufenbasierte, indikatorengestützte Bewertungsmethodik des BSI HV-Benchmarks, die sechs krypto-agilitätsspezifischen Dimensionen und die wissenschaftliche Fundierung des CAMM-

[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

Modells sowie die praxisorientierten Anforderungen und die Compliance-Perspektive des NIST CSWP 39.

Die folgende Tabelle definiert die fünf Reifegradstufen des Q-Day Readiness Frameworks:

Stufe	Bezeichnung	Beschreibung
1	**Initial**	Kein oder nur rudimentäres Bewusstsein für kryptografische Abhängigkeiten. Kein Inventar, keine dokumentierten Prozesse, keine dedizierte Verantwortlichkeit. Kryptografie wird als selbstverständlich vorausgesetzt und nicht aktiv gemanagt.
2	**Bewusst**	Grundlegendes Bewusstsein für die Quantenbedrohung vorhanden. Erste Inventarisierungsmaßnahmen eingeleitet, kritische Systeme identifiziert. Verantwortlichkeiten sind benannt, erste Dokumentation existiert. Der Weg zur Krypto-Agilität ist als Bedarf erkannt.
3	**Systematisch**	Vollständiges kryptografisches Inventar vorhanden. Formale Prozesse und Richtlinien etabliert. Systematische Bewertung und priorisierte Migrationsstrategie. Hybrid-Implementierungen in kritischen Systemen. Regelmäßiges Monitoring und Reporting. Dies ist der kritische Schwellenwert für regulatorische Compliance.
4	**Fortgeschritten**	Weitgehend automatisierte kryptografische Prozesse. Continuous Discovery und Compliance-Überwachung. Algorithmus-Austausch ohne Betriebsunterbrechung möglich. Integration in Enterprise Risk Management und Lieferketten-Management.
5	**Exzellent**	Vollständig orchestrierte, selbstoptimierende Krypto-Agilität. Proaktive Evaluierung neuer Algorithmen und Bedrohungen. Prädiktive Analysen. Nachgewiesene Fähigkeit, bei Zero-Day-Schwachstellen innerhalb definierter Zeitfenster organisationsweit zu reagieren. Krypto-Agilität als integraler Bestandteil der Unternehmenskultur.

Stufe 3 (Systematisch) bildet den **kritischen Schwellenwert**: Organisationen, die dieses Niveau erreichen, verfügen über die grundlegenden Fähigkeiten, die regulatorische Compliance erfordern, und sind in der Lage, eine geordnete PQC-Migration durchzuführen. Stufe 3 korrespondiert mit CAMM Level 2–3 und NIST Tier 3 (Standardized).

2.5 Durchführung der Bewertung

Die Bewertung erfolgt dimensionsweise anhand der in Kapitel 3 definierten Fragen. Für jede Dimension wird die erreichte Reifegradstufe ermittelt, indem geprüft wird, ob die Anforderungen der jeweiligen Stufe erfüllt sind. Es gilt das **Prinzip der schwächsten Kette**: Eine Stufe gilt nur dann als erreicht, wenn alle Fragen dieser Stufe überwiegend mit „Ja“ beantwortet werden können. Einzelne Fragen, die nur teilweise erfüllt sind, können toleriert werden, solange das Gesamtbild der Stufe konsistent ist.

Der **Gesamtreifegrad** der Organisation entspricht dem niedrigsten Einzelwert über alle sechs Dimensionen. Dieses Prinzip stellt sicher, dass keine kritischen Lücken übersehen werden.

Praktische Hinweise für die Durchführung:

Beteiligte Personen: Die Bewertung sollte unter Einbeziehung der IT-Leitung, des CISO bzw. IT-Sicherheitsbeauftragten, der Systemadministration, der Softwareentwicklung (falls vorhanden) und der Geschäftsleitung durchgeführt werden. Eine externe Moderation kann die Objektivität erhöhen.

Zeitaufwand: Für die erstmalige Durchführung sollten 4 bis 8 Stunden eingeplant werden, verteilt auf ein bis zwei Workshops. Folgebewertungen sind in der Regel in 2 bis 4 Stunden durchführbar.

3 Die sechs Dimensionen der Krypto-Agilität

Das Dimensionsmodell basiert auf dem CAMM-Framework von Näther et al.[18] und wurde für die praktische Anwendung in Organisationen adaptiert. Die sechs Dimensionen decken sowohl technische Aspekte (Inventory, Substitutability, Configurability, Automation, Monitoring) als auch organisatorische Aspekte (Governance) der Krypto-Agilität ab. Gemeinsam bilden sie ein ganzheitliches Bild der Fähigkeit einer Organisation, kryptografische Veränderungen zu bewältigen.

Für jede Dimension werden zunächst Zweck, Umfang und typische Herausforderungen beschrieben. Anschließend ermöglicht die Reifegradtabelle die konkrete Bewertung anhand prüfbarer Fragen. Die Antwort-Spalte kann mit „Ja“, „Teilweise“ oder „Nein“ gefüllt werden, die Kommentar-Spalte dient der Dokumentation von Evidenzen und Maßnahmen.

3.1 Dimension 1 – Inventory

Die Dimension **Inventory** erfasst, inwieweit eine Organisation einen vollständigen und aktuellen Überblick über ihre kryptografischen Assets besitzt. Dazu zählen eingesetzte Algorithmen, Protokolle, Schlüssel, Zertifikate und deren Abhängigkeiten.

Ein kryptografisches Inventar ist die unverzichtbare Grundlage jeder PQC-Migration. Ohne zu wissen, wo und wie Kryptografie eingesetzt wird, ist eine systematische Migration unmöglich. Die EU PQC Roadmap nennt die Erstellung kryptografischer Inventare als ersten Meilenstein bis Ende 2026.

Typische Herausforderungen für KMU: Shadow-IT und nicht dokumentierte Systeme erschweren die Inventarisierung. Legacy-Systeme nutzen häufig ältere kryptografische Verfahren, deren Abhängigkeiten nicht transparent sind. Cloud-Dienste und SaaS-Anwendungen verlagern Kryptografie in die Verantwortung Dritter, ohne dass die konkret eingesetzten Verfahren bekannt sind. Eingebettete Systeme und IoT-Geräte verwenden oft hardcodierte kryptografische Implementierungen, die sich einer einfachen Inventarisierung entziehen.

Stufe	Frage / Indikator	Antwort	Kommentar
1	**Initial**		
1	Existiert eine Übersicht der wichtigsten Systeme, die Kryptografie nutzen (z. B. VPN, E-Mail, Webserver, Datenbankverschlüsselung)?		
1	Ist bekannt, welche kryptografischen Verfahren (Algorithmen, Protokolle, Schlüssellängen) in der Organisation eingesetzt werden?		
1	Ist bekannt, welche Zertifikate und Schlüssel im Einsatz sind und wann diese ablaufen?		

2	**Bewusst**		
2	Wurde eine systematische Bestandsaufnahme der kryptografischen Assets eingeleitet?		
2	Werden kritische Systeme und deren kryptografische Abhängigkeiten dokumentiert?		
2	Ist eine verantwortliche Person für die kryptografische Inventarisierung benannt?		
2	Werden Discovery-Tools zur Identifizierung kryptografischer Assets evaluiert oder eingesetzt?		
3	**Systematisch**		
3	Existiert ein vollständiges kryptografisches Inventar über alle Ebenen (Infrastruktur, Anwendungen, Cloud)?		
3	Werden Abhängigkeiten zwischen Systemen und kryptografischen Komponenten systematisch erfasst (Dependency Mapping)?		
3	Sind quantenanfällige Algorithmen (RSA, ECC, DH) im Inventar markiert und nach Risiko priorisiert?		
3	Wird das Inventar regelmäßig aktualisiert (mindestens quartalsweise)?		
3	Existiert ein CBOM (Cryptographic Bill of Materials) für Schlüsselsysteme?		
4	**Fortgeschritten**		
4	Werden automatisierte Continuous-Discovery-Werkzeuge eingesetzt?		
4	Ist das kryptografische Inventar in CMDB / Asset Management integriert?		
4	Werden Lieferketten und Drittanbieter in die Inventarisierung einbezogen?		
4	Sind SBOMs mit kryptografischen Komponenten angereichert?		
5	**Exzellent**		

5	Existiert ein kryptografischer Digital Twin für Szenarioanalysen und Migrationssimulationen?		
5	Erfolgt eine Echtzeit-Synchronisation des Inventars über alle Umgebungen?		
5	Können Sie innerhalb von 24 Stunden einen vollständigen Bericht über Ihre kryptografische Exposition erstellen?		

3.2 Dimension 2 – Substitutability

Die Dimension **Substitutability** bewertet die Fähigkeit, kryptografische Algorithmen, Bibliotheken und Protokolle durch alternative oder neuere Verfahren zu ersetzen. Dies ist der Kern der Krypto-Agilität: die technische und organisatorische Fähigkeit, einen Algorithmus-Wechsel durchzuführen.

Die Austauschbarkeit wird durch verschiedene Faktoren bestimmt: die Architektur der Systeme (modular vs. monolithisch), die verwendeten APIs und Abstraktionsschichten, die Verfügbarkeit von PQC-fähigen Bibliotheken sowie die Existenz von Test- und Rollback-Mechanismen.

Typische Herausforderungen für KMU: Viele ältere Anwendungen verwenden hardcodierte kryptografische Verfahren ohne Abstraktionsschicht. Proprietäre Systeme bieten oft keine Möglichkeit, kryptografische Komponenten unabhängig auszutauschen. Der Mangel an Testumgebungen erschwert die sichere Erprobung neuer Algorithmen. Darüber hinaus sind Entwickler häufig nicht in krypto-agilen Designprinzipien geschult.

Stufe	Frage / Indikator	Antwort	Kommentar
1	**Initial**		
1	Ist bekannt, in welchen Systemen Kryptografie hardcodiert ist?		
1	Können kryptografische Bibliotheken prinzipiell aktualisiert werden?		
1	Ist die Austauschbarkeit kryptografischer Verfahren bei der Beschaffung neuer Systeme ein Kriterium?		
2	**Bewusst**		
2	Werden bei neuen Systemen modulare Krypto-Architekturen als Anforderung definiert?		
2	Werden algorithmus-unabhängige APIs und Abstraktionsschichten evaluiert (z. B. PKCS#11, JCA/JCE)?		

2	Ist PQC-Austauschbarkeit in den Beschaffungsrichtlinien verankert?		
2	Werden Entwickler in krypto-agilen Designprinzipien geschult?		
3	**Systematisch**		
3	Können kritische Systeme Algorithmen ohne Code-Änderungen austauschen?		
3	Sind Hybrid-Implementierungen (klassisch + PQC) in Schlüsselsystemen eingeführt?		
3	Werden PQC-fähige Bibliotheken eingesetzt (z. B. liboqs, BouncyCastle mit PQC-Support)?		
3	Existieren Rollback-Mechanismen für fehlgeschlagene Migrationen?		
3	Ist eine Testumgebung für Algorithmus-Migrationen verfügbar?		
4	**Fortgeschritten**		
4	Können alle produktiven Systeme Algorithmen ohne Betriebsunterbrechung austauschen?		
4	Existiert eine Validierungspipeline für Algorithmus-Migrationen vor Produktivschaltung?		
4	Werden Vendor-Abhängigkeiten bei kryptografischen Bibliotheken systematisch gemanagt?		
4	Ist die Austauschbarkeit über die gesamte Lieferkette sichergestellt?		
5	**Exzellent**		
5	Ist ein vollautomatisierter Algorithmus-Austausch über die gesamte Infrastruktur implementiert?		
5	Werden neue PQC-Algorithmen proaktiv in Pilotumgebungen evaluiert?		
5	Können Sie bei einer Zero-Day-Schwachstelle innerhalb von 72 Stunden organisationsweit reagieren?		

5	Ist Crypto-agile by Design als architektonisches Standardprinzip durchgesetzt?		

3.3 Dimension 3 – Configurability

Die Dimension **Configurability** bewertet, inwieweit kryptografische Parameter und Einstellungen ohne Code-Änderungen angepasst werden können. Konfigurierbarkeit ermöglicht schnelle Reaktionen auf neue Bedrohungen oder regulatorische Anforderungen, ohne aufwendige Entwicklungs- und Release-Zyklen durchlaufen zu müssen.

Zu den konfigurierbaren Parametern zählen unter anderem erlaubte Cipher Suites, Schlüssellängen, Protokollversionen, Zertifikatsvalidierungsregeln und Algorithmus-Präferenzen. Eine hohe Konfigurierbarkeit ist Voraussetzung für eine agile Anpassung an sich verändernde Anforderungen.

Typische Herausforderungen für KMU: Viele Standardanwendungen bieten nur eingeschränkte Konfigurationsmöglichkeiten für Kryptografie. Die Vielzahl unterschiedlicher Systeme und Plattformen erschwert eine einheitliche Konfiguration. Fehlende zentrale Steuerung führt zu inkonsistenten Konfigurationen. Änderungen werden häufig ohne formales Change Management durchgeführt, was Risiken erhöht.

Stufe	Frage / Indikator	Antwort	Kommentar
1	**Initial**		
1	Ist bekannt, welche kryptografischen Parameter konfigurierbar sind?		
1	Können Cipher Suites in den wichtigsten Systemen angepasst / ausgewechselt werden?		
1	Existiert eine Dokumentation der aktuellen kryptografischen Konfigurationen?		
2	**Bewusst**		
2	Werden kryptografische Parameter zentral über Konfigurationsdateien gesteuert?		
2	Ist ein Deaktivierungsplan für veraltete Cipher Suites vorhanden?		
2	Wird Cipher-Suite-Verhandlung in neuen Systemen als Anforderung definiert?		
2	Sind die aktuellen kryptografischen Konfigurationen dokumentiert?		
3	**Systematisch**		

3	Existiert eine zentrale Richtlinie für erlaubte Cipher Suites und Algorithmen?		
3	Ist ein formales Change Management für Konfigurationsänderungen eingeführt?		
3	Sind PQC-fähige Cipher Suites (z. B. hybrides TLS 1.3) konfiguriert?		
3	Können alle kritischen Systeme ohne Code-Änderungen konfiguriert werden?		
3	Sind Konfigurationsstandards dokumentiert und kommuniziert?		
4	**Fortgeschritten**		
4	Ist Policy-as-Code für kryptografische Konfigurationsrichtlinien implementiert?		
4	Erfolgt eine kontinuierliche Validierung der Konfigurationskonformität?		
4	Werden Konfigurationsabweichungen automatisch erkannt und eskaliert?		
4	Ist eine richtliniengesteuerte Algorithmusauswahl infrastrukturweit implementiert?		
5	**Exzellent**		
5	Erfolgt eine dynamische, kontextabhängige Konfigurationsanpassung?		
5	Ist eine organisationsweite automatisierte Cipher-Suite-Optimierung implementiert?		
5	Können neue Konfigurationsanforderungen innerhalb definierter Zeitfenster umgesetzt werden?		
5	Werden Konfigurationen kontinuierlich auf Performance und Sicherheit optimiert?		

3.4 Dimension 4 – Automation

Die Dimension **Automation** bewertet den Grad der Automatisierung kryptografischer Prozesse, insbesondere im Bereich des Zertifikats- und Schlüssel-Lifecycle-Managements. Manuelle Prozesse sind fehleranfällig, schwer skalierbar und reagieren zu langsam auf dynamische Bedrohungslagen.

Die Automatisierung umfasst die Provisionierung, Rotation, Erneuerung und Revokation von Schlüsseln und Zertifikaten sowie die automatisierte Überwachung der Einhaltung kryptografischer Richtlinien und die Integration in DevOps-Prozesse.

Typische Herausforderungen für KMU: Begrenzte Budgets erschweren die Investition in Certificate-Lifecycle-Management-Plattformen. Die manuelle Verwaltung von Zertifikaten führt regelmäßig zu Ausfällen durch abgelaufene Zertifikate. Fehlende Integration zwischen verschiedenen Systemen verhindert eine durchgängige Automatisierung. Der Übergang von manuellen zu automatisierten Prozessen erfordert initiale Investitionen in Tooling und Kompetenzaufbau.

Stufe	Frage / Indikator	Antwort	Kommentar
1	**Initial**		
1	Existiert eine Übersicht aller Zertifikats-Ablaufdaten?		
1	Werden Schlüssel und Zertifikate manuell verwaltet?		
1	Ist bekannt, wer für die Erneuerung von Zertifikaten zuständig ist?		
2	**Bewusst**		
2	Existiert eine grundlegende Automatisierung für die Zertifikatsverwaltung?		
2	Sind automatische Benachrichtigungen für ablaufende Zertifikate eingerichtet?		
2	Ist eine zeitgesteuerte Schlüsselrotation für kritische Systeme implementiert?		
2	Werden Certificate Lifecycle Management-Plattformen evaluiert?		
3	**Systematisch**		
3	Ist ein zentrales Certificate Lifecycle Management (CLM) implementiert?		
3	Erfolgt die Schlüsselrotation automatisiert nach definierten Richtlinien?		
3	Werden automatisierte Compliance-Checks für kryptografische Richtlinien durchgeführt?		
3	Werden HSMs oder Cloud-KMS für die sichere Schlüsselverwaltung eingesetzt?		

3	Existiert eine Prozessdokumentation für kryptografische Operationen?		
4	**Fortgeschritten**		
4	Ist eine End-to-End-Automatisierung (Provisionierung, Rotation, Erneuerung, Revokation) umgesetzt?		
4	Ist die kryptografische Automatisierung in CI/CD-Pipelines integriert?		
4	Werden Fehler automatisch erkannt, protokolliert und eskaliert?		
4	Sind automatisierte Rollback-Mechanismen implementiert?		
5	**Exzellent**		
5	Existiert ein vollständig orchestriertes, selbstheilendes Lifecycle Management?		
5	Werden Algorithmus-Migrationen (z. B. RSA→ML-KEM) automatisiert organisationsweit durchgeführt?		
5	Ist KI/ML-gestützte Anomalieerkennung für kryptografische Operationen integriert?		
5	Erfolgt eine kontinuierliche Optimierung basierend auf Performance- und Sicherheitsmetriken?		

3.5 Dimension 5 – Monitoring

Die Dimension **Monitoring** bewertet die Fähigkeit einer Organisation, den kryptografischen Zustand ihrer Systeme kontinuierlich zu überwachen, Abweichungen zu erkennen und darauf zu reagieren. Monitoring ist die Voraussetzung für die Erkennung von Schwachstellen, die Messung des Migrationsfortschritts und die Einhaltung regulatorischer Anforderungen.

Kryptografisches Monitoring umfasst die Überwachung eingesetzter Algorithmen und Protokollversionen, die Erkennung veralteter oder unsicherer Konfigurationen, die Messung von Schlüsselstärken und Zertifikatsgültigkeiten sowie die Verfolgung des PQC-Migrationsfortschritts.

Typische Herausforderungen für KMU: Kryptografische Ereignisse werden in Standard-Log-Systemen oft nicht gesondert erfasst oder ausgewertet. Die Integration kryptografischer Findings in bestehende SIEM-Systeme erfordert zusätzliche Konfiguration. Fehlende Metriken und KPIs erschweren die Messung des Fortschritts und die Berichterstattung an das Management.

Stufe	Frage / Indikator	Antwort	Kommentar
1	**Initial**		
1	Werden kryptografische Ereignisse (TLS-Fehler, Zertifikatsfehler) in Log-Systemen erfasst?		
1	Existiert ein grundlegendes Bewusstsein für kryptografische Risiken?		
1	Sind Verantwortlichkeiten für kryptografisches Monitoring definiert?		
2	**Bewusst**		
2	Werden regelmäßig Scans auf veraltete kryptografische Konfigurationen durchgeführt?		
2	Werden Monitoring-Ergebnisse in Sicherheitsberichten aufbereitet?		
2	Existiert eine Baseline für die aktuelle kryptografische Nutzung?		
2	Werden kryptografische Findings in Security-Reviews einbezogen?		
3	**Systematisch**		
3	Ist ein dediziertes kryptografisches Monitoring implementiert (Algorithmus-Nutzung, Schlüsselstärken, Protokollversionen)?		
3	Sind kryptografische Findings in SIEM/SOC integriert?		
3	Werden Compliance-Abweichungen automatisch erkannt und gemeldet?		
3	Wird der PQC-Migrationsfortschritt über definierte Metriken gemessen?		
3	Existiert ein Dashboard für den kryptografischen Status?		
4	**Fortgeschritten**		
4	Erfolgt eine Echtzeit-Erkennung kryptografischer Anomalien mit automatischer Eskalation?		

4	Sind KPIs für kryptografische Sicherheit auf Management-Ebene definiert und berichtet?		
4	Werden Drittanbieter und Lieferketten in das Monitoring einbezogen?		
4	Existiert ein vollständiger kryptografischer Audit-Trail?		
5	**Exzellent**		
5	Ist Continuous Cryptographic Assurance als Prozess etabliert?		
5	Werden prädiktive Analysen für kryptografische Risiken eingesetzt?		
5	Wird die Effektivität des Monitorings selbst gemessen und verbessert?		
5	Können Sie bei einer neuen Schwachstelle den organisationsweiten Expositionsgrad innerhalb von Stunden ermitteln?		

3.6 Dimension 6 – Governance

Die Dimension **Governance** bewertet die organisatorischen Rahmenbedingungen für kryptografische Sicherheit: Richtlinien, Verantwortlichkeiten, Schulungen, regulatorische Compliance und die strategische Verankerung des Themas in der Organisation. Ohne angemessene Governance bleiben technische Maßnahmen Insellösungen ohne nachhaltige Wirkung.

Governance schafft den organisatorischen Rahmen, in dem technische Maßnahmen wirksam werden: klare Verantwortlichkeiten, dokumentierte Richtlinien, Schulungsprogramme, Eskalationswege und die Einbettung kryptografischer Sicherheit in die Unternehmensführung.

Typische Herausforderungen für KMU: Kryptografie wird häufig als rein technisches Thema betrachtet, das keiner Governance-Strukturen bedarf. Die Quantenbedrohung ist vielen Entscheidungsträgern nicht bekannt oder wird als zu abstrakt wahrgenommen. Begrenzte Personalressourcen erschweren die Einrichtung dedizierter Rollen und Gremien. Die Integration in bestehende Management-Systeme (z. B. ISMS) erfordert zusätzlichen Aufwand.

Stufe	Frage / Indikator	Antwort	Kommentar
1	**Initial**		
1	Existiert eine grundlegende Kryptografie-Richtlinie?		
1	Sind Rollen und Verantwortlichkeiten für kryptografische Sicherheit definiert?		

1	Werden regulatorische Anforderungen an Kryptografie nachverfolgt?		
2	**Bewusst**		
2	Ist eine RACI-Matrix für kryptografische Verantwortlichkeiten erstellt?		
2	Existiert ein Ausnahmen-Dokumentationsprozess für kryptografische Abweichungen?		
2	Werden grundlegende Awareness-Schulungen zur Quantenbedrohung durchgeführt?		
2	Werden regulatorische Anforderungen (NIS2, DSGVO, branchenspezifisch) aktiv nachverfolgt?		
3	**Systematisch**		
3	Existiert ein organisationsweites Policy-Framework für Kryptografie?		
3	Ist ein Executive Sponsor für das Quantum-Readiness-Programm benannt?		
3	Sind Vendor-Anforderungen für PQC-Readiness in der Beschaffung definiert?		
3	Ist die Krypto-Governance in das ISMS (z. B. ISO 27001) integriert?		
3	Sind Eskalationspfade für kritische kryptografische Findings definiert?		
4	**Fortgeschritten**		
4	Existiert ein cross-funktionales Quantum-Readiness-Team?		
4	Werden Drittanbieter-Risiken systematisch bewertet?		
4	Ist eine risikobasierte Priorisierung für die PQC-Migration implementiert?		
4	Sind KPIs für Krypto-Agilität auf Management-Ebene definiert?		
5	**Exzellent**		

5	Ist die Krypto-Governance in die unternehmensweite Risikostrategie eingebettet?		
5	Werden Richtlinien automatisch durchgesetzt (Policy-as-Code)?		
5	Erfolgt eine kontinuierliche Compliance mit automatisierter Attestierung?		
5	Erfolgt eine proaktive Anpassung an neue regulatorische Anforderungen?		
5	Wird die Effektivität der Governance gemessen und kontinuierlich verbessert?		

4 Maßnahmenkatalog: Von Stufe zu Stufe

Der folgende Maßnahmenkatalog beschreibt für jede der sechs Dimensionen konkrete, umsetzbare Tätigkeiten, die eine Organisation von einer Reifegradstufe zur nächsten führen. Die Maßnahmen sind priorisiert und so formuliert, dass sie auch für KMU mit begrenzten Ressourcen nachvollziehbar und umsetzbar sind. Jeder Übergang umfasst vier bis sechs Maßnahmen, die in der angegebenen Reihenfolge sinnvoll abzuarbeiten sind.

4.1 Dimension 1 – Inventory

Die Inventarisierung bildet das Fundament jeder PQC-Migration. Ohne ein vollständiges und aktuelles Inventar kryptografischer Assets ist eine risikobasierte Priorisierung nicht möglich.

Übergang	Maßnahmen
1 → 2	1. Verantwortliche Person für die kryptografische Inventarisierung benennen. 2. Workshops mit IT-Teams durchführen, um kryptografische Systeme zu identifizieren. 3. Kritische Systeme und deren kryptografische Abhängigkeiten in einer Tabelle dokumentieren. 4. Discovery-Tools evaluieren. 5. Erste Ergebnisse in einem zentralen Dokument zusammenfassen.
2 → 3	1. Vollständiges kryptografisches Inventar erstellen über alle Ebenen (Infrastruktur, Anwendungen, Cloud). 2. Dependency Mapping einführen, um Abhängigkeiten zwischen Systemen sichtbar zu machen. 3. Regelmäßige Aktualisierungszyklen definieren (mindestens quartalsweise). 4. Quantenanfällige Algorithmen (RSA, ECC, DH) im Inventar markieren und nach Risiko priorisieren. 5. CBOM (Cryptographic Bill of Materials) für Schlüsselsysteme erstellen.
3 → 4	1. Automatisierte Continuous-Discovery-Werkzeuge implementieren. 2. Software Bill of Materials (SBOM) mit kryptografischen Komponenten anreichern. 3. Risikobasierte Priorisierung implementieren (High-Value Assets zuerst). 4. Lieferketten und Drittanbieter in die Inventarisierung einbeziehen. 5. Integration des Inventars in CMDB/Asset Management.
4 → 5	1. Kryptografischen Digital Twin aufbauen für Szenarioanalysen und Migrationssimulationen. 2. Echtzeit-Synchronisation über alle Umgebungen (On-Premises, Cloud, Hybrid) sicherstellen. 3. Automatische Verknüpfung von Inventaränderungen mit Risikobewertungen implementieren. 4. Fähigkeit aufbauen, innerhalb von 24 Stunden vollständigen Bericht über kryptografische Exposition zu erstellen.

4.2 Dimension 2 – Substitutability

Die Austauschbarkeit kryptografischer Komponenten ist der technische Kern der Krypto-Agilität. Investitionen in modulare Architekturen und Abstraktionsschichten zahlen sich bei jeder zukünftigen kryptografischen Änderung aus.

Übergang	Maßnahmen
1 → 2	1. Analyse durchführen, wo Kryptografie hardcodiert ist. 2. Bei neuen Systemen modulare Architekturen als Anforderung definieren. 3. Algorithmus-unabhängige APIs und Abstraktionsschichten evaluieren (z. B. PKCS#11, JCA/JCE). 4. PQC-Austauschbarkeit in Beschaffungsrichtlinien aufnehmen. 5. Entwickler in krypto-agilen Designprinzipien schulen.
2 → 3	1. Kritische Systeme auf Algorithmus-Austauschbarkeit ohne Code-Änderungen umbauen. 2. Hybrid-Implementierungen (klassisch + PQC) in Schlüsselsystemen einführen. 3. PQC-fähige Bibliotheken einsetzen (z. B. liboqs, BouncyCastle mit PQC-Support). 4. Rollback-Mechanismen für fehlgeschlagene Migrationen implementieren. 5. Testumgebung für Algorithmus-Migrationen aufbauen.
3 → 4	1. Algorithmus-Austausch in allen produktiven Systemen ohne Betriebsunterbrechung ermöglichen. 2. Validierungspipeline für Algorithmus-Migrationen vor Produktivschaltung etablieren. 3. Vendor-Abhängigkeiten bei kryptografischen Bibliotheken systematisch managen. 4. Austauschbarkeit über die gesamte Lieferkette sicherstellen.
4 → 5	1. Vollautomatisierten Algorithmus-Austausch über die gesamte Infrastruktur implementieren. 2. Proaktive Evaluierung neuer PQC-Algorithmen in Pilotumgebungen. 3. Reaktionsfähigkeit bei Zero-Day-Schwachstelle innerhalb von 72 Stunden sicherstellen. 4. Crypto-agile by Design als architektonisches Standardprinzip durchsetzen.

4.3 Dimension 3 – Configurability

Die Konfigurierbarkeit ermöglicht schnelle Reaktionen auf neue Bedrohungen oder regulatorische Anforderungen. Zentrale Steuerung und Policy-as-Code sind Schlüsselelemente für eine effiziente kryptografische Konfiguration.

Übergang	Maßnahmen
1 → 2	1. Bestandsaufnahme konfigurierbarer kryptografischer Parameter durchführen. 2. Zentrale Steuerung über Konfigurationsdateien für kritische Systeme einführen. 3. Cipher-Suite-Verhandlung in neuen Systemen als Anforderung definieren. 4. Veraltete Cipher Suites identifizieren und Deaktivierungsplan erstellen. 5. Dokumentation der aktuellen kryptografischen Konfigurationen.
2 → 3	1. Zentrale Richtlinie für erlaubte Cipher Suites und Algorithmen definieren und umsetzen.

	2. Formales Change Management für Konfigurationsänderungen einführen. 3. PQC-fähige Cipher Suites (z. B. hybrides TLS 1.3) konfigurieren. 4. Alle kritischen Systeme auf Konfiguration ohne Code-Änderungen umstellen. 5. Konfigurationsstandards dokumentieren und kommunizieren.
3 → 4	1. Policy-as-Code für kryptografische Konfigurationsrichtlinien implementieren. 2. Kontinuierliche Validierung der Konfigurationskonformität (Compliance-Scans). 3. Automatische Erkennung und Eskalation von Konfigurationsabweichungen. 4. Richtliniengesteuerte Algorithmusauswahl infrastrukturweit implementieren.
4 → 5	1. Dynamische, kontextabhängige Konfigurationsanpassung (basierend auf Risiko/Bedrohungslage). 2. Organisationsweite automatisierte Cipher-Suite-Optimierung. 3. Fähigkeit aufbauen, neue Konfigurationsanforderungen innerhalb definierter Zeitfenster umzusetzen. 4. Kontinuierliche Performance- und Sicherheitsoptimierung der Konfigurationen.

4.4 Dimension 4 – Automation

Die Automatisierung kryptografischer Prozesse reduziert Fehlerquellen, erhöht die Reaktionsgeschwindigkeit und ermöglicht Skalierbarkeit. Zentrales Certificate Lifecycle Management ist der wichtigste Meilenstein auf dem Weg zur vollständigen Automatisierung.

Übergang	Maßnahmen
1 → 2	1. Überblick über alle Zertifikats-Ablaufdaten konsolidieren. 2. Erste Automatisierungslösung für Zertifikatsverwaltung einführen (z. B. ACME, Let's Encrypt). 3. Automatische Benachrichtigungen für ablaufende Zertifikate einrichten. 4. Zeitgesteuerte Schlüsselrotation für kritische Systeme implementieren. 5. Evaluation von CLM-Plattformen starten.
2 → 3	1. Zentrales Certificate Lifecycle Management (CLM) implementieren. 2. Automatisierte Schlüsselrotation nach definierten Richtlinien. 3. Automatisierte Compliance-Checks für kryptografische Richtlinien. 4. HSMs oder Cloud-KMS für sichere Schlüsselverwaltung einsetzen. 5. Prozessdokumentation für kryptografische Operationen erstellen.
3 → 4	1. End-to-End-Automatisierung (Provisionierung, Rotation, Erneuerung, Revokation). 2. Integration in CI/CD-Pipelines und DevOps-Prozesse. 3. Automatische Fehlererkennung, Protokollierung und Eskalation. 4. Automatisierte Rollback-Mechanismen implementieren. 5. Kryptografische Automatisierung in Cloud-Umgebungen integrieren.
4 → 5	1. Vollständig orchestriertes und selbstheilendes Lifecycle Management. 2. Kontinuierliche Optimierung basierend auf Performance- und Sicherheitsmetriken. 3. Automatisierte Algorithmus-Migrationen (z. B. RSA→ML-KEM) organisationsweit ohne manuelle Eingriffe. 4. KI/ML-gestützte Anomalieerkennung und prädiktive Analysen integrieren.

4.5 Dimension 5 – Monitoring

Monitoring liefert die Datenbasis für fundierte Entscheidungen, Compliance-Nachweise und die Messung des Migrationsfortschritts. Ohne kontinuierliche Überwachung bleibt die kryptografische Sicherheitslage intransparent.

Übergang	Maßnahmen
1 → 2	1. Kryptografische Ereignisse in Log-Systemen erfassen (TLS-Fehler, Zertifikatsfehler, Handshake-Probleme). 2. Regelmäßige Scans auf veraltete kryptografische Konfigurationen durchführen. 3. Monitoring-Ergebnisse in Sicherheitsberichten aufbereiten. 4. Baseline für aktuelle kryptografische Nutzung erstellen. 5. Verantwortlichkeiten für kryptografisches Monitoring definieren.
2 → 3	1. Dediziertes kryptografisches Monitoring implementieren (Algorithmus-Nutzung, Schlüsselstärken, Protokollversionen). 2. Integration kryptografischer Findings in SIEM/SOC. 3. Automatische Erkennung und Meldung von Compliance-Abweichungen. 4. PQC-Migrationsfortschritt über definierte Metriken messen. 5. Dashboard für kryptografischen Status erstellen.
3 → 4	1. Echtzeit-Erkennung kryptografischer Anomalien mit automatischer Eskalation. 2. KPIs für kryptografische Sicherheit auf Management-Ebene definieren und berichten. 3. Drittanbieter und Lieferketten in das Monitoring einbeziehen. 4. Vollständigen kryptografischen Audit-Trail für alle Operationen führen.
4 → 5	1. Continuous Cryptographic Assurance als Prozess etablieren. 2. Prädiktive Analysen für kryptografische Risiken einsetzen. 3. Effektivität des Monitorings selbst messen und verbessern. 4. Fähigkeit aufbauen, bei neuer Schwachstelle den organisationsweiten Expositionsgrad innerhalb von Stunden zu ermitteln.

4.6 Dimension 6 – Governance

Governance schafft den organisatorischen Rahmen, ohne den technische Maßnahmen nicht nachhaltig wirksam werden. Executive Sponsorship, klare Verantwortlichkeiten und die Integration in bestehende Management-Systeme sind entscheidende Erfolgsfaktoren.

Übergang	Maßnahmen
1 → 2	1. Kryptografie-Richtlinie dokumentieren. 2. RACI-Matrix für Rollen und Verantwortlichkeiten erstellen. 3. Regulatorische Anforderungen (NIS2, DSGVO, branchenspezifisch) nachverfolgen. 4. Ausnahmen-Dokumentationsprozess einführen. 5. Grundlegende Awareness-Schulungen durchführen.
2 → 3	1. Organisationsweites Policy-Framework etablieren und kommunizieren. 2. Executive Sponsor für Quantum-Readiness-Programm sichern.

	3. Vendor-Anforderungen für PQC-Readiness in Beschaffung definieren. 4. Krypto-Governance in ISMS (ISO 27001) integrieren. 5. Eskalationspfade für kritische kryptografische Findings definieren.
3 → 4	1. Cross-funktionales Quantum-Readiness-Team etablieren. 2. Drittanbieter-Risiken systematisch bewerten. 3. Risikobasierte Priorisierung für PQC-Migration implementieren. 4. KPIs für Krypto-Agilität auf Management-Ebene definieren. 5. Zentrale Verwaltung von Abweichungen und Ausnahmen.
4 → 5	1. Krypto-Governance in unternehmensweite Risikostrategie einbetten. 2. Richtlinien automatisch durchsetzen (Policy-as-Code). 3. Kontinuierliche Compliance mit automatisierter Attestierung. 4. Proaktive Anpassung an neue regulatorische Anforderungen. 5. Effektivität der Governance messen und verbessern.

5 Roadmap zur PQC-Readiness

Die folgende Roadmap übersetzt die Ergebnisse der Reifegradbe-wertung in einen zeitlich strukturierten Umsetzungsplan. Die vier Phasen korrespondieren mit den Übergängen zwischen den Reifegradstufen und sind an den Meilensteinen der EU PQC Roadmap ausgerichtet[19]. Die Zeiträhmen sind als Richtwerte für mittlere Organisationen zu verstehen und können je nach Ausgangslage und verfügbaren Ressourcen variieren.

5.1 Phase 1: Grundlagen schaffen (Stufe 1 → 2, Zeitrahmen: 3–6 Monate)

Die erste Phase legt die organisatorischen und wissensbezogenen Grundlagen für die PQC-Migration. Der Fokus liegt auf Bewusstseinsbildung, erster Bestandsaufnahme und der Etablierung grundlegender Verantwortlichkeiten. Diese Phase ist auch mit begrenzten Ressourcen realisierbar und sollte unverzüglich begonnen werden.

Kernmaßnahmen:

Bewusstsein schaffen und Executive Awareness herstellen: Die Geschäftsleitung muss die Relevanz der Quantenbedrohung verstehen. Kurze Briefings und Entscheidungsvorlagen helfen, das Thema auf die Agenda zu setzen.

Quantum Champion benennen: Eine Person oder Rolle wird als zentrale Ansprechperson für das Thema PQC-Readiness definiert. Diese Person treibt die Initiative voran und koordiniert die Aktivitäten.

Grundlegende Awareness-Schulungen: IT-Mitarbeitende und Entscheidungsträger werden über die Quantenbedrohung, HNDL-Risiken und die Grundzüge der PQC-Migration informiert.

Erste kryptografische Bestandsaufnahme: In Workshops mit IT-Teams werden die wichtigsten kryptografischen Systeme und Abhängigkeiten identifiziert und dokumentiert.

Quantum-Threat-Baseline dokumentieren: Die aktuelle kryptografische Exposition wird erfasst, insbesondere im Hinblick auf quantenanfällige Verfahren und HNDL-Risiken.

Regulatorische Anforderungen sichten: Die für die Organisation relevanten regulatorischen Vorgaben (NIS2, DSGVO, branchenspezifische Anforderungen) werden identifiziert und dokumentiert.

Regulatorisches Alignment: *Diese Phase sollte bis spätestens* ***31.12.2026*** *abgeschlossen sein, um den ersten Meilenstein der EU PQC Roadmap zu erfüllen.*

5.2 Phase 2: Systematisierung (Stufe 2 → 3, Zeitrahmen: 6–18 Monate)

Die zweite Phase überführt die in Phase 1 geschaffenen Grundlagen in systematische, dokumentierte Prozesse. Der Fokus liegt auf der Vervollständigung des kryptografischen Inventars, der Etablierung formaler Governance-Strukturen und ersten technischen Pilotprojekten. Das Erreichen von Stufe 3 stellt den kritischen Schwellenwert für regulatorische Compliance dar.

Kernmaßnahmen:

Vollständiges kryptografisches Inventar: Das in Phase 1 begonnene Inventar wird über alle Ebenen (Infrastruktur, Anwendungen, Cloud) vervollständigt. Dependency Mapping macht Abhängigkeiten sichtbar.

Executive Sponsor sichern: Ein Mitglied der Geschäftsleitung übernimmt die Schirmherrschaft für das PQC-Programm und stellt die notwendigen Ressourcen bereit.

Formales PQC-Programm aufsetzen: Ziele, Meilensteine, Budget und Verantwortlichkeiten werden in einem formalen Programm definiert und dokumentiert.

Hybrid-TLS-Piloten starten: In ausgewählten Systemen werden hybride TLS-Konfigurationen (klassisch + PQC) als Pilot implementiert, um Erfahrungen zu sammeln und Kompatibilität zu testen.

CLM implementieren: Ein zentrales Certificate Lifecycle Management wird eingeführt, um die automatisierte Verwaltung von Zertifikaten und Schlüsseln zu ermöglichen.

Krypto-Governance in ISMS integrieren: Kryptografische Richtlinien und Prozesse werden in das bestehende Informationssicherheits-Managementsystem (z. B. ISO 27001) integriert.

Regulatorisches Alignment: *Diese Phase sollte bis spätestens **31.12.2028** abgeschlossen sein. Die EU PQC Roadmap fordert bis Ende 2026 lediglich Inventarisierung, Risikoanalyse und Planung („First Steps"), nicht das Erreichen systematischer Reife. Das UK NCSC gibt für die Discovery-Phase ebenfalls bis 2028 Zeit. Das Erreichen von Stufe 3 schafft eine fundierte Grundlage zur Erfüllung der regulatorischen Anforderungen nach NIS2 und EU PQC Roadmap – die konkrete Compliance-Bewertung ist jedoch stets organisationsspezifisch vorzunehmen.*

5.3 Phase 3: Operative Reife (Stufe 3 → 4, Zeitrahmen: 12–24 Monate)

Die dritte Phase baut auf den systematischen Grundlagen auf und entwickelt die Organisation zu einem fortgeschrittenen Reifegrad. Der Fokus liegt auf Automatisierung, Integration in die operative Steuerung und der Einbeziehung der Lieferkette. In dieser Phase werden PQC-Migrationen in produktiven Systemen durchgeführt.

Kernmaßnahmen:

Automatisierte Inventarisierung und Compliance: Continuous-Discovery-Werkzeuge ersetzen manuelle Inventarisierungsprozesse. Automatisierte Compliance-Checks überwachen die Einhaltung kryptografischer Richtlinien.

PQC-Pilotdeployments in Produktion: Ausgewählte produktive Systeme werden auf PQC-Algorithmen migriert, beginnend mit den hochkritischsten Anwendungsfällen.

Quantitative KPIs und Management-Reporting: Messbare Kennzahlen für den kryptografischen Sicherheitsstatus und den Migrationsfortschritt werden definiert und regelmäßig an das Management berichtet.

Lieferketten-Integration: Drittanbieter und Lieferanten werden in die PQC-Readiness-Bewertung einbezogen. Anforderungen an die kryptografische Sicherheit werden in Verträgen und Beschaffungsprozessen verankert.

Risikobasierte Migrationspriorisierung: Die Migration wird nach dem HNDL-Risiko priorisiert: Systeme mit langlebigen Geheimnissen und hohem Schutzbe-darf werden zuerst migriert.

5.4 Phase 4: Exzellenz (Stufe 4 → 5, Zeitrahmen: 24–36 Monate)

Die vierte Phase führt die Organisation zur höchsten Reifegradstufe. Der Fokus liegt auf vollständiger Automatisierung, proaktiver Bedrohungsanalyse und der Verankerung von Krypto-Agilität als Kernkompetenz der Organisation. Diese Phase adressiert den langfristigen EU-Meilenstein 2035.

Kernmaßnahmen:

Vollautomatisierung und Orchestrierung: Alle kryptografischen Prozesse – von der Inventarisierung über die Konfiguration bis zur Migration – sind vollständig automatisiert und orchestriert.

Crypto-agile by Design als Prinzip: Krypto-Agilität ist als architektonisches Standardprinzip verankert. Alle neuen Systeme werden von Beginn an krypto-agil entworfen.

Prädiktive Analysen: KI/ML-gestützte Werkzeuge ermöglichen prädiktive Risikoanalysen und die frühzeitige Erkennung kryptografischer Trends und Bedrohungen.

Continuous Cryptographic Assurance: Die kryptografische Sicherheitslage wird kontinuierlich und automatisiert überprüft. Attestierungen werden automatisch generiert.

Digital Twin für Migrationssimulationen: Ein kryptografischer Digital Twin ermöglicht die Simulation von Migrationsszenarien und die Analyse von Auswirkungen, bevor Änderungen produktiv umgesetzt werden.

6 Gesamtbewertung

Die folgende Tabelle fasst die Ergebnisse der Bewertung über alle sechs Dimensionen zusammen. Tragen Sie für jede Dimension die erreichte Reifegradstufe ein. Der Gesamtreifegrad entspricht – gemäß dem Prinzip der schwächsten Kette – dem niedrigsten Einzelwert.

Dimension	Erreichte Stufe	Zielstufe
1 – Inventory		
2 – Substitutability		
3 – Configurability		
4 – Automation		
5 – Monitoring		
6 – Governance		
Gesamtreifegrad		

Empfehlung: ***Stufe 3 (Systematisch)*** sollte als **Mindestziel** angestrebt werden, um die regulatorischen Anforderungen nach NIS2, EU PQC Roadmap und BSI Joint Statement zu erfüllen. Die Erreichung von Stufe 3 korrespondiert mit NIST CSWP 39 Tier 3 (Standardized), das als Minimum für regulatorische Compliance definiert ist.

Organisationen, die aktuell unter Stufe 3 liegen, sollten die **Roadmap (Kapitel 5)** und den **Maßnahmenkatalog (Kapitel 4)** als Leitfaden nutzen, um schrittweise das Mindestniveau zu erreichen. Das Alignment mit den EU-Meilensteinen (2026/2030/2035) bietet dabei den zeitlichen Orientierungsrahmen.

7 Empfehlungen für KMU

Kleine und mittlere Unternehmen stehen bei der PQC-Migration vor besonderen Herausforderungen: begrenzte Budgets, knappe Personalressourcen und oft fehlendes Spezialwissen im Bereich Kryptografie. Die folgenden Empfehlungen adressieren diese Herausforderungen und zeigen pragmatische Wege zur Verbesserung der Krypto-Agilität.

7.1 Pragmatischer Einstieg: Stufe 1 → 2 ist machbar

Der Übergang von Stufe 1 zu Stufe 2 erfordert keine großen Investitionen. Die wesentlichen Maßnahmen – Bewusstseinsbildung, erste Bestandsaufnahme, Benennung einer verantwortlichen Person – können mit vorhandenen Ressourcen umgesetzt werden. Der wichtigste Schritt ist, überhaupt zu beginnen. Selbst ein unvollständiges Inventar ist besser als gar keines, denn es schafft die Grundlage für alle weiteren Maßnahmen.

7.2 Commodity-IT: PQC-Migration durch Vendor-Updates

Ein erheblicher Teil der kryptografischen Migration wird für KMU automatisch durch Vendor-Updates erfolgen. Browser, Betriebssysteme und Cloud-Dienste migrieren auf PQC-Standards, ohne dass der Endnutzer eingreifen muss. Google Chrome und Mozilla Firefox unterstützen bereits hybrides TLS mit ML-KEM. Microsoft und AWS integrieren PQC in ihre Cloud-Plattformen. Für Standard-IT-Infrastruktur bedeutet dies: Regelmäßige Updates und Patches sind die einfachste und kostengünstigste Migrationsstrategie.

7.3 Fokus auf Custom-Software und spezielle Systeme

Der größte Handlungsbedarf besteht bei individuell entwickelter Software, eingebetteten Systemen, Legacy-Anwendungen und spezialisierten Branchenlösungen. Diese Systeme erhalten ggfs. keine automatischen PQC-Updates und müssen aktiv migriert werden. Hier ist eine frühzeitige Inventarisierung und Risikoanalyse besonders wichtig, um den Migrationsaufwand realistisch einzuschätzen und rechtzeitig zu planen.

7.4 Kosten-Nutzen: HNDL-Risiko gegen Migrationskosten abwägen

Nicht alle Daten und Systeme sind gleich schützenswert. KMU sollten die Migrationsreihenfolge nach dem HNDL-Risiko priorisieren: Systeme, die langlebige Geheimnisse verarbeiten (z. B. Kundendaten, geistiges Eigentum, Verträge), sollten zuerst migriert werden. Systeme mit kurzlebigen Daten und geringem Schutzbedarf können später adressiert werden. Diese Priorisierung ermöglicht eine effiziente Allokation begrenzter Ressourcen.

7.5 Externe Unterstützung nutzen

KMU müssen die PQC-Migration nicht allein bewältigen. Zahlreiche Ressourcen stehen zur Verfügung: Das BSI bietet Empfehlungen und Leitfäden für die kryptografische Sicherheit. Branchenverbände und Industrie- und Handelskammern (IHK) bieten Information und Vernetzung. Managed Security Service Provider (MSSPs) können die operative Umsetzung unterstützen. Förderprogramme auf Bundes- und EU-Ebene können die finanziellen Hürden senken.

7.6 Quick Wins identifizieren

Einige Maßnahmen bieten unmittelbaren Sicherheitsgewinn bei geringem Aufwand: TLS-Konfigurationen aktualisieren und unsichere Cipher Suites deaktivieren. Zertifikatsmanagement

automatisieren Schlüsselrotation für kritische Systeme einführen. Software und Betriebssysteme aktuell halten, um von PQC-Updates der Hersteller zu profitieren. Diese Quick Wins verbessern die Sicherheitslage sofort und schaffen Momentum für weiterführende Maßnahmen.

8 Quellenverzeichnis

[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

[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

[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

[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, Dezember 2025, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf