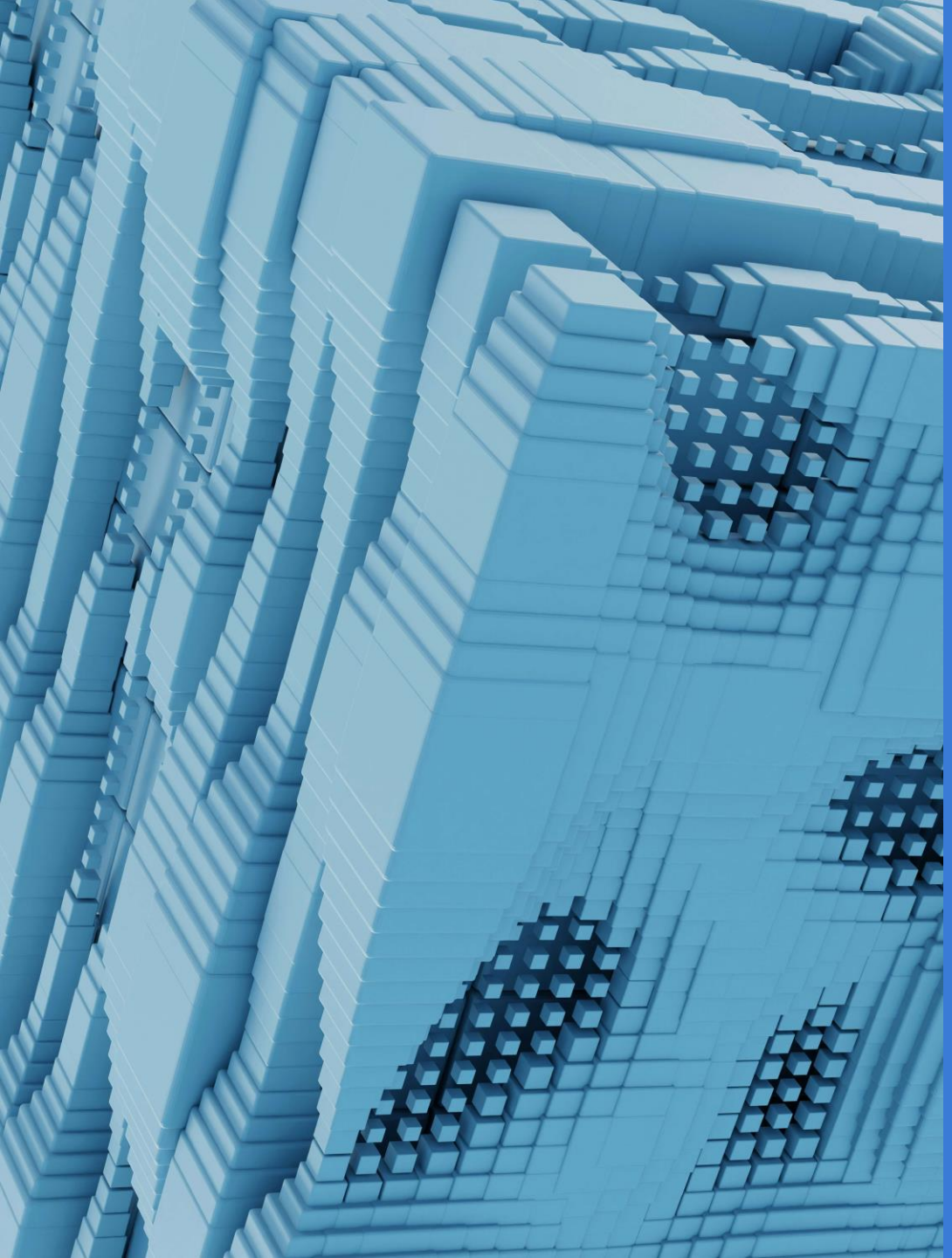


Mastering the CRA

Webinar

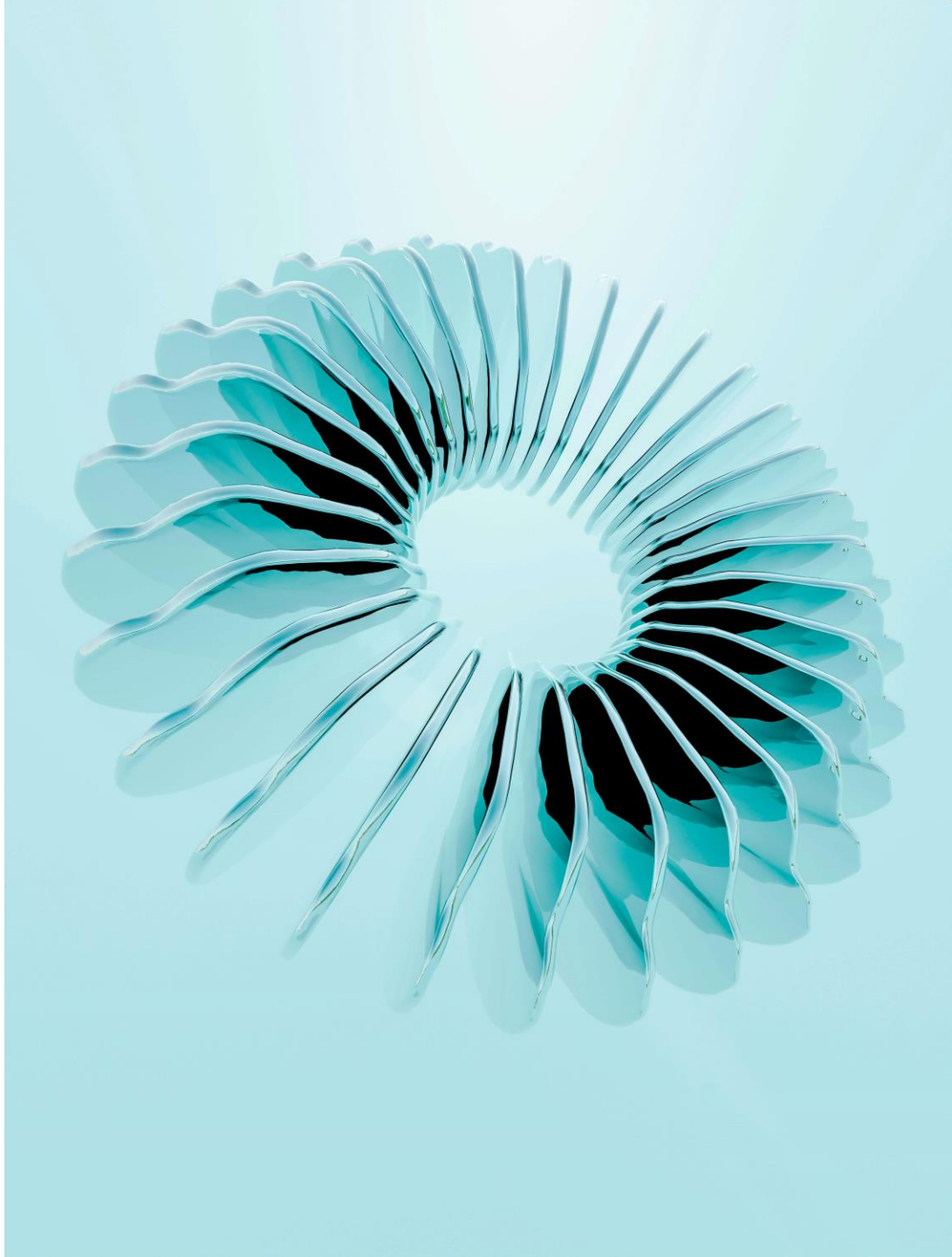
Nemko Digital

March 5, 2026

Nemko Digital

CRA webinar: topics today

1. Introduction to Nemko Digital
2. Overview of CRA
    i. Timeline
    ii. Scope
    iii. Requirement
    iv. Approach towards compliance
3. Getting ready for testing
    i. Testing preparation
    ii. Testing execution
    iii. Result & Certification
4. How to get started & next steps
5. Q&A



With you today

Daniel Breive Havre
Senior Cyber Security Evaluator
Nemko Group

- **Cyber security expert:** Turns cybersecurity complexity into clear, actionable strategies grounded in strong analytical expertise (NTNU background in electronic system design & signal processing).
- **Product digital safety:** Helps clients strengthen product security and manage digital risk with pragmatic, business-focused guidance.
- **Security-by-design:** Drives security by design to build resilience and long-term trust.

Bas Overtoom
Sr. AI Trust Expert
Nemko Digital

- **Experienced AI & Data Executive:** +10 years of consultancy experience, driving AI and data transformations for top global organizations.
- **Responsible AI Advocate:** Passionate about RAI to address business, social, and environmental challenges.
- **Global Business Expertise:** Strong international background i.e., 7 years in Asia, fostering cross-cultural collaboration. Leads global BD at Nemko Digital, promoting AI Trust worldwide.
- **VC Advisor for AI Scale-Ups:** Supports AI startups within a prominent Dutch VC fund to achieve global growth.

Pep van der Laan, Ph.D.
Digital Trust Expert
Nemko Digital

- **Scaling AI impact**: +10 years in realizing business value by scaling AI-powered digital products from initial proof-of-concept to enterprise-wide solutions.
- **Strategy advisory:** Extensive experience shaping the AI & Data transformation and architecture for global leaders and national champions across industries.
- **Capability building:** Led a team of 90 data engineers, AI developers, and data scientists through the transformation from the traditional consulting model and introducing modern delivery and development practices.
- **Growing Digital Trust:** Recognized for consistently bridging the gap between technology and the risk & legal stakeholders, building mutual understanding. Certified as ISO 27001 and ISO 42001 Lead Auditor.

Introduction Nemko Digital

Nemko: Compliance without Complexity

Strong heritage

1933 — Established by the Norwegian government as *Norges Elektriske Materiellkontroll*

1991 — Became independent self-owned private foundation

1992 - 2003 — Established offices and laboratories around the world

2020 — Launched Cybersecurity services

2024 — **Established *Nemko Digital* to consolidate AI Trust services**

Global reach & local presence

28 locations on 3 continents

Over **850** employees worldwide.

Offering services in more than **150** countries

Serving **7,000** customers across **80** countries.

In June 2025, Nemko signed a strategic partnership with KSA to shape the future of AI certification and trust in Korea and beyond

Proven track record

Roster of clients and services (not exhaustive)

SAMSUNG Panasonic LG JOTRON WÄRTSILÄ KÄRCHER

What is top-of-mind for our clients?

We deliver Digital Trust through end-to-end compliance and advisory support, combining technical, regulatory, and process expertise.

Regulatory Compliance — Beyond AI

Technical Assurance / AI Testing

ISO Readiness
ISO 42001, ISO 27001…
— Beyond AI

AI Assurance Tools

Global Market Access — Beyond AI

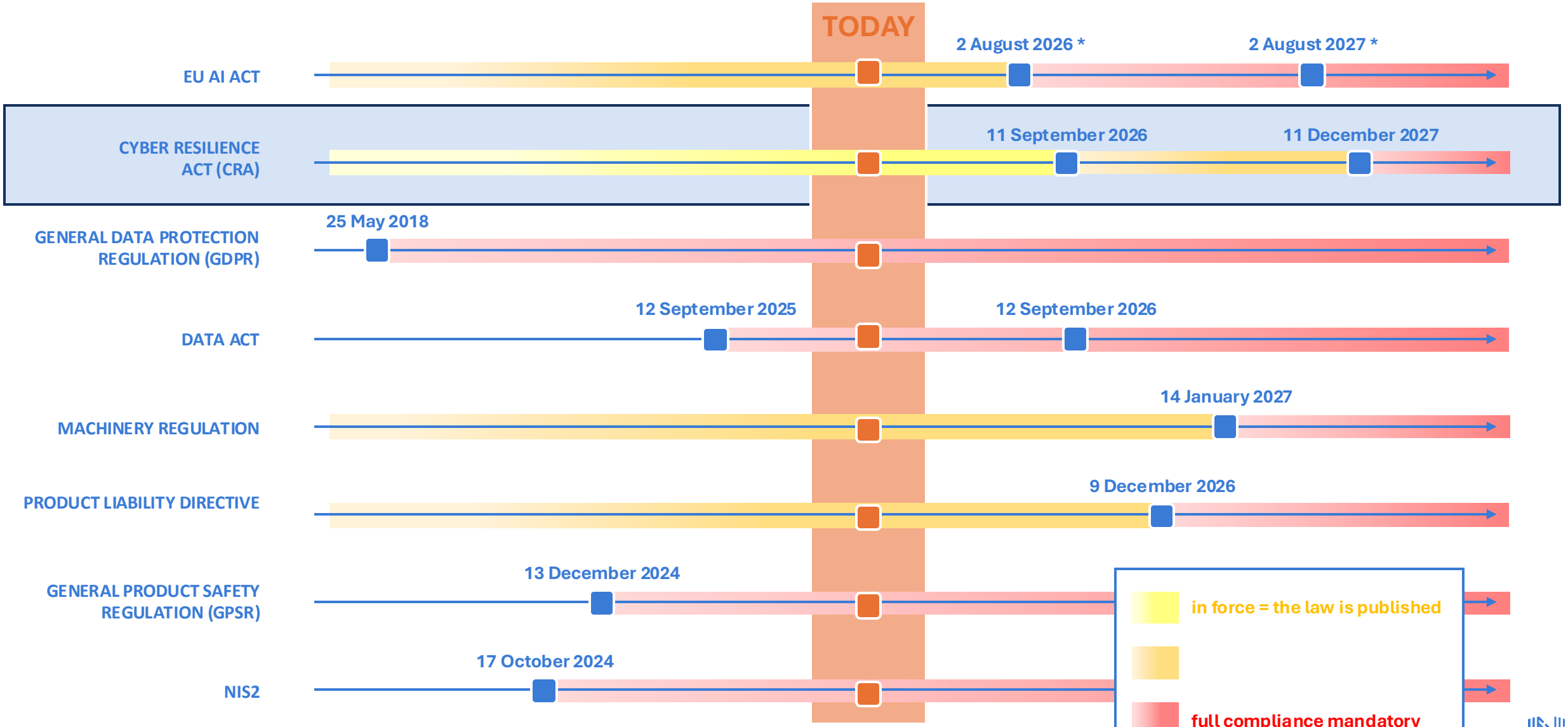
Governance Maturity — Beyond AI

Nemko AI Trust Mark

Strategy and roadmaps — Beyond AI

Why the CRA

The CRA is part of a broader framework of digital regulations



** Timeline subject to change due to proposed Digital Omnibus package*

CRA: Cyber Security for products

Fines up to
€ 15M or 2.5% of
global turnover

Objective of the CRA (EU) 2024/2847 is to **reduce cybersecurity vulnerabilities** for **products with digital elements**[1] and create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements

Key concepts:

- **Products with digital elements:** the CRA concerns both hardware and software
- **Remote data processing:** data processing at a distance is in scope of the CRA if it is essential for functioning
- **Support period:** CRA obligations stretch over the full product lifecycle
- **Software Bill of Materials (SBOM):** CRA obligations cover the full digital supply chain

Key dates:

- **11 September 2026**: Mandatory incident reporting. manufacturers must report serious security incidents within strict timelines.
- **11 December 2027:** Full compliance with CRA required. Non-compliant products cannot be sold in the EU.

Links to other regulations

The CRA has important connections with the broader EU legislative framework

Radio Equipment Directive (RED)

- RED incudes radio, Electromagnetic compatibility (EMC), safety and cyber requirements
- RED cyber requirements are notably more limited than CRA requirements: additional effort is required to prove CRA compliance

AI Act

- High-risk AI systems that comply with CRA requirements have presumption of conformity on cybersecurity requirements as set out in the AI Act

Exceptions for specific product categories

Examples:

- Motor vehicles (EU) 2019/2144,
- Aviation (EU) 2018/1139 and
- Medical devices (EU) 2017/745&6

The way to Demonstrate conformity differs by product category

Cybersecurity certificate

Critical products[1]

- Hardware devices with security boxes
- Smart meter gateways within smart metering systems
- Smartcards

Conformity assessment procedure

Important Products[1]

Class I

- Identity management systems
- Browsers
- Password managers
- Malware protection software
- VPN products
- Network management systems
- SIEM systems
- Boot managers
- Key/certificate issuance software
- Network interfaces
- Operating systems
- Routers, modems and switches
- Microprocessors with security function
- Microcontrollers with security function
- ASIC & FPGA with security function
- Smart home GP VAs
- Smart home products with security functionalities
- Internet connected toys
- Personal wearables for health monitoring

Class II

- Hypervisors and container runtime systems
- Firewalls
- Tamper-resistant microprocessors
- Tamper-resistant microcontrollers

Self-declaration

Default Products

- All the rest

1. Implementing regulation (EU) 2025/2392 provides the official technical description of the categories of important and critical products with digital elements, as required by the CRA.

Overview of key CRA requirements

The Cyber Resilience Act puts requirements both on the **products** with digital elements and on the processes that **manufacturers** of these products have in place

Product requirements

- Secure by default and design
- Security updates
- Data minimization
- Resilience (after incidents)
- User information
- Data transfer

Process requirements

- Vulnerability risk assessment
- Testing and review
- Information sharing (vulnerabilities and updates)
- Secure dissemination of security updates

Overview of key CRA requirements

The Cyber Resilience Act puts requirements both on the **products** with digital elements and on the processes that **manufacturers** of these products have in place

Product requirements

- Secure by default and design
- Security updates
- Data minimization
- Resilience (after incidents)
- User information
- Data transfer

Process requirements

- Vulnerability risk assessment
- Testing and review
- Information sharing (vulnerabilities and updates)
- Secure dissemination of security updates

What this asks from organizations:

- Integrating **product security** with **organizational governance**
- Moving from ad-hoc controls to **repeatable, documented processes**
- Linking **engineering**, **compliance**, and **operational security**
- Embedding continuous **vulnerability management**
- Connecting **product lifecycle** with corporate **risk frameworks**

Common challenges we see at clients

Unclarity about standards

- Lack of harmonized standards yet
- Relationships with RED, NIS2, etc.

Decentralized processes

- Independently operating product teams
- Fragmented ownership across departments

Limited visibility on software components

- SBOM gaps and dependency management
- Supplier risk and OSS governance

Resource and capability constraints

- Limited CRA expertise
- Competing priorities in product roadmaps

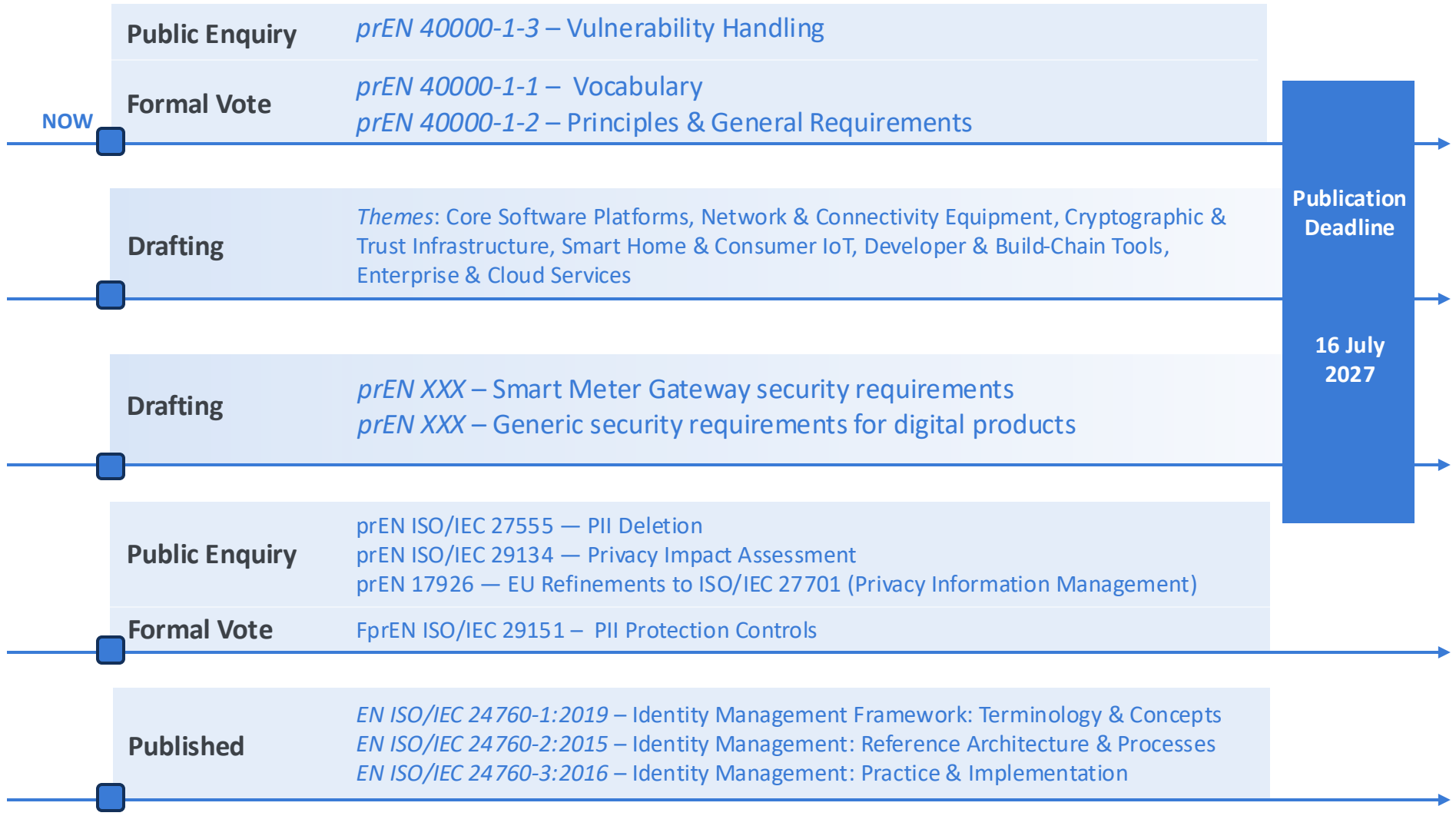
Organizational readiness

- Proactive security design over reactive fixes
- X-functional accountability and collaboration

Draft standards inform the ‘definition of done’

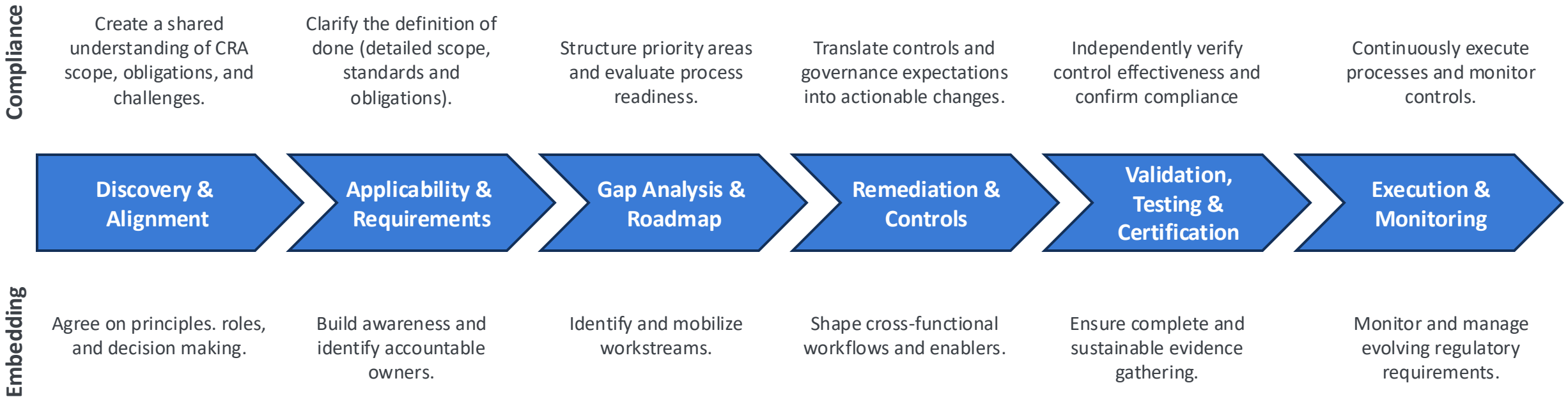
Existing draft standards and the text of CRA itself provide strong guidance on CRA testing requirements

Work program: M/606



Nemko’s CRA readiness approach

A phased approach to interpret, remediate, validate, and continuously manage regulatory obligations.



Case example

CRA compliance for an IoT company

- Client was fully focused on product development and innovation, but **started to realize** that evolving regulation would pose a **compliance threat** if left unattended
- Nemko Digital constructed an **applicability matrix**, clarifying **regulatory obligations**, identified the **gap** with current controls, developed a roadmap towards compliance
- **Concrete recommendations** and **hands-on support** increased resource efficiency and team confidence
  - Internal projects were **re-prioritized** in accordance with compliance needs
  - Nemko Digital support in selected areas **accelerates implementation** of controls
  - Hands-on Nemko Digital support with ‘soft controls’ **frees up key technical resources** for accelerating the product roadmap
  - Ongoing **regulatory monitoring** ensures continued compliance

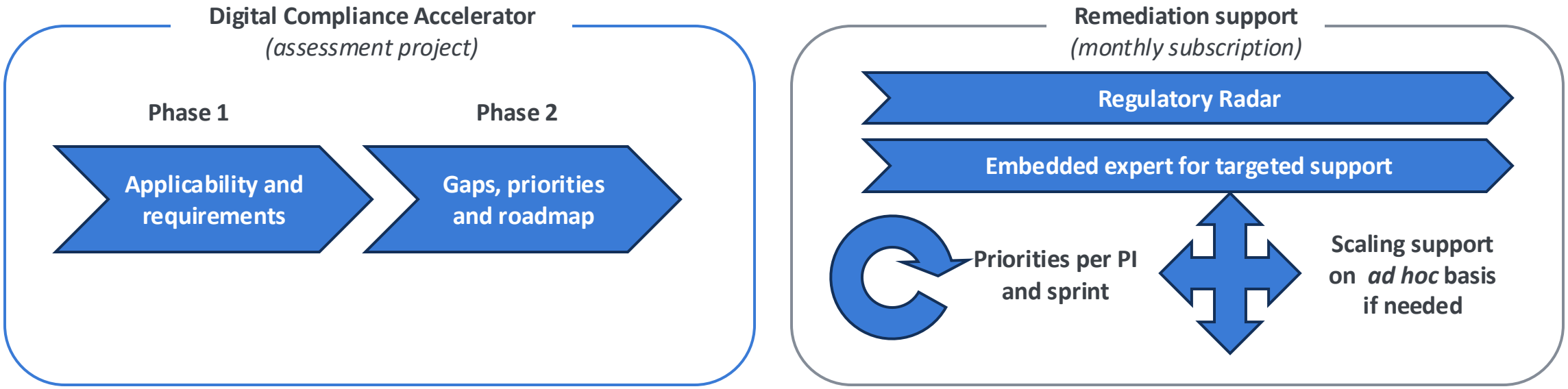
Applicability matrix

Regulation specific deep-dive

Obligations and controls

A pragmatic support model where you stay in the driver seat

We start with a focused assessment to confirm which **regulations and standards** apply to you and to map out any gaps with a clear **remediation plan**. From there, we can step in with ad-hoc projects whenever you need targeted support.



Key Benefits

- Reduced risk
- Continuous improvement
- Strategic differentiation
- Resource efficiency
- Team confidence

Client case: How we support with CRA

Client case

Client example illustrating how we provide end-to-end support for compliance with the Cyber Resilience Act (CRA) within the broader cybersecurity domain, covering governance, risk assessment, and implementation.

	GPSR & CRA	Must/ Should
Nemko Digital executes Nemko drafts documents, executes analyses, and aligns with stakeholders	Cyber risk assessment	Must
	Support & usage policies	Must
	SDLC & SBOM management policies	Must
	Response and disclosure policies	Must
	Technical documentation & SBOM	Must
	Harmonized standards gap	Must
	Technical testing*	Must
	Documentation	Must
Nemko Digital consults Nemko gives guidance, validates requirements, participates in discussions, and reviews drafts	Implement policies and processes	Must
	Implement harmonized standards	Must
Nemko drives	• Activate stakeholders, coordinate activities, monitor progress	

* Restricted to planned systems for which intended use and specifications are available
** Technical testing for CRA will be delivered through Nemko Scandinavia

Let’s hear from you!

What’s your CRA mood right now?

- “Teach me everything.”
- “We need structure and support.”
- “We think we’ve got it. This is just a sanity check?”
- “Almost there. This is my final validation.”
- “We’re ahead, but still looking for more insights.”

Getting ready for testing

How to prepare for CRA

Overall goal:
Ensure that digital connected hardware and software products placed on the EU market are more secure

New terms: Secure-by-design and secure-by-default

Risks analysis based on the intended purpose and reasonably foreseeable use

Manufacturers remain responsible for product's cybersecurity 5+ years after sales

Reporting of exploited security vulnerabilities of products

Various product risk classifications and classes

Harmonized standards are not required to get going!

Default category (the majority of products) does not require the use of harmonized standard

The requirements are listed in the CRA

Annex I

Part I: Essential cybersecurity requirements (14 Product requirements)

Part II: Vulnerability handling requirements (8 System requirements)

Annex II

Information and instructions to the user (14 requirements)

Presumption of conformity needs to be established through an extended risk analysis (compared to when using a harmonized standard)

Essential Requirements – Products – Annex I

- Risk assessment – Secure design, development, production
- No known exploitable vulnerabilities
- Secure by default configuration
- Automatic security updates
- Protection from unauthorized access
- Protection of integrity and confidentiality of data
- Data minimization
- Protection and mitigation of denial-of-service attacks
- Minimise the negative impact of the product themselves or connected devices
- Limited attack surface
- Appropriate exploitation mitigation mechanisms and techniques
- Logging mechanism
- Deletion of user data

Essential Requirements – Vulnerability handling – Annex I

- Identify and document vulnerabilities and components including maintaining an SBOM
- Provide security updates without delay
- Apply effective and regular tests and reviews of the security
- Publicly disclose information about fixed vulnerabilities
- Coordinated vulnerability disclosure
- Provide contact information for reporting of vulnerabilities
- Provide mechanisms to securely distribute security updates in an automatic manner
- Keep products updates for the support period (5 years) free of charge.

Information provided with the product – Annex II

- Contact information of the manufacturer
- Single point of contact for vulnerability disclosure and information on CVD
- Unique identification of the product
- The intended purpose and security environment, as well as essential functionality and security properties
- Known or foreseeable circumstances that can lead to significant cybersecurity risks
- The type of technical security support offered and the end-date of the support period
- Detailed instructions or link to instructions and information on initial setup to ensure secure use, changes that can affect the security, how to perform security updates, deletion of user data, how to disable automatic updates, how to integrate the product with other products.
- How to access the SBOM, if publicly available

Typical Cyber Security Evaluation Process

Step 1

Documentation

- Secure Development
- Vulnerability handling
- Information to customer
- Product Context
- Product security

Don’t underestimate the documentation requirements!

Step 2

Functional testing/verification

- Test product according to product standard.
- Amount of testing will differ between standards.

Step 3

Report

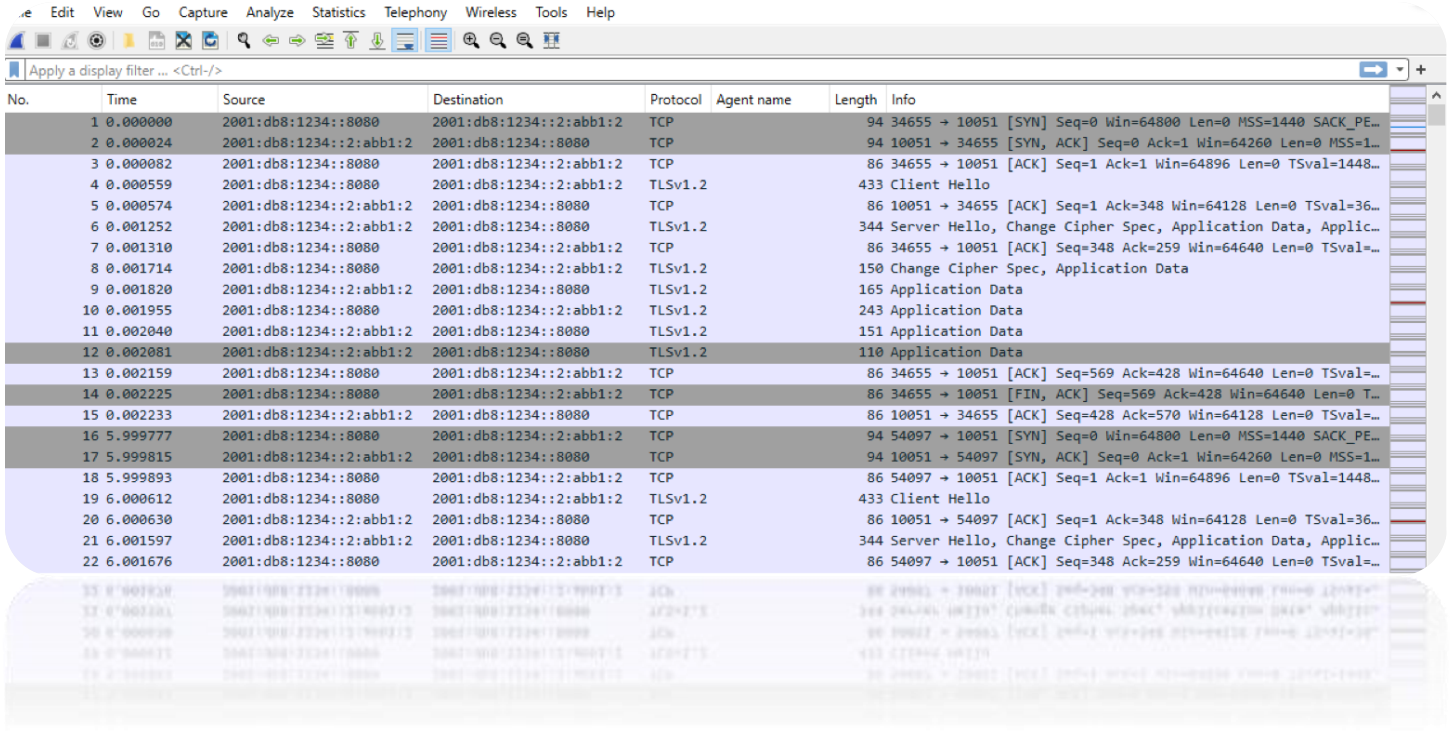
- Output of step 1 and 2 is a report to be included in your Technical file

Typical testing case

Test Case for Secure communication mechanism

Test – Sniffing network traffic:

- Verification of protocol
- Protocol version
- Undocumented traffic
- Cipher suites



No.	Time	Source	Destination	Protocol	Agent name	Length	Info
1	0.000000	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		94	34655 → 10051 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PE…
2	0.000024	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TCP		94	10051 → 34655 [SYN, ACK] Seq=0 Ack=1 Win=64260 Len=0 MSS=1…
3	0.000082	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		86	34655 → 10051 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=1448…
4	0.000559	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TLSv1.2		433	Client Hello
5	0.000574	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TCP		86	10051 → 34655 [ACK] Seq=1 Ack=348 Win=64128 Len=0 TSval=36…
6	0.001252	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TLSv1.2		344	Server Hello, Change Cipher Spec, Application Data, Applic…
7	0.001310	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		86	34655 → 10051 [ACK] Seq=348 Ack=259 Win=64640 Len=0 TSval=…
8	0.001714	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TLSv1.2		150	Change Cipher Spec, Application Data
9	0.001820	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TLSv1.2		165	Application Data
10	0.001955	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TLSv1.2		243	Application Data
11	0.002040	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TLSv1.2		151	Application Data
12	0.002081	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TLSv1.2		110	Application Data
13	0.002159	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		86	34655 → 10051 [ACK] Seq=569 Ack=428 Win=64640 Len=0 TSval=…
14	0.002225	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		86	34655 → 10051 [FIN, ACK] Seq=569 Ack=428 Win=64640 Len=0 T…
15	0.002233	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TCP		86	10051 → 34655 [ACK] Seq=428 Ack=570 Win=64128 Len=0 TSval=…
16	5.999777	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		94	54097 → 10051 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PE…
17	5.999815	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TCP		94	10051 → 54097 [SYN, ACK] Seq=0 Ack=1 Win=64260 Len=0 MSS=1…
18	5.999893	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		86	54097 → 10051 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=1448…
19	6.000612	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TLSv1.2		433	Client Hello
20	6.000630	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TCP		86	10051 → 54097 [ACK] Seq=1 Ack=348 Win=64128 Len=0 TSval=36…
21	6.001597	2001:db8:1234::2:abb1:2	2001:db8:1234::8080	TLSv1.2		344	Server Hello, Change Cipher Spec, Application Data, Applic…
22	6.001676	2001:db8:1234::8080	2001:db8:1234::2:abb1:2	TCP		86	54097 → 10051 [ACK] Seq=348 Ack=259 Win=64640 Len=0 TSval=…

Test Case 2

Test Case for verifying services and ports

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.11.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 11:02 CEST
Nmap scan report for 192.168.11.94
Host is up (0.00010s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Test - scanning product for ports / services:

- Verify only documented ports
- Verify no unused ports are present

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.11.94 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 14:07 CEST
Nmap scan report for 192.168.11.94
Host is up (0.000075s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
```

Note: the command used in the picture is for refence only.

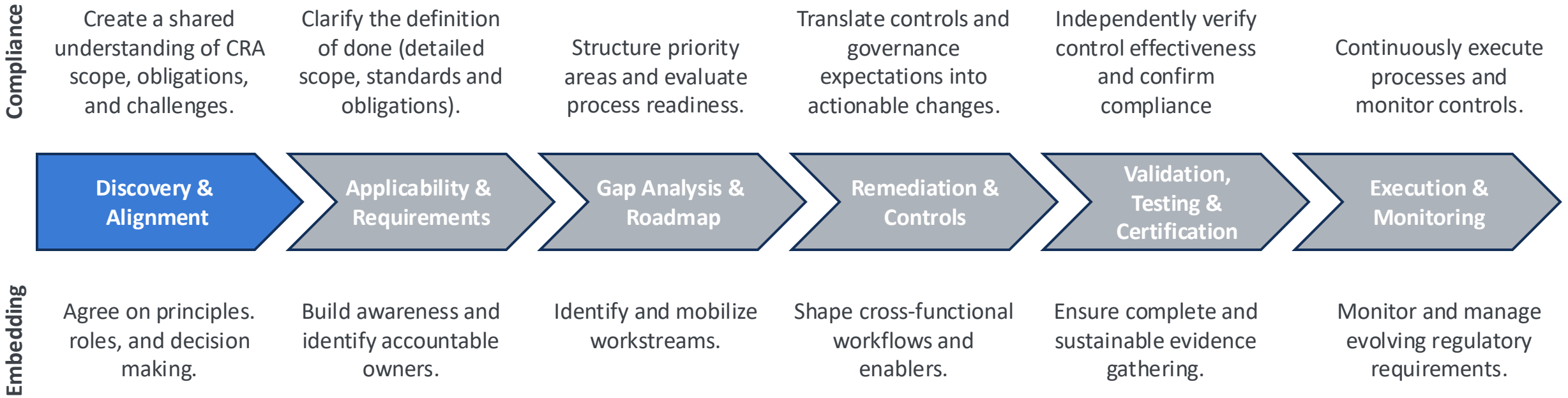
Getting started

Nemko’s CRA readiness approach

Scope of proposal

Future/optional scope

Nemko offers a phased approach to interpret, remediate, validate, and continuously manage regulatory obligations.



Discovery & Alignment Workshop

We propose a 2-day workshop with key stakeholders

Purpose and outcomes

Establish the foundation for a CRA implementation roadmap

- Shared understanding of requirements and their impact
- Clarity on gaps in processes, governance, and development
- Strategic approach for achieving CRA compliance

Participants

- Product Management
- Engineering / R&D Leadership
- Security Leadership
- Compliance / Risk / Legal
- Quality
- Architecture & IT
- …

Agenda outline

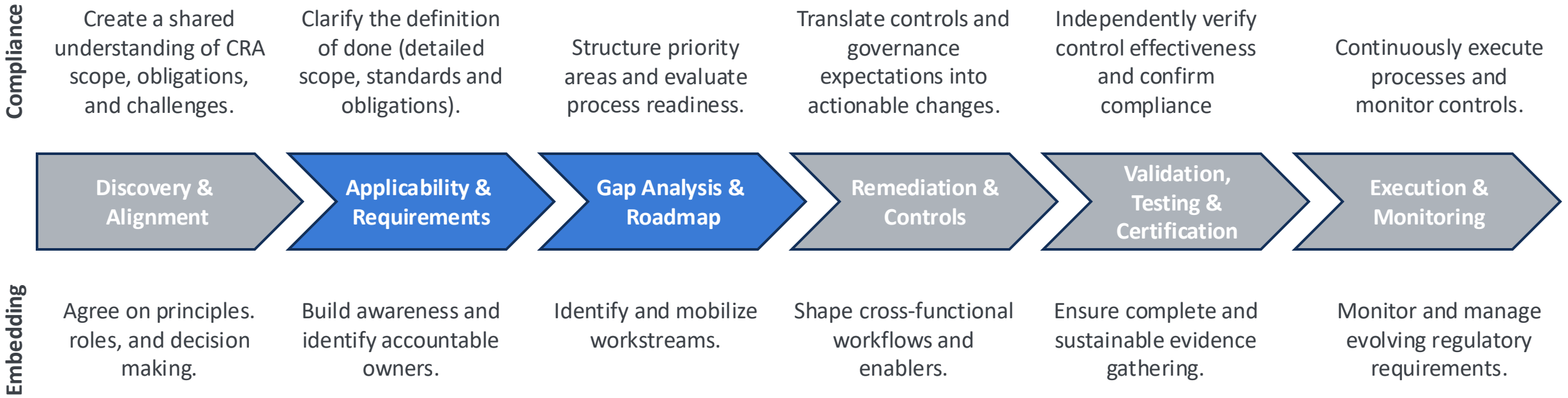
1. **Introduction and objectives**
   Purpose and outcomes
2. **CRA deep-dive**
   Scope, key obligations, and required processes
3. **Current state**
   Discussion on policies, practices, and pain points
4. **Gap identification**
   Plotting practices and capabilities versus requirements
5. **Compliance approach**
   Guiding principles, key considerations, and program structure
6. **Roadmap outline**
   Milestones, key activities, concrete next steps

Nemko’s CRA readiness approach

Scope of proposal

Future/optional scope

Nemko offers a phased approach to interpret, remediate, validate, and continuously manage regulatory obligations.



Digital Compliance Accelerator approach

The Digital Compliance Accelerator provides a **structured approach** to evaluate and ensure compliance with relevant digital regulations

Phase 1 — **6-8 weeks** — **Applicability and requirements**

Actions:

- Review relevant EU regulations (**CRA, and possible other**)
- Map products and components to the regulatory scope
- Identify and interpret relevant requirements and (draft) standards as they apply
- Conduct stakeholder interviews (legal, technical, operational)
- Document applicability and obligations for each regulation

Deliverables:

- **Applicability matrix** showing which regulations apply and why
- **Requirements summary** in plain, actionable language
- **Open points** that need further or clarification and/or additional research

Phase 2 — **Gap Analysis & Roadmap**

Actions:

- Compare the currently implemented policies, processes, and technical controls to requirements summary
- Identify gaps, risks, and compliance priorities
- Propose remediation actions with cost/effort estimates
- Assign ownership (internal teams or external support)

Deliverables:

- **High level Gap analysis report** with severity and priority levels
- **Initial remediation roadmap** with timelines, milestones, and responsible parties
- **Resourcing requirements**, outlining the division of roles

Assessment Boundaries

- **Confirm stakeholder involvement** — agree on engagement-level responsibilities, and availability for workshops or interviews.
- **Set level of detail** — determine a realistic, risk-based balance between a full regulatory deep dive or a high-level applicability screening.

Call to action

CRA – EU Updates

Deepdive Webinar | 8 April | Free to Join

Join us for a deep dive into the latest EU updates on standards related to CRA.

What we'll cover:

- Overview of the newest EU developments impacting CRA
- Key standard updates you need to know
- What these changes mean for your organization
- Practical steps to stay compliant and prepared

Reserve your spot today – limited availability.

We will share you all the link via email for registration

Nemko Digital

Call with our CRA experts now!

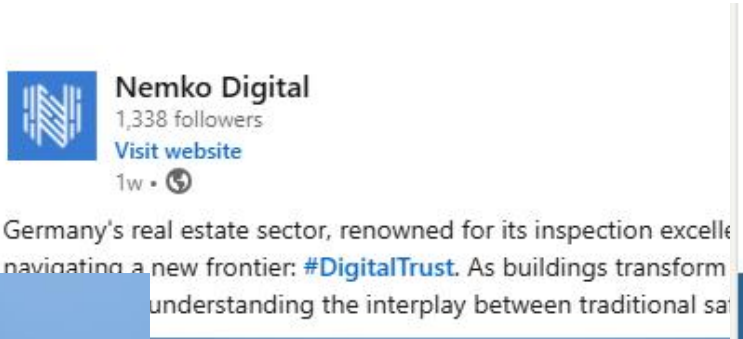
Don’t wait till April for the next step

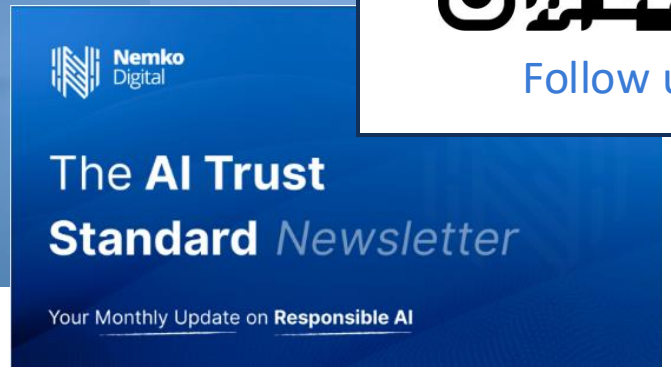
- Open to Webinar Participants
- Complete Application Form
- Share topic you want to talk about

https://digital.nemko.com/cra-expert-call

Scan to apply

Stay updated!





Follow us

Nemko
Digital