

Our journey to CRA

23rd October 2025

Petri Maanonen

Director Product Management Office

The Qt Company



CRA

The Qt Group

Helping our customers improve productivity in the entire product development process.



- Millions of Users
- Every 4th C++ developer using Qt
- Qt Community Edition is the de facto UI framework for Embedded Linux
- 3500+ Commercial Customers
- 70+ Industries
- 900+ Employees
- 209 million Euro Revenue (2024)



Disclaimer

This is not legal advice,
instructions or commitment for
CRA or related compliancy.

A scenic landscape featuring a winding asphalt road with white dashed lines, bordered by wooden guardrails. The road leads through a dark, rocky, and sparsely vegetated area towards a range of rugged, light-colored mountains under a blue sky with scattered white clouds. A large, semi-transparent white 'CRA' watermark is centered over the image, with a bright yellow diagonal line passing through it from the top right to the bottom left.

CRA

Heard there is new
Cybersecurity
legislation coming
up. Perhaps we
should have a look
at it...



2024

2025

We get our first
customer
queries about
CRA

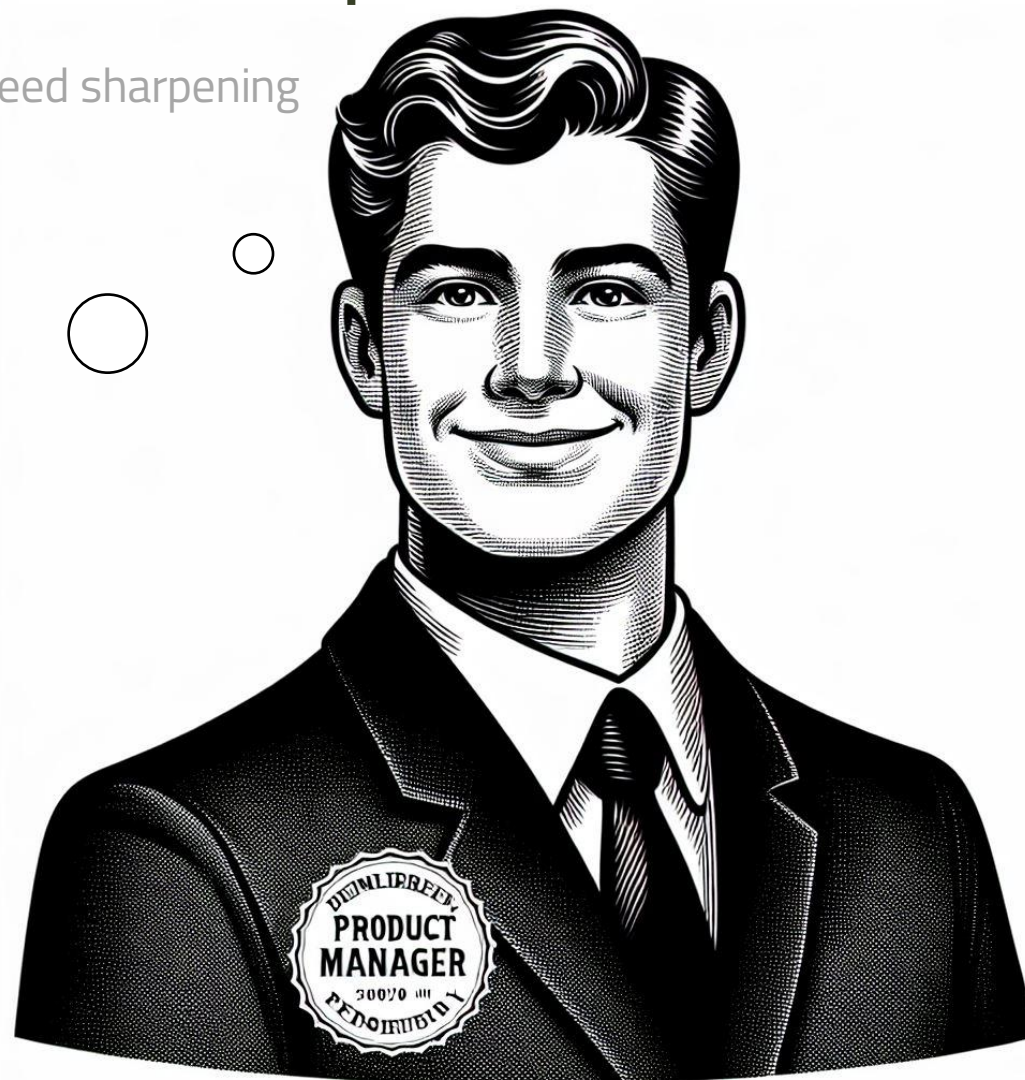
This triggered initial
discussions in
Product
Management and
R&D

2024

2025

- ✓ Vulnerability handling in action already, notification practices need sharpening
- ✓ R&D processes aligned, we are working on ISO27001
- ✓ 3rd party components documented
- SBOM not done, we need to do it

How hard can
this be, think
we got this...



2024

2025

More customer requests

–

We draw our first roadmap
and internal FAQ...

2026

2027

Average customer project creating a product is ~18 months

CRA comes into force
for our customers
early in 2027

2026

2027

Average customer project creating a product is ~18 months

We should be
ready in the 2nd
half of 2025

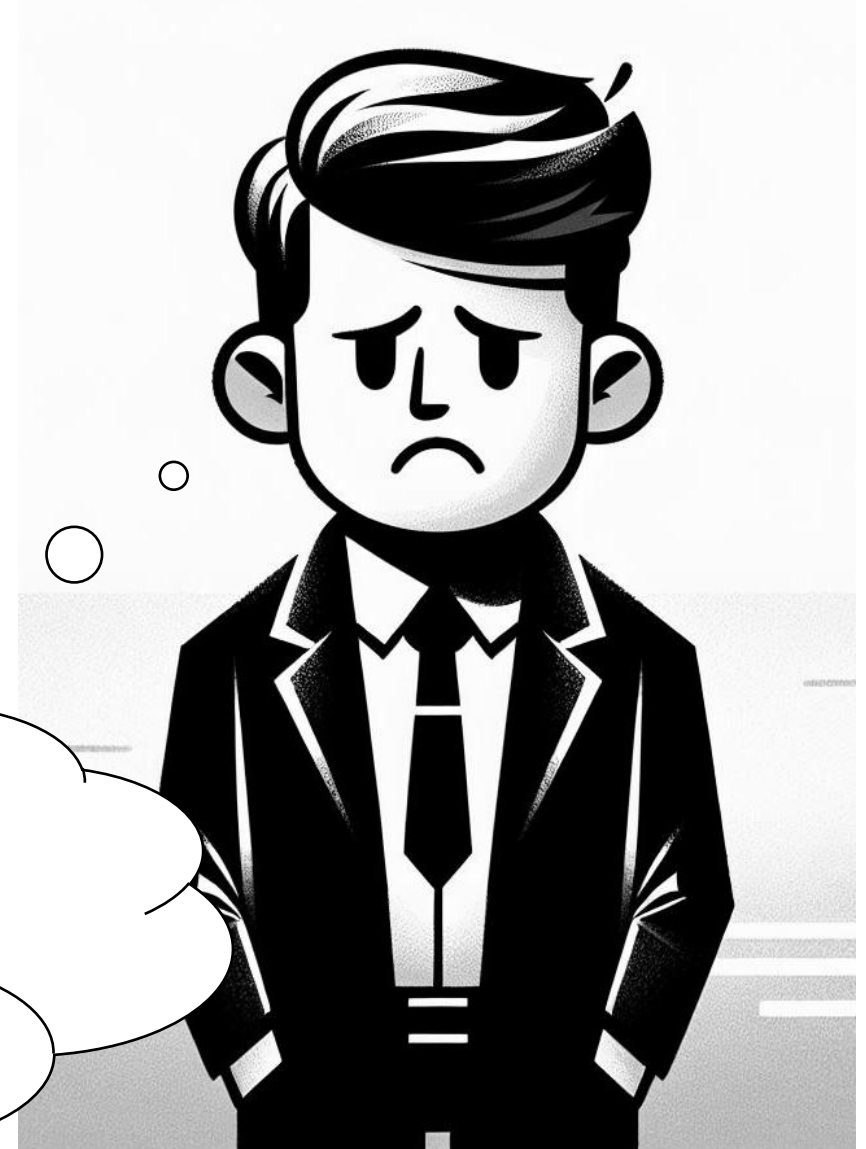
CRA comes into force
for our customers
early in 2027

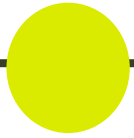
2024

2025

Also, our own legal gets involved, plus we read the new draft again

This is going to be quite a lot of work





2025

Decision:
Establish CRA
program with
dedicated
resources and
product area
owners

Systematic requirements gathering

Create a budget

Manage roadmap

Customer messaging

Sales enablement

Internal communications

Process, quality, legal, competence

Working streams for products

<https://www.qt.io/blog/qt-group-achieves-iso-270012022-certification-strengthening-data-security-and-privacy>



Products Solutions Resources Support



Learning Hub Developers

Price. Buy.

Download. Try.

BLOG Latest Biz Circuit Dev Loop Design Sphere QA Orbit

Qt Group Achieves ISO 27001:2022 Certification, Strengthening Data Security and Privacy

June 07, 2024 by [Jussi Mikkonen](#) | [Comments](#)

Qt Group has successfully achieved the ISO 27001:2022 certification. This achievement is a significant milestone in the company's cybersecurity strategy and underscores its commitment to ensuring the highest levels of information security management (ISMS).

What is ISO 27001:2022?

ISO 27001:2022 is the world's best-known standard for Information Security Management Systems (ISMS), and our certification reflects compliance with 100% of the standard's requirements. ISMS is a documented management system comprising a set of security controls that protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

The basic goal of ISO/IEC 27001 is to protect three aspects of information:

- Confidentiality: Only authorized personnel have the right to access information
- Availability: The information must be accessible to authorized personnel whenever it is needed

Subscribe to our newsletter

[Subscribe](#)

Try Qt 6.8 Now!

Download the latest release
here: www.qt.io/download.

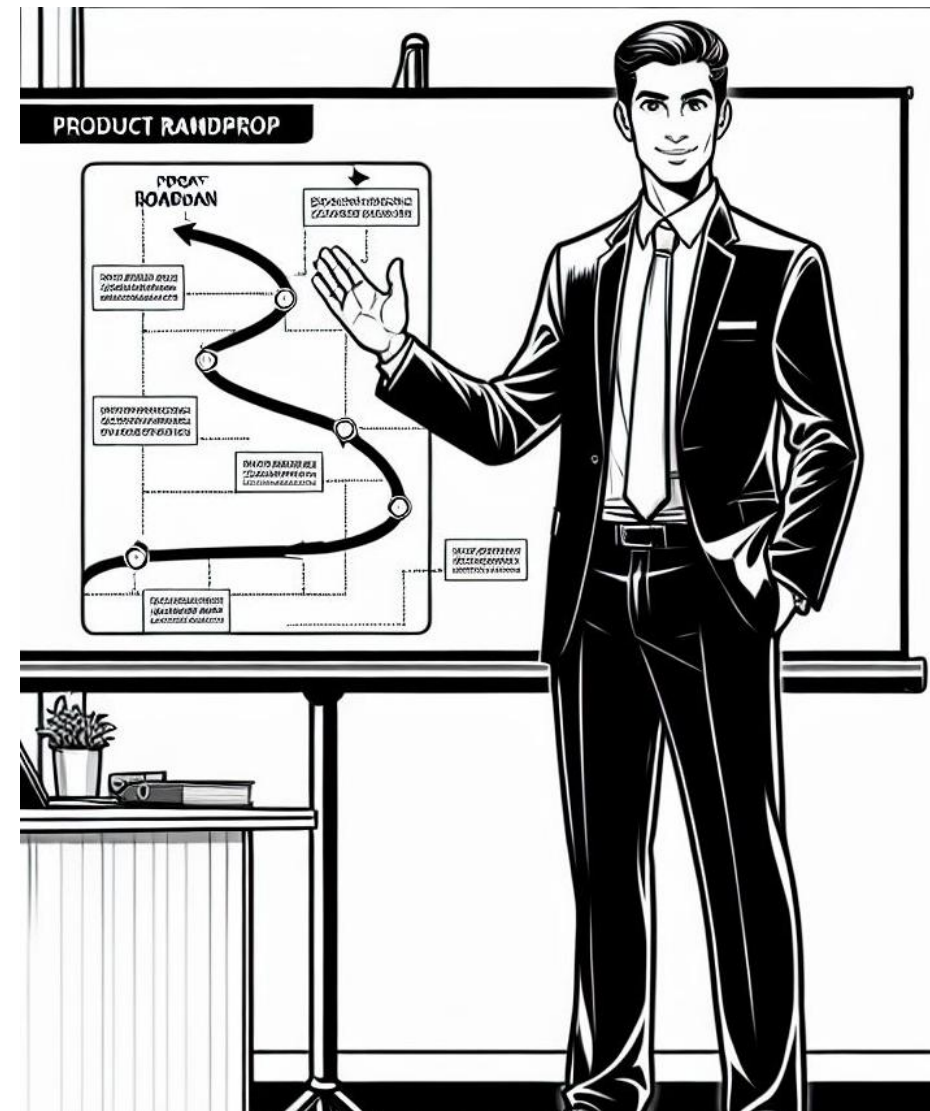
Qt 6.8 release focuses on technology trends like spatial computing & XR, complex data visualization in 2D & 3D, and ARM-based development for desktop.

We're Hiring

Check out [all our open positions here](#) and follow us on Instagram to see what it's like to be #QtPeople.

2025

More customer
workshops for CRA

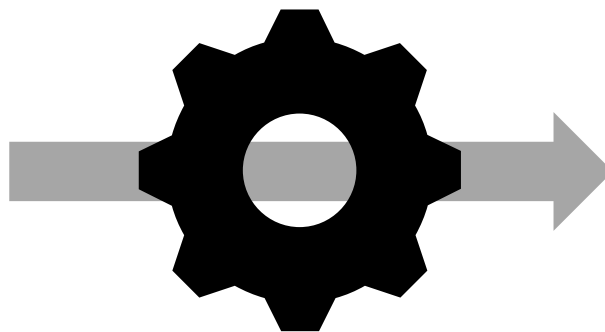


Examples of the kind of questions we run into:

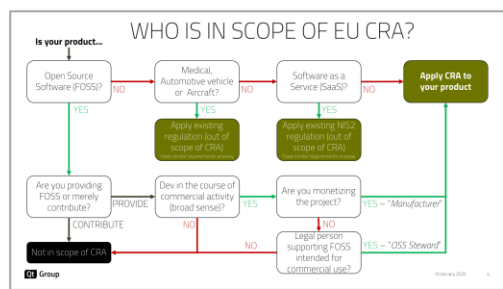
How do the dual licensing
and CRA fit with each other?

Policy and process to mark parts
that are "*Safety Critical*"

What is our role and
category?



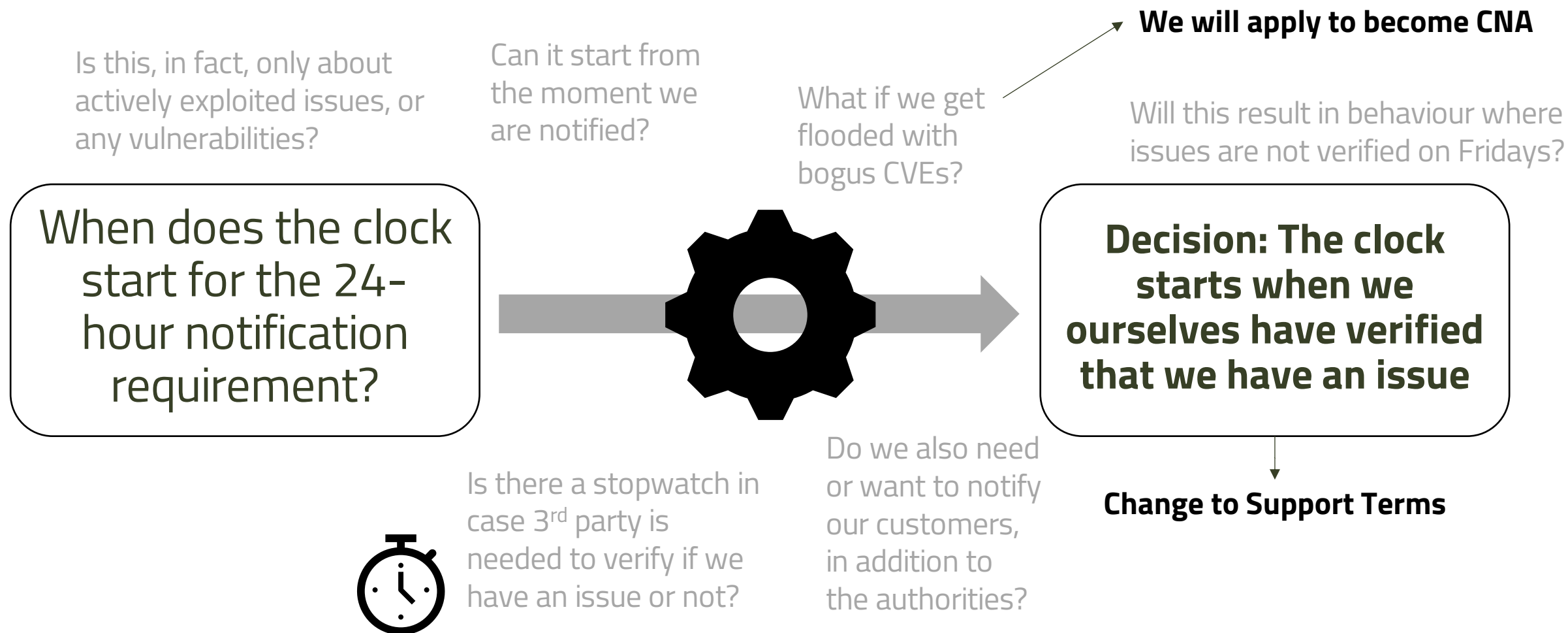
**For Qt Community Edition,
we are a "*Steward*".
For commercial Qt, we are
"*Manufacturer*", but...**



We have customers
doing class 1 and 2
products?

For the full framework,
being Class 1 or 2 is
way too heavy

Examples of the kind of questions we run into:



<https://www.qt.io/blog/qt-6.8-software-bill-of-materials>

Qt Group

Products Solutions Resources Support



Learning Hub

Developers

Price. Buy.

Download. Try.

BLOG Latest Biz Circuit Dev Loop Design Sphere QA Orbit

Qt 6.8 Software Bill of Materials

December 03, 2024 by [Alexandru Croitor](#) | [Comments](#)



An SBOM is:

A machine-processable document containing the details and supply chain relationships of various components used in building software, similar to food ingredient labels on packaging.

Why SBOM?

Building and shipping software requires a lot of care. Some aspects of building software are often neglected yet are considered important by many. I'm talking about security, build reproducibility, supply chain tracking, license compliance, and copyright attribution.

The European Union partly shares that opinion, which is why, among other things, it is adopting the [Cyber-Resilience Act \(CRA\)](#) regulation, which aims to improve the security of hardware and software.

The CRA mentions automatic security updates, as well as vulnerability and incident reports. Now, software

Subscribe to our newsletter

Subscribe

Try Qt 6.8 Now!

Download the latest release
here: www.qt.io/download.

Qt 6.8 release focuses on technology trends like spatial computing & XR, complex data visualization in 2D & 3D, and ARM-based development for desktop.

We're Hiring

Check out [all our open positions here](#) and follow us on Instagram to see what it's like to be #QtPeople.

2025

Subcontract an external party to help with requirements gathering and objective gap analysis



Systematic and objective interviews across the org

Read through the current process and product documentation

Understand the current state and maturity per product area

Compare the Qt state against the CRA text and industry practices

Create a detailed list of requirements

Feedback
loop

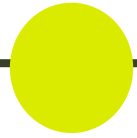
2026

Out of this, we have the Requirements

JIRA:
~80 items in To Do
< 10 *In Progress*
< 5 *Done*

XLS: Additional 50+ items not yet in JIRA

[illegible]

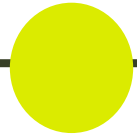


2025

2026

Identified Requirement categories

- Cybersecurity risk assessment processes and practices
- Product Maintenance Period practices and documentation
- Secure Software Development Lifecycle (SSDL)
 - Design and software architecture
 - Implementation
 - Testing
- Software Bill of Materials (SBOM)
- Vulnerability Management
 - Especially 3rd party software
 - Patching and releasing
 - Incident response
- User Instructions and public documentation
- General



2025

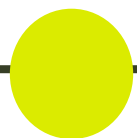
Identified Requirement categories

- Cybersecurity risk assessment processes and practices
- Product Maintenance Period practices and documentation
- Secure Software Development Lifecycle (SSDL)
 - Design and software architecture
 - Implementation
 - Testing
- Software Bill of Materials (SBOM)
- Vulnerability Management
 - Especially 3rd party software
 - Patching and releasing
 - Incident response
- User Instructions and public documentation
- General

Requirement definition

- Description
- Priority (P1 to P5)
- Steps (to re-produce or fulfil)
- Outcome
- JIRA ticket(s) (created, refined)
- Dependencies
- Justification
 - Industry best practice
 - CRA Article reference
 - OWASP SAMM reference
- Needed schedule

2026
















Example:

▪ **QTBUG-120586 Epic: Create automated SBOM process for Qt framework and tools**

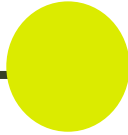
- **What is the benefit? Why is this valuable?** Making manual work to create SBOM (Software Bill of Materials) information unnecessary.
- **What are common use cases?** Licence due diligence and compliance: Identifying copyright, license information for deliverables (license compliance). Configuration management / Cybersecurity: Identifying software components and versions that end up in deliverables.
- **Relevant standards:** SPDX (currently using SPDX 2.1) and/or CycloneDX
- **SBOM Types:** Source SBOMs for source deliverables, Binary SBOMs for binary deliverables
- **Overview of the task:** Generate SBOMs for all relevant Qt products. Automate SBOM generation to ensure efficiency and accuracy. For the Qt Framework, consider how to address customer demand for SBOMs specific to host-target combinations. The CRA does not require the provision of SBOMs to customers, so this is a business question.
- **Steps** 1. Automate SBOM generation for all products. 2. Generate SBOMs for all versions of all Qt products. 3. For the Qt Framework, consider how to address customer demand for SBOMs specific to host-target combinations.
- **Outcome:** Automated SBOM generation for all Qt products and an SBOM generated for each version of all Qt products. The SBOM must be provided in a machine-readable format covering at the very least the top-level dependencies of the product.
- **Reasoning why this is needed:** The CRA requires that Qt produce a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies for each product. Generating accurate SBOMs manually is not scalable, and automation is thus necessary.
- **CRA reference:** Annex I, Part II § 1, link: <https://data.consilium.europa.eu/doc/document/PE-100-2023-INIT/en/pdf>
- **OWASP SAMM reference:** Secure Build practice includes activities such as keeping a record of all dependencies used throughout the target production environment, i.e., generating a bill of materials for every application.
- **Needed schedule:** This is mandated by the EU CRA by 11.12.2027. This can be done any day earlier.

- **QTBUG-120586** Epic: Create automated SBOM process for Qt framework and tools

- Note: You can find our (public) CRA requirements under bugreporst.qt.io with query "labels = EUCRA"

▼ Issues in epic			
QTBUG-122899	Generate SBOM from Qt build system		IN PROGRESS
QTBUG-125211	Generate SBOM for Qt Sources		IN PROGRESS
✔ QTBUG-126403	Use only valid SPDX expressions in LicenseId (qt_attribution.json)		CLOSED
✔ QTM-2179	Blog post about Qt SBOM tools		CLOSED
QTBUG-128320	Generate an SBOM for qttranslations		IN PROGRESS
QTBUG-128893	sbom for qtpdf gets lost , as it ends up as qtwebengine sbom		IN PROGRESS
QTBUG-129601	Provide custom SBOM's in deployment tooling		OPEN
QTCREATORBUG-31681	Create automated SBOM process for Qt Creator		OPEN
QTBUG-129901	Provide an SBOM for Qt WebEngine And Qt Pdf		OPEN
QTBUG-130959	SBOMs for Qt legacy versions as committed to customer(s) in Agreements [Spike]		OPEN
QTBUG-131377	Include Chromium in SBOM		REPORTED
QTBUG-131434	qtqa license test must read Source SBOM		OPEN
✔ QTBUG-131477	Review SBOM generation and documentation to include third party components		CLOSED

2025



2026

What we have worked on during 2025 in preparation for CRA compliance.

- Threat analysis and risk assessment
- Product level risk assessment and processes
- Product Maintenance Period practices for the whole portfolio
- Creating more material to support CRA communications
 - Qt World Summit presentations
 - **Vision paper and CRA landing pages** www.qt.io/cra
 - Blogs, webinars, sales enablement, presentations, workshops with customers...
- Software Bill of Materials (SBOM) for the whole portfolio
- Vulnerability Management
 - Company-level unified process
 - Early Warning List per product
 - Incident response
 - ENISA interface
- User Instructions and public documentation

The EU Cyber Resilience Act (CRA)

Are You Ready?

CRA is a new piece of regulation that aims to ensure lifetime security and resilience against cyber threats for all products with digital elements. All manufacturers that sell their products in the EU market are responsible for their product's security throughout its lifetime, including 3rd party components, maintenance, documentation and official assessments.

Pick a CRA Topic to Learn More*



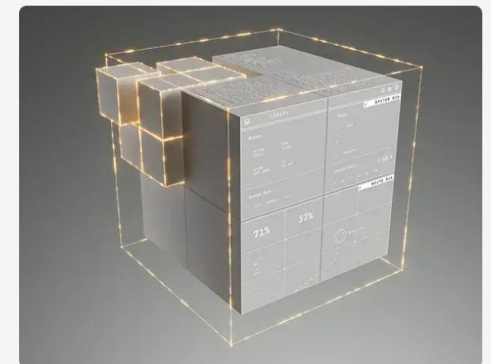
Vision Paper

Food for Thought on the EU Cyber Resilience Act

Get your free CRA Vision Paper for new angles on how to navigate the EU Cyber Resilience Act with confidence. Learn how the CRA reshapes product development and how you can leverage compliance as a competitive edge. Qt Group shares insights from decades of experience in regulated industries, topped with expert interviews.

No sign-up required.

[Get the Vision Paper Now](#)





High-level summary of the findings (so far):

- Many things are, in fact, done, but are missing some
 - Documentation (e.g., process documentation)
 - Evidence of being done (e.g., recorded results and checks, ability to demonstrate product level compliance systematically)
 - Cross-organization practices were repeated the same way in all teams
- We have competence gaps, and this will also be a (company culture) change management project
- Doing ISO27001 in 2023-2024 really helped us towards CRA
- We will need a solution for 3rd-party software management
- All things are not P1 priority; there are also lower priority items

Things we still need to address....

To what degree do we apply an SSDLC?

Change management and security champions

Competencies ramp up.
How do we do that?

How to tackle CRA with emerging products?

Will a certifying party be able to help us certify our products in time?

OSS Stewardship and Qt position?

How do we communicate the CRA value?

How about all other Acts in EU legislation?

What are the CRA items' ranking against all other work at Qt?

How do we engage with 3rd party software providers?

Exempt verticals (medical, automotive, etc), are they really exempted?

Can we network with colleagues? Do they have the same issues and questions?

Q&A?