EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PQC Maturity Assessment Framework

A self-assessment approach for EU SMEs

Dr. Prokopios DROGKARIS – Cybersecurity Expert & Deputy DPO

byRisk International Workshop

04-11-2026

Future-proofing protection of personal data

Risk

A sufficiently capable quantum computer could undermine widely used public-key cryptography

“Harvest now, decrypt later” puts long-lived personal data at risk

GDPR

Article 32 – Security of processing

Taking into account the **state of the art**, the **costs of implementation** and the nature, scope, context and purposes of processing …, the controller and the processor shall **implement appropriate technical and organisational measures** to ensure a level of security appropriate to the risk…

Migration

Treat PQC as a risk-management and crypto-agility programme.

Assess the quantum risk now and protect personal data.

PQC Transition



How can SMEs understand where they stand?

How can they start the migration journey?

How can they realize the effect of each action?

Why (another) maturity assessment framework?

Convert SMEs awareness to actionable way(s) forward

01	A “common” baseline	Provide a common approach to self-assess
02	Reveal gaps	Identify areas for improvement across six domains
03	Guide actions	Translate low scores into practical next steps
04	Support migration	Understand how each action gets you closer

Self assessment → No need to share outcome or feel “being audited”

! No direct interplay with National Roadmaps and regulatory guidance !

Framework Overview

01 **Cybersecurity foundations**

Establishing the baseline

02 **Governance and asset inventory**

Ownership

03 **Cryptography management**

Agility

04 **Quantum awareness**

Threat understanding

05 **Regulatory and resilience context**

Obligations

06 **PQC transition planning**

Migration actions

6
DOMAINS

36
QUESTIONS IN TOTAL

6
QUESTIONS PER DOMAIN

4
POSSIBLE ANSWERS

A small snapshot

1.4 Do you monitor your systems for vulnerabilities, threats and potential cybersecurity incidents?

WHY IT MATTERS

Continuous monitoring enables you to identify vulnerabilities and threats early or before an incident occurs. Should an incident take place, it enables you to address it immediately and minimize the impact.

GUIDANCE

(if your reply is No or Partially)

Enable logging and alerts in systems and tools such as firewall, antivirus. If in-house capacity is limited, a managed security service can support you and monitor on your behalf.

- ☐ No (0 pt)
- ☐ Partially / in progress (1 pt)
- ☐ Yes (2 pt)
- ☐ N/A

3.2 Do you maintain a cryptographic usage inventory — where each cryptographic component is used and by whom?

WHY IT MATTERS

The context of using cryptographic elements can support in identifying dependencies, owners and criticality of the data being protected.

GUIDANCE

(if your reply is No or Partially)

Supplement the inventory with information on system and data each component protects, who depends on it and whether it supports business sensitive data.

- ☐ No (0 pt)
- ☐ Partially / in progress (1 pt)
- ☐ Yes (2 pt)
- ☐ N/A

3.5 When developing or acquiring a new product or service, do you set requirements for the cryptographic elements being used?

WHY IT MATTERS

Predefined cryptographic requirements reduce the risk for ending up with non-adequate level of cryptographic protection, either short or long term.

GUIDANCE

(if your reply is No or Partially)

Add specific requirements based on good practises and guidance from national cybersecurity authorities.

- ☐ No (0 pt)
- ☐ Partially / in progress (1 pt)
- ☐ Yes (2 pt)
- ☐ N/A

4.2 Is your management/leadership aware of quantum technologies and quantum threats?

WHY IT MATTERS

Management awareness is critical for prioritization and allocation of relevant resources.

GUIDANCE

(if your reply is No or Partially)

Provide a concise note with problem statement, possible transition timelines and resources along with possible process owners.

- ☐ No (0 pt)
- ☐ Partially / in progress (1 pt)
- ☐ Yes (2 pt)
- ☐ N/A

Crunching the numbers

Maturity Scores

0-33%	34-66%	67-99%	100%
Initial	**Developing**	**Established**	**Optimised**
Prioritise	Reduce Gaps	Refine	Maintain
Little seems to be in place	There is a gap that the organization needs to gradually reduce.	Most elements seem to be in place however some refinement and maintenance will be required.	All elements seem to be in place and the organization shall work in maintaining this posture.

Self-assessment is (only) the starting point…

Feel free to have a go!



https://ec.europa.eu/eusurvey/runner/PQC_maturity_assessment

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Thank you for your attention

 +30 28 14 40 9711

 info@enisa.europa.eu

 enisa.europa.eu

ENISA
European Union Agency
for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium