REPORT REGULATION & COMPLIANCE

Post-quantum readiness in 2026: what the EU's first deadline means for Belgian organisations

The EU's first post-quantum milestone falls on 31 December 2026. What NIS2, DORA and the CRA require, and a 12-month plan for Belgian organisations.



Sokaïna Jabbar
CEO, Co-Founder · Executive MBA
Reviewed by Carlos E. Avimadjessi

PUBLISHED	LAST REVIEWED	READING TIME
24 November 2026	24 November 2026	11 min

KEY TAKEAWAYS

- No EU or Belgian law yet names post-quantum cryptography. But NIS2, DORA and the Cyber Resilience Act all require cryptography that follows the state of the art, and the state of the art now has end dates for RSA and elliptic curves.
- The EU roadmap sets three milestones: start by the **end of 2026**, protect high-risk use cases by the **end of 2030**, and finish medium-risk ones by the **end of 2035**. NIST's dates match: deprecated after 2030, disallowed after 2035.
- 2026 is about knowing and planning, not buying: an inventory of your cryptography, a quantum risk analysis, questions to your suppliers and a written plan.
- Data that must stay confidential for 10 years or more is the priority. It can be recorded today and decrypted later, so the roadmap wants it protected by the end of 2030.
- An organisation without a cryptography team can do the first year's work with the people and lists it already has.

© 2026 Sorlos

Contents

01 Why the end of 2026 matters

02 The dates the EU and its partners have set

03 What the rules require today

04 How much time you really have

05 A 12-month plan for an organisation without a cryptography team

06 What to do next

07 Sources

Why the end of 2026 matters

In April 2024, the European Commission asked Member States to coordinate their move to post-quantum cryptography. In June 2025, the NIS Cooperation Group, where Member States work together under NIS2, answered with a coordinated roadmap. Its first milestone is 31 December 2026, five weeks after this Report is published.

The roadmap is addressed to Member States, not directly to companies. By the end of 2026, each Member State should have implemented the roadmap's "First Steps", established an initial national transition roadmap, and initiated "PQC transition planning and pilots for high- and medium-risk use cases". But the First Steps describe work that only organisations can do: inventories of cryptography, dependency maps, risk analysis, talks with suppliers. The roadmap also calls these steps "no-regret" moves that "support the compliance with cybersecurity regulations, in particular the NIS2 Directive".

So the question for a Belgian organisation is not whether the roadmap binds it. It is whether its supervisor, its clients and its board will expect it to have started. The rest of this Report sets out what the texts actually say, how much time the dates leave, and what to do in the next 12 months.

> NOTE
>
> This Report is information, not legal advice. Whether an obligation applies to you depends on your sector, your size, the services you provide and your role in the supply chain.

The dates the EU and its partners have set

The EU roadmap does not stand alone. The US National Institute of Standards and Technology (NIST), whose standards most products follow, published its final transition plan in October 2026, and the UK's National Cyber Security Centre (NCSC) published its own timeline in March 2025. The dates line up.

11 APRIL 2024

European Commission Recommendation

Member States are asked to coordinate their transition to post-quantum cryptography.

13 AUGUST 2024

First NIST post-quantum standards

FIPS 203 (ML-KEM) for key establishment, FIPS 204 and 205 for signatures.

23 JUNE 2025
EU coordinated roadmap
Common milestones for 2026, 2030 and 2035.

27 OCTOBER 2026
NIST transition plan
Final dates for deprecating and disallowing quantum-vulnerable algorithms.

31 DECEMBER 2026
EU milestone 1
First steps done, national roadmaps in place, planning and pilots started for high- and medium-risk use cases.

11 DECEMBER 2027
Cyber Resilience Act applies
Products with digital elements must protect confidentiality with state-of-the-art mechanisms.

31 DECEMBER 2030
EU milestone 2
Transition completed for high-risk use cases. NIST deprecates quantum-vulnerable public-key algorithms after 2030.

31 DECEMBER 2035
EU milestone 3
Transition completed for medium-risk use cases, and for low-risk ones as far as feasible. NIST disallows quantum-vulnerable algorithms after 2035.

Three points matter for planning.

The dates are about stand-alone use. For high-risk use cases, the roadmap says quantum-vulnerable public-key mechanisms “shall not be used stand-alone after the end of 2030”. It recommends “standardised and tested hybrid solutions, whenever feasible and suitable”: a hybrid key exchange combines a classical algorithm with a post-quantum one such as ML-KEM, so that security holds as long as either of them does. NIST notes that hybrid solutions add complexity and are “typically expected to be temporary measures”.

Key size does not buy time. NIST will deprecate quantum-vulnerable public-key algorithms after 2030 and disallow them after 2035, for RSA and elliptic curves at every security level. Moving from RSA-2048 to RSA-4096 does not change the dates. Our Insight Is RSA-2048 already broken? explains why.

Symmetric cryptography mostly stays. NIST “does not expect to need to transition away” from its symmetric standards, such as AES, as part of the migration. The work concerns key exchange and digital signatures, not the encryption of your disks and databases.

The UK gives the same rhythm from the organisation's side: a full discovery of where cryptography is used by 2028, the highest-priority migrations by 2031, and full migration by 2035.

Which of your systems are "high risk"?

The roadmap sorts use cases by quantum risk, based on three factors: how vulnerable the cryptography is, the impact if it were broken, and how long the migration would take. It gives a rough guide for systems that use today's public-key cryptography:

How the EU roadmap classifies quantum risk

SITUATION	RISK LEVEL	DEADLINE IN THE ROADMAP
Data that must stay confidential for 10 years or more, where a later breach would still cause significant damage	High	End of 2030
A migration that would take more than 8 years, for a system whose compromise has a high impact, such as software updates	High	End of 2030
Any other data whose confidentiality must be protected	Medium or high	End of 2030 or 2035
A migration that would take more than 8 years	Medium or high	End of 2030 or 2035

The first line is the harvest now, decrypt later problem: data intercepted today can be stored and decrypted once a large enough quantum computer exists. The roadmap draws the conclusion itself: data that must stay confidential for at least 10 years "should be protected from quantum computer attacks starting no later than by the end of 2030". It adds that migrating all relevant systems "might easily take about 5 to 10 years".

What the rules require today

Three EU texts cover most regulated Belgian organisations. None names an algorithm or sets a quantum deadline. Each asks for cryptography that is managed by policy and kept up to date with the state of the art.

Cryptography in NIS2, DORA and the Cyber Resilience Act

TEXT	WHO IT COVERS	WHAT IT SAYS ABOUT CRYPTOGRAPHY	APPLIES FROM
NIS2 (Belgian law of 26 April 2024)	Essential and important entities in the sectors listed in the law	Policies and procedures on the use of cryptography and, where appropriate, encryption; measures that take the state of the art into account	18 October 2024
DORA and Delegated Regulation 2024/1774	Banks, insurers, investment firms, payment institutions and other financial entities	A policy on encryption and cryptographic controls, with provisions to change the technology "on the basis of developments in cryptanalysis"	17 January 2025
Cyber Resilience Act	Manufacturers of hardware and software products with digital elements sold in the EU	Protect confidentiality "by encrypting relevant data at rest or in transit by state of the art mechanisms"	11 December 2027

The roadmap sums up why this matters at board level: NIS2 and DORA require "state-of-the-art cryptography" and "provide that the entities' management bodies can be held liable for failing to comply with these requirements".

NIS2 and the Belgian law

Article 21 of the NIS2 Directive requires "policies and procedures regarding the use of cryptography and, where appropriate, encryption", and measures that take into account "the state-of-the-art". The Belgian law of 26 April 2024 transposes it and has applied since 18 October 2024. The Centre for Cybersecurity Belgium (CCB) advises entities to use its CyberFundamentals (CyFun) framework; a validated implementation gives a presumption of conformity.

For DNS, cloud, data centre and managed service providers, and a few other digital services, Implementing Regulation 2024/2690 goes further. Their cryptography policy must name approved algorithms "following, where appropriate, a cryptographic agility approach", and be reviewed "taking into account the state of the art in cryptography". Our Insight Does NIS2 require post-quantum cryptography? covers these texts in detail.

DORA for financial entities

DORA has applied since 17 January 2025. Its technical standards (Delegated Regulation 2024/1774) are the most precise EU text on cryptography so far. Article 6 requires a policy on encryption and cryptographic controls, based on data classification and risk assessment, and that policy must include "provisions for

updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis". An entity that cannot update its cryptography must adopt mitigation and monitoring measures, record them and explain why.

Article 7 adds key management over the whole life of a key, and a register of certificates and certificate-storing devices, at least for ICT assets supporting critical or important functions. That register is a ready-made starting point for a cryptographic inventory.

The smallest financial entities, under DORA's simplified framework (Article 16), are not covered by these two articles and follow lighter rules.

The Cyber Resilience Act for product makers

The Cyber Resilience Act (CRA) applies from 11 December 2027 to manufacturers of products with digital elements, including software. Its essential requirements (Annex I) ask products to protect confidentiality "by encrypting relevant data at rest or in transit by state of the art mechanisms", and to allow vulnerabilities to be fixed through security updates.

Two details make the quantum question concrete for manufacturers. First, the support period for security updates must in general be at least five years (Article 13(8)): a product placed on the market in 2028 will still be supported after NIST's 2030 deprecation date. Second, the EU roadmap asks that products "with an expected lifetime beyond 2030" be upgradable to post-quantum cryptography, and that software and firmware updates be signed with post-quantum signatures.

What none of them says

None of these texts requires post-quantum algorithms today, and none sets a date by which you must use them. A supervisor cannot fault you for still using RSA in 2026. What they can reasonably ask is whether your cryptography policy follows the state of the art, whether you know where your quantum-vulnerable cryptography is, and whether you have a plan to replace it before the dates above.

How much time you really have

Nobody knows when a quantum computer able to break today's public-key cryptography will exist. NIST confirmed in October 2026 that none exists yet. Published estimates of the machine needed have fallen sharply, and in the Global Risk Institute's 2025 expert survey, such a machine is considered "likely" within 15 years. Our Insight Is RSA-2048 already broken? sets out the figures and their sources.

What you can measure is your own side of the equation: how long your data must stay confidential, and how long your migration will take. If the two together reach beyond the arrival of a quantum computer, you are already late for that data. Our Insight What

is the Mosca inequality? shows how to turn this into a priority list.

For most organisations, the migration time is the number they underestimate. Cryptography sits in websites, VPNs, email, identity systems, backups, databases, signed software, payment links and in every supplier that handles your data. Much of it you do not control directly: it changes when your suppliers change it.

A 12-month plan for an organisation without a cryptography team

The First Steps of the EU roadmap translate into a year of work that an organisation of 50 to 500 people can do with its IT team or provider. Nothing in this plan requires buying a product.

Months 1 to 3: an owner, and what you already know

- **Name an owner.** The work spans IT, security, procurement, legal and the business. One person must be accountable, with a mandate from management. The roadmap asks for the quantum threat to be part of "top-level risk management", so that it is discussed at board level.
- **Add the quantum threat to your risk register.** Record it as a risk with an owner and a review date, like any other.
- **Collect the lists you already have.** Certificate lists from your certificate authorities and cloud providers, your asset register, supplier contracts and, for financial entities, the DORA certificate register.

Months 4 to 6: the inventory and the risk ranking

- **Build a first cryptographic inventory** of your critical services: where cryptography is used, with which algorithms, keys and certificates, who supplies it, and how long the data must stay confidential. Our Insight What is a cryptographic inventory, and where do you start? explains what to record. The roadmap recommends a standard format such as CBOM (Cryptographic Bill of Materials) as the inventory grows.
- **Map the dependencies** between your applications, platforms and suppliers. They decide what can move first.
- **Rank each use case** as high, medium or low risk using the table above. Long-lived confidential data and software updates come first.

Months 7 to 9: suppliers and policy

- **Ask your critical suppliers** which algorithms their products use, whether and when they support the NIST post-quantum standards, and how the change will reach you. Add post-quantum readiness to new contracts and renewals.

- **Update your cryptography policy.** Name the approved algorithms, say how quantum-vulnerable ones will be replaced, and set a review date. For NIS2 digital providers and DORA entities, link it to the requirements above.
- **Require crypto-agility in what you buy or renew.** Any system you replace before 2030 should let you change algorithms without being redesigned.

Months 10 to 12: a written plan and a first pilot

- **Write a transition plan** approved by management: priorities, owners, dates aligned with 2030 and 2035, and a budget spread over several years. It is the document a supervisor, an auditor or a large client will ask for.
- **Run a first pilot** on a high-risk use case, for example enabling hybrid key exchange on an external service where your supplier already supports it. The roadmap asks for planning and pilots for high- and medium-risk use cases to have started by the end of 2026.

What to do next

1. **Before 31 December 2026:** name an owner, add the quantum threat to your risk register and start collecting the lists you already have.
2. **Within six months:** have a first cryptographic inventory of your critical services, ranked by risk.
3. **Within nine months:** send your questions to your critical suppliers and update your cryptography policy.
4. **Within a year:** have a management-approved transition plan, and a first pilot under way for a high-risk use case.

Sources

1. NIS Cooperation Group, EU PQC Workstream, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (Part 1, version 1.1), 23 June 2025.
   https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
2. European Parliament and Council of the EU, Directive (EU) 2022/2555 (NIS2 Directive), Article 21, 14 December 2022.
   https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
3. European Commission, Implementing Regulation (EU) 2024/2690 on cybersecurity risk-management measures, Annex, point 9 (Cryptography), 17 October 2024.
   https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
4. Centre for Cybersecurity Belgium, The NIS2 Law (Law of 26 April 2024), 26 April 2024.
   https://atwork.safeonweb.be/nis2

5. European Parliament and Council of the EU, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), Articles 16 and 64, 14 December 2022.
https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
6. European Commission, Commission Delegated Regulation (EU) 2024/1774 on ICT risk management tools, methods, processes and policies (DORA), Articles 6 and 7, 13 March 2024.
https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj/eng
7. European Parliament and Council of the EU, Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 13, Article 71 and Annex I, 23 October 2024.
https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
8. National Institute of Standards and Technology (US), FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, 13 August 2024.
https://csrc.nist.gov/pubs/fips/203/final
9. National Institute of Standards and Technology (US), Transition to Post-Quantum Cryptography Standards (NIST IR 8547), 27 October 2026.
https://csrc.nist.gov/pubs/ir/8547/final
10. National Cyber Security Centre (UK), Timelines for migration to post-quantum cryptography, 20 March 2025.
https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
11. Michele Mosca and Marco Piani, Global Risk Institute and evolutionQ, Quantum Threat Timeline Report 2025, 9 March 2026.
https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

AI tools assisted with the research, drafting and fact-checking of this article. The author wrote and approved the final text, and a second reviewer checked every source against the original.

Need assistance for your transition?

Sorlos runs quantum readiness assessments. We assess your risk from your cryptographic inventory and design a migration roadmap you can rely on. Vendor-independent, from Brussels.

Talk to us · www.sorlos.eu/#contact



Sokaïna Jabbar

ICT and emerging Technology leader with 12+ years in operational management, innovation, tech strategy, and intra/entrepreneurship.

This PDF reproduces the article as of 24 November 2026. The online version, kept up to date, is at https://www.sorlos.eu/insights/post-quantum-readiness-2026/. © 2026 Sorlos. All rights reserved.