PQC-Bereitschaftsbewertung — Zusammenfassung

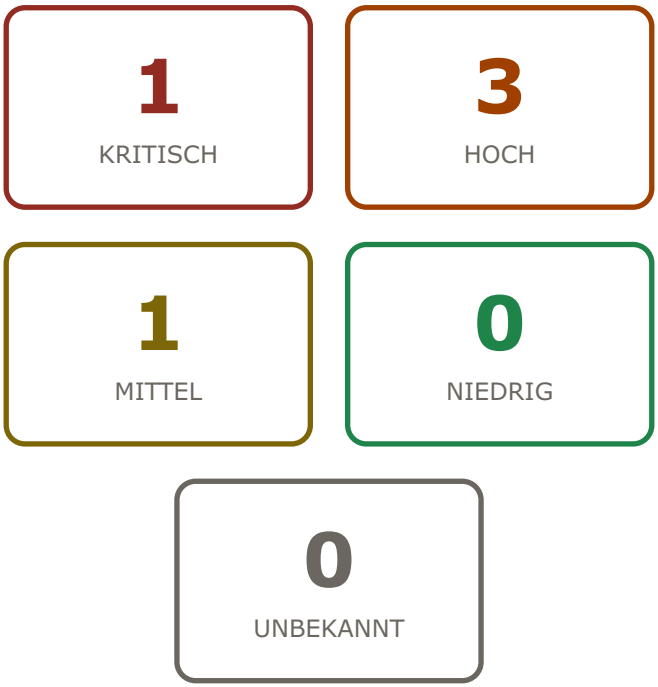
Auftraggeber: **Bank Krajowy Sp. z o.o.**

Audit-ID: `00000000-0000-0000-0001-000000000001`

Erstellt am: 2026-06-03 19:29 UTC

Modellkonfidenz: **84%**

Risikoubersicht



Regulatorische Bereitschaftsindikatoren

k.A.

NIS2-Bereitschaftsindikator

Unzureichende Scandaten fur eine Gesamtbewertung. Es wurden nur offentlich erreichbare TLS-Endpunkte gescannt; interne Kontrollen, Governance und ICT-Prozesse wurden nicht bewertet. Eine vollstandige Bewertung erfordert eine manuelle Prufsitzung.

k.A.

DORA-Bereitschaftsindikator

Unzureichende Scandaten fur eine Gesamtbewertung. Es wurden nur offentlich erreichbare TLS-Endpunkte gescannt; interne Kontrollen, Governance und ICT-Prozesse wurden nicht bewertet. Eine vollstandige Bewertung erfordert eine manuelle Prufsitzung.

Indikativer Behebungszeitraum: **540** Tage

Feststellungen

KRITISCH RSA-2048 → REQUIRES_REVIEW:TLS 1.3 with X25519+ML-KEM-768 hybrid key exchange (FIPS 203)

Legacy TLS 1.2 with RSA key exchange on main banking portal bankkrajowy.pl. Financial transaction data and PSD2 authentication credentials are at risk of Harvest-Now-Decrypt-Later attack. RSA-2048 key exchange is quantum-vulnerable (NIST PQC: FIPS 203). DORA Art.9 requires cryptographic protection based on approved data classification.

Komponente: TLS handshake on bankkrajowy.pl:443 (legacy cipher) | **Aufwand:** mittel | **HNDL-Indikator:** ja

HOCH REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid) → REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid (FIPS 203) — available in Caddy 2.9+, nginx 1.27+, AWS ALB (preview)

TLS 1.3 is enabled on API, mobile, and corporate endpoints, but without post-quantum hybrid key exchange. The X25519-only configuration offers no protection against HNDL attacks on intercepted TLS sessions. Polish National Cybersecurity Strategy 2025-2029 explicitly mandates planning for PQC migration.

Komponente: TLS 1.3 modern endpoints (api, mobile, corp) | **Aufwand:** gering | **HNDL-Indikator:** ja

HOCH RSA-2048 → REQUIRES_REVIEW:ML-DSA-65 CA root (FIPS 204) — requires EJBCA 8.x + PQC-capable HSM firmware

Internal EJBCA PKI uses RSA-2048 as CA root. All internal certificates derive from a quantum-vulnerable root. Migration to ML-DSA-65 (FIPS 204) root CA is a multi-month project requiring HSM firmware updates and certificate re-issuance across all internal services.

Komponente: EJBCA internal PKI — RSA-2048 CA root | **Aufwand:** hoch | **HNDL-Indikator:** nein

Regulatorischer Kontext

Rechtsrahmen	Artikel	KRITISCH	Verbundene Feststellungen
DORA	`REQUIRES_REVIEW:DORA Art. 9(2)`	KRITISCH	F-001, F-002
Cryptographic protection of financial transaction data and authentication credentials relies on quantum-vulnerable RSA-2048 key exchange on the main banking portal. Potential non-conformity with DORA Art.9(2) requirement for cryptographic key protection based on approved data classification.			
NIS2	`NIS2 Art.21(2)(f)`	HOCH	F-003
Cryptographic policies do not yet address post-quantum migration as required under NIS2 Art. 21(2)(f) and its PL transposition (UoKSC). Internal PKI migration planning is absent.			
DORA	`REQUIRES_REVIEW:DORA Art. 9(2)`	HOCH	F-005
SHA-1 in audit log signing indicates insufficient cryptographic controls under DORA ICT risk management framework.			

> *NIS2 — illustrative Obergrenze fur Verwaltungsbussen bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (angewendet von der zustandigen Behorde in schwerwiegenden Fallen). Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

> *DORA — mogliche Zwangsgelder bis zu 1 % des taglichen Gesamtumsatzes pro Tag bei anhaltender Nichtkonformitat. Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

Prioritare Massnahmen

1. **RSA-2048 → REQUIRES_REVIEW:TLS 1.3 with X25519+ML-KEM-768 hybrid key exchange (FIPS 203)** mittel
   Legacy TLS 1.2 with RSA key exchange on main banking portal bankkrajowy.pl. Financial transaction data and PSD2 authentication credentials are at risk of Harvest-Now-Decrypt-Later attack. RSA-2048 key exchange is quantum-vulnerable (NIST PQC: FIPS 203). DORA Art.9 requires cryptographic protection based on approved data classification.

   REQUIRES_REVIEW:DORA Art.9(2) · NIS2 Art.21(2)(f)

2. **REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid) → REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid (FIPS 203) — available in Caddy 2.9+, nginx 1.27+, AWS ALB (preview)** gering
   TLS 1.3 is enabled on API, mobile, and corporate endpoints, but without post-quantum hybrid key exchange. The X25519-only configuration offers no protection against HNDL attacks on intercepted TLS sessions. Polish National Cybersecurity Strategy 2025-2029 explicitly mandates planning for PQC migration.

   REQUIRES_REVIEW:DORA Art.9(2) · REQUIRES_REVIEW:UoKSC Art.10(5)

3. **RSA-2048 → REQUIRES_REVIEW:ML-DSA-65 CA root (FIPS 204) — requires EJBCA 8.x + PQC-capable HSM firmware** hoch
   Internal EJBCA PKI uses RSA-2048 as CA root. All internal certificates derive from a quantum-vulnerable root. Migration to ML-DSA-65 (FIPS 204) root CA is a multi-month project requiring HSM firmware updates and certificate re-issuance across all internal services.

   REQUIRES_REVIEW:DORA Art.9(2) · REQUIRES_REVIEW:KNF Rekomendacja D pkt. 5.3

Massnahmenplan

Schnelle Massnahmen (0-3 Monate)

Zeitrahmen: 0-3

- Enable TLS 1.3 exclusively on bankkrajowy.pl main portal; disable TLS 1.2
- Deploy X25519+ML-KEM-768 hybrid on all TLS 1.3 endpoints (Caddy or nginx patch)

+ 2 weitere detaillierte Schritte im technischen Bericht

Hauptmigration (3-12 Monate)

Zeitrahmen: 3-12

- Plan EJBCA PKI migration: evaluate HSM firmware PQC support (Thales Luna, Utimaco)
- Issue new ML-DSA-65 intermediate CA; begin dual-issuing certificates

+ 3 weitere detaillierte Schritte im technischen Bericht

Langfristig (12-24 Monate)

Zeitrahmen: 12-24

- Complete EJBCA root CA migration to ML-DSA-65 — re-issue all internal certificates
- Decommission all RSA-2048 key material from HSM

+ 2 weitere detaillierte Schritte im technischen Bericht