OPEN INDUSTRY 4.0 ALLIANCE

CYBER RESILIENCE ACT

COUNTDOWN ON COMPLIANCE. ARE YOU READY?



SHORT CUT

WHAT

The Cyber Resilience Act is EU law, not a proposal, in force since December 2024. It sets a minimum cybersecurity level for any product with digital elements sold in Europe, reaching manufacturers, suppliers and distributors alike. Reporting duties start September 2026, full enforcement including the CE mark requirement lands December 2027, and a product that misses it can no longer be sold in Europe at all.

WHY

Because connected products have shipped under different security standards depending on the country, insecure by default, with the cost landing on the customer rather than the manufacturer who built it.

WHO

For manufacturers, suppliers and anyone responsible for getting a connected product onto the European market, especially where cybersecurity has so far lived in IT and never really made it into OT.

SAMUEL GREISING, MANAGING DIRECTOR & COO @FLECS

THE CYBER RESILIENCE ACT IS A REAL CHANCE FOR EUROPEAN INDUSTRY. IT TURNS SECURITY INTO A QUALITY MARK CUSTOMERS CAN SEE AND TRUST. MANUFACTURERS WHO BUILD SECURITY, TRANSPARENCY AND GOOD UPDATE PRACTICES INTO THEIR PRODUCTS FROM THE START WON'T JUST MEET THE REQUIREMENTS. THEY'LL SHIP BETTER PRODUCTS, AND THEY'LL SHIP THEM FASTER.

NOT SURE WHICH CRA DEADLINE ACTUALLY APPLIES TO YOU?

DOES CYBERSECURITY STILL FEEL LIKE SOMETHING YOU'LL DEAL WITH LATER?

DO YOU KNOW EXACTLY WHAT YOUR PRODUCTS NEED BY 2027?

IF YOU ANSWER ONE OF THE Q'S WITH „YES" - YOU SHOULD CONTINUE READING.

CONTENT

01 WHAT IS THE CYBER RESILIENCE ACT & HOW DOES IT IMPACT YOU?

02 WHY THE COUNTDOWN STARTS

03 THE RISK BASED PATH TO COMPLIANCE

04 WHY PKI IS THE KEY

05 SO.. WHAT NOW?

Authors

Björn Jansen | Product Manager | secunet

Lucas Wolf | Technical Content Manager | Open Industry 4.0 Alliance

Editor

Lucas Wolf | Technical Content Manager | Open Industry 4.0 Alliance

Publisher

Open Industry 4.0 Alliance
Christoph Merian-Ring 12, 4153 Reinach, Switzerland
https://openindustry4.com
info@openindustry4.com

OPEN INDUSTRY 4.0 ALLIANCE

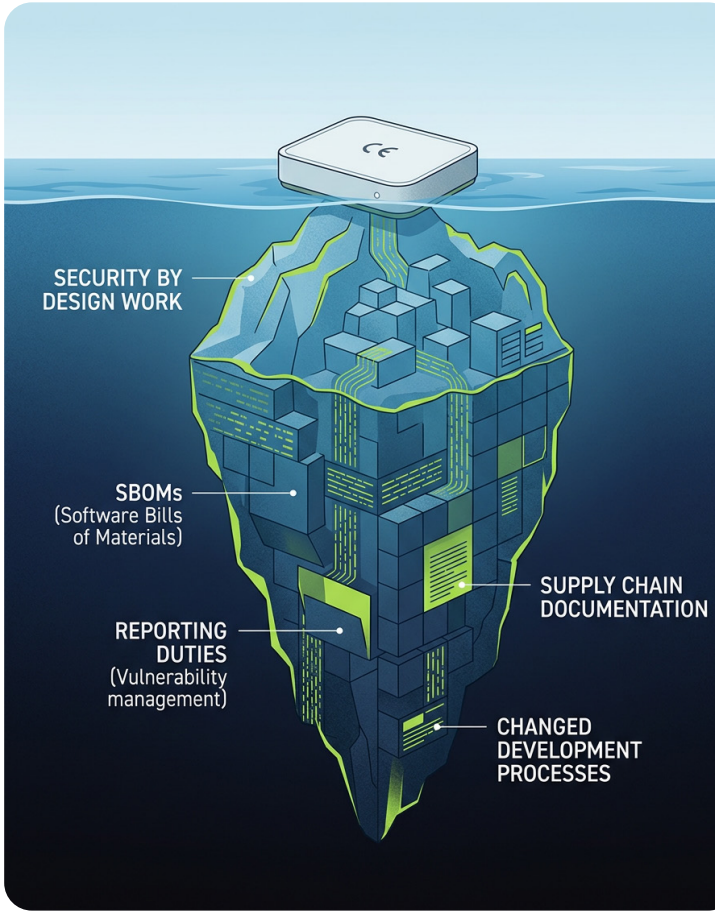
01 | WHAT IS THE CYBER RESILIENCE ACT & HOW DOES IT IMPACT YOU?

SECURITY IS NO LONGER OPTIONAL FOR CONNECTED PRODUCTS

Let‘s clear up the first question people usually have before anything else: this is not a proposal, a draft, or an industry idea floating around waiting for approval. The Cyber Resilience Act, formally regulation (EU) 2024/2847, is EU law and entered into force on December 10, 2024. It is already on the books. What‘s still ahead is the rollout of when each part of it actually starts biting. That rollout happens in stages, and each stage matters on its own.

Reporting obligations come first, and they land sooner than most people expect. From September 11, 2026, manufacturers have to report actively exploited vulnerabilities and severe incidents to ENISA. The clock on that one is brutal: 24 hours for an early warning the moment you become aware of it, 72 hours for a more detailed notification, and a final report within roughly a month once a fix is available. Not a paperwork deadline you can quietly push back. It requires a live process that can actually detect something, escalate it internally, and get it reported in time, which for most companies today doesn‘t exist yet.

Then comes the big one. From December 11, 2027, the full regulation applies. That includes the CE marking and conformity assessment requirements this whole paper keeps coming back to. From that date, a new product with digital elements simply cannot be legally placed on the EU market unless it carries that mark, and that mark now includes CRA compliance baked into it.

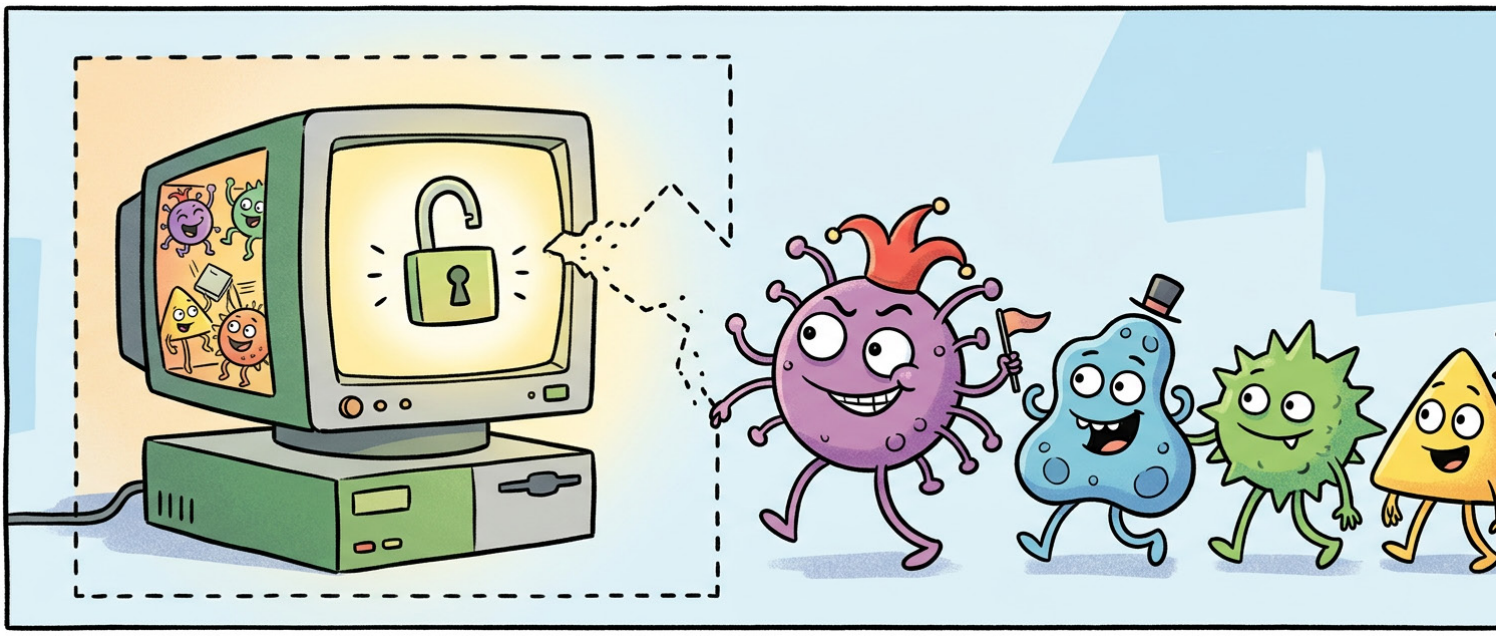


And this isn‘t a soft law with symbolic penalties. Get it wrong and the fines go up to 15 million euros or 2.5 percent of ones global annual turnover, whichever number turns out higher. For a large manufacturer, that second option is usually the far more painful one. On top of the fine, a non-compliant product loses its right to be sold in Europe at all, which for most companies is the part that actually hurts, long before any invoice for a fine ever shows up.

So why does this law exist in the first place? It‘s worth answering honestly, because the reasoning explains almost every requirement that follows. For years, connected products entered the European market with wildly inconsistent security standards. One country had its own rules, another had none at all, and a product built to a lower bar in one place could still ship freely across the entire union once it was inside.

Attackers never cared about those borders anyway. An insecure device is an insecure device no matter which country sold it. On top of that, a lot of products simply shipped insecure mechanisms by default. Speed to market and price competition regularly won out over security, and the cost of that decision rarely landed on the manufacturer who made it. It landed on the customer running the product, and by extension, on the wider network that product was plugged into. With well over ten billion connected devices already in use and IoT growth showing no sign of slowing down, that pattern stopped being a tolerable risk and started being a systemic one. The CRA exists to put the responsibility for security back where it belongs, on the people designing and building the product, not on the people who bought it afterwards trusting that someone else had already handled it.

That reasoning is also exactly why the CRA reaches past the manufacturer's own four walls. Your product is only ever as compliant as the components sitting inside it. If your supplier can't tell you what's in their component, you can't fully answer that question for your own customer either. That single dependency is why this regulation ends up touching far more companies than the ones actually shipping a finished, branded product, and why the idea driving most of it, security by design, means going into your actual development process and building security in from the start rather than bolting it on right before shipping.



02 | WHY THE COUNTDOWN STARTS

2027 SOUNDS FAR AWAY, YOUR SUPPLY CHAIN DISAGREES

2027 sounds distant, right up until you sit down and actually list out everything that needs to happen before that date arrives. It applies first to new products entering the market. What happens with products already out there today is a fair and very common question, and honestly, it's not fully settled yet.

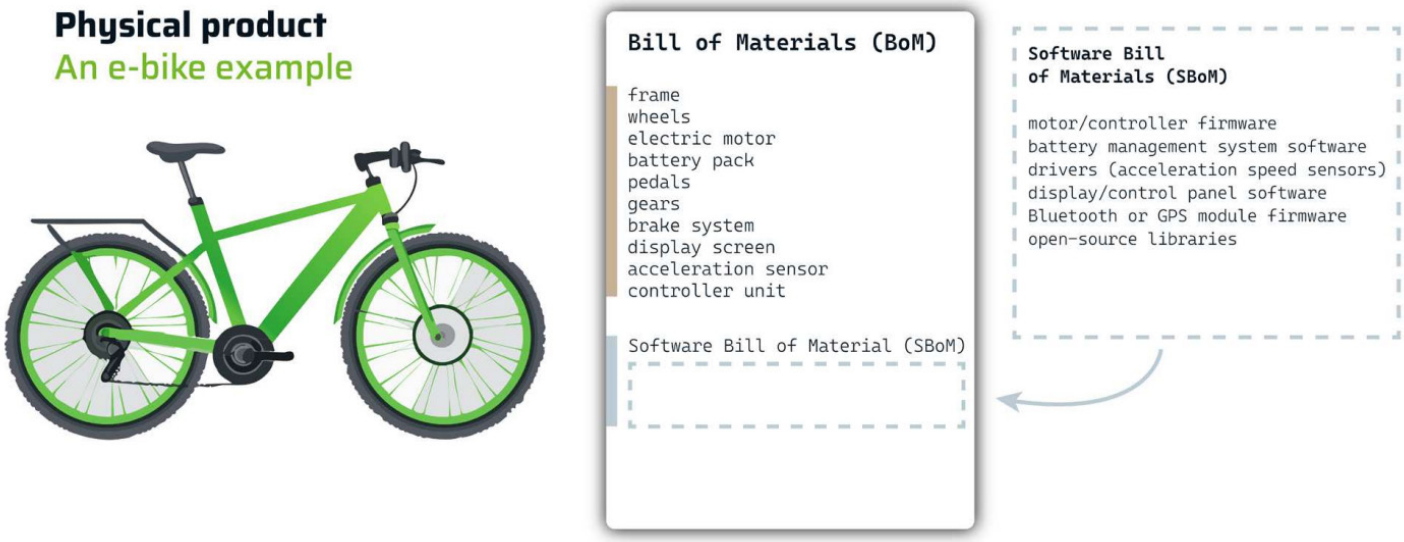


Part of the reason is that the harmonized standards that would spell out the fine details in full simply don't exist yet. We know what's coming. We don't yet know every last detail of how it will be measured, because the regulation itself, by design, tells you that something needs to be done without prescribing the exact how down to the letter.

That uncertainty pushes a lot of companies to look for something more concrete to orient around, and that's where the supply chain comes in, arguably as the biggest practical challenge of the whole topic. With SBOM requirements in particular, you suddenly need to think through your entire supply chain and actively pull information out of it, not just assume it will show up when asked.

and anyone who wants to keep supplying them, or start supplying them, will end up dealing with this faster than they might like, whether they feel ready or not.

At the end of the day, this comes down to the CE mark. It's being extended to include the requirements of the Cyber Resilience Act. Without that extended mark, a product simply cannot be placed on the market in Europe anymore. That's the hard stop everything else in this chapter is building toward. The good news buried in all of it: the CRA explicitly calls for a risk based approach. Not every company starts from the same place. Not every product carries the same requirements, and not every product faces the same attack vectors. Something that represents a real problem for one machine builder might barely register as a risk for



Here's the part most companies underestimate, and it's worth saying plainly: the pressure rarely comes from the regulation itself first. It comes from the supply chain. Large manufacturers, the OEMs, write these requirements directly into their supplier contracts. Whether the regulation is good or bad, whether you personally agree with how it was written, is a separate discussion entirely. What's much more certain is that the big European manufacturers will put these requirements into their supplier terms,

another, simply because a component sits differently inside the machine, or because a particular attack path just isn't reachable in that specific setup. Recognizing that difference early saves a huge amount of wasted effort chasing generic requirements that don't actually apply to your specific product.

03 | THE RISK BASED PATH TO COMPLIANCE

WHY ISO 27001 AND IEC 62443 NEED EACH OTHER TO FIT

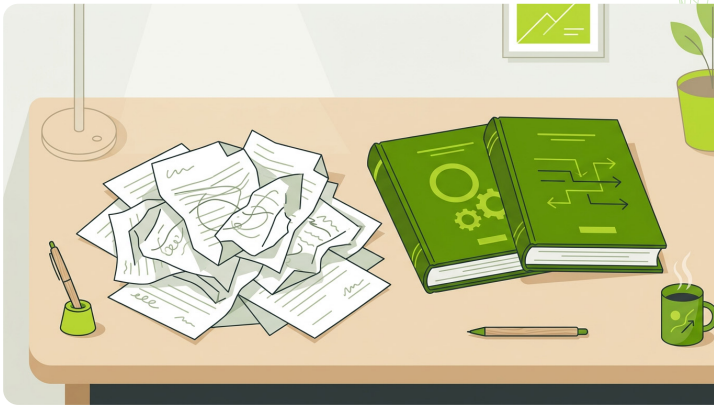
Two regulations sit on most desks at the same time right now, and they're easy to confuse if you look at them from far enough away. NIS2 protects the organization. The Cyber Resilience Act protects the product. Both come out of Europe, one landing as a regulation, the other as a directive, which is a technical difference worth knowing but not worth losing sleep over. What matters more in daily practice is how much overlap they actually share once you get past the labels: risk management, technical measures, protection of the supply chain, incident handling, and reporting duties show up in both, almost line for line.



That overlap is genuinely good news, because it means you don't need two completely separate compliance programs running in parallel. The practical starting point looks the same either way: a lay of the land, an audit, a gap analysis, and an honest answer to the question of where you actually stand today, before deciding what makes sense for your specific company, your specific product, and your specific status quo. **Skipping this step and jumping straight to buying a solution is one of the most common and most expensive mistakes companies can make.**

On the standards side, most companies already have something to build on, and it's worth knowing what you actually have before assuming it covers you. ISO 27001 gives you an information security management system, the classic ISMS approach most people have at least heard of. IEC 62443 is the OT specific standard, and depending on which part of it you're working with, you'll also run into things like TISAX alongside it.

Here's the trap worth calling out directly. If you've already implemented ISO 27001, or you already hold a TISAX certification, that's a solid foundation, sometimes a genuinely strong one. But the question that always needs asking right after is: what was the actual scope? If your ISO 27001 certification only ever covered your IT environment, it barely moves the needle for NIS2, because NIS2 explicitly requires you to bring your OT environment into scope as well. You have a great foundation, you understand how the process works, you've built the right muscles, but you cannot let that lull you into a false sense of security. The scope has to widen, not just the paperwork.



There is no harmonized EU standard for the Cyber Resilience Act yet, and that's an honest gap to acknowledge rather than paper over. That work is expected to land sometime next year, more likely toward the end of it than the beginning. Everyone currently in this space, everyone we talk to, orients around IEC 62443 in the meantime. It probably won't survive completely untouched once the harmonized standard finally arrives, there will likely be extensions and adjustments, but building on that

foundation now puts a company in a genuinely strong position regardless of exactly how those final details shake out.

The combination that actually works in practice looks like this: take the requirements out of IEC 62443, feed them into an ISO 27001 framework, and fill in whatever gaps the ISO standard leaves uncovered on its own. Together, they form one coherent approach that can be tailored to the size of the company, the nature of the product, and its current level of cybersecurity maturity. Not a generic template stretched over every company the same way, but something actually cut to measure.

IF THIS CHAPTER FEELS HEAVY, THAT'S FAIR. TWO STANDARDS, ONE REGULATION, ONE DIRECTIVE, A SCOPE QUESTION THAT TRIPS UP COMPANIES THAT ALREADY THOUGHT THEY WERE COVERED. GETTING YOUR FIRST OVERVIEW AND FINDING YOUR BEARINGS IN THIS TOPIC IS GENUINELY ONE OF THE HARDEST PARTS, AND YOU DON'T HAVE TO DO IT ALONE. OVER 100 MEMBERS INSIDE THE OPEN INDUSTRY 4.0 ALLIANCE ARE ALREADY WORKING ON EXACTLY THIS, COMPARING NOTES, SHARING WHAT'S WORKED AND WHAT HASN'T, AND BUILDING A SHARED UNDERSTANDING INSTEAD OF EVERYONE STARTING FROM ZERO. IF YOU'RE LOOKING FOR ADVICE OR A PLACE TO GET ORIENTED, OI4 IS A SOLID PLACE TO START.

START HERE

CRA <> NIS2



STANDARDS

ISO 27001

covers how you manage security as an organizationoften IT scoped only

IEC 62443

covers how you secure the actual OT systems themselves.

TISAX

can be a good foundation

tailored fit
shaped to company, product, status quo

No harmonized EU standard for CRA yet.
Until an official standard is published, IEC 62443 is the main technical reference.

04 | WHY PKI IS THE KEY

THE TRUST ANCHOR YOU'RE ALREADY USING WITHOUT KNOWING IT

Strip away the regulatory language and what CRA and NIS2 actually ask for comes down to a short list of protection goals: strong authentication, integrity protection, data encryption, and non-repudiation, so nobody can later deny they sent or received something. Someone at a trade show in Hannover put it well: the industry needs PKI (Public Key Infrastructure), it just hasn't realized it yet.

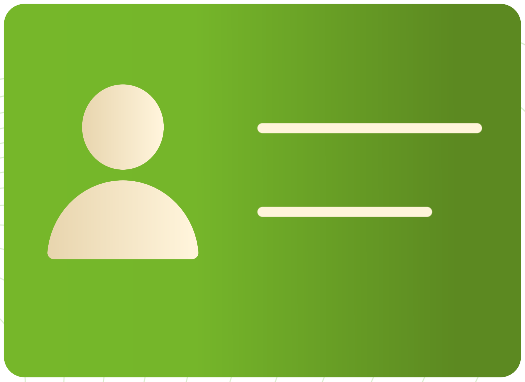


Most companies already run on PKI without thinking of it that way. Code signing, VPNs, predictive maintenance connections, secure boot, all of it quietly depends on a public key infrastructure in the background. More specifically, it shows up in secure key injection during manufacturing, secure access, secure communication inside a plant, and secure remote maintenance.

The analogy that makes it click is the ID card in your wallet. In the physical world, it's your trust anchor, held up whenever someone needs to verify who you are. In the digital world there's no time for a manual check at machine speed, so PKI carries that same trust anchor concept into the digital world, fully automated. Take access control. A digital certificate makes a device's identity provable and checkable instantly, and data only gets released after that automatic check. A second factor comes along almost for free, since the whole exchange between devices is already digital.

Encryption works the same way underneath: protecting firmware and IP, moving data securely regardless of environment, all running on asymmetric encryption with private and public key pairs. One thing worth naming directly is harvest now, decrypt later attacks, where someone captures encrypted data today and just waits for quantum computing to crack it open later. If that data still matters in five or ten years, post quantum ready PKI stops being optional.

One last example makes it concrete: component identity. Modern vehicles constantly authenticate control units against each other, which is exactly how the automotive industry has prevented unauthorized part swapping for decades. The engine only starts once every connected component confirms it's original and certified. Apply that same logic to a supply chain and you get the same protection: only original, verified components get to participate.





Take a **power plant** as a first real world example. One physical site, feeding data continuously up into a cloud environment, connected out to potentially thousands of individual households acting as customers on the other end. Nobody is manually checking an ID card for every single one of those thousands of connections, and nobody realistically could. A PKI, tailored to that product and that organization, handles it automatically instead. Communication only ever happens between partners that have been verified and are actually trusted, and individual components stay protected the whole way through, without any1 needing to peek inside the actual data itself to make that happen.



Down on the **production floor**, certificates get injected directly into devices during the manufacturing process itself, without slowing the production line down even a little. In some setups this gets pushed even further: a single certificate might only live for a few seconds, existing purely to secure one specific production step and nothing beyond it. It adds measurable value both to the manufacturer running the line and to the end customer eventually holding the finished product. And once it‘s genuinely set up correctly, that‘s really the punch line, nobody in the building even notices it‘s running anymore. It just happens.



Or look at a **full automotive ecosystem** instead of a single car. A manufacturer produces its own energy, runs a handful of additional services on the side, and its actual product, the car itself, needs to talk to public charging stations out in the world and, ideally, to a wallbox sitting quietly in someone‘s garage at home too. Add a billing provider handling the transaction in the background, and in most, though admittedly not quite all, of these individual pieces, a PKI is already sitting there doing the work. Code signing, secure boot, VPN connections running back to the manufacturer with proper backend credentials, all of it riding on the exact same underlying infrastructure.



Agricultural machinery tells a strikingly similar story, from a different corner of industry. Modern machines out in the field drive themselves for long stretches, carrying more onboard technology than most rockets that made it to the moon. A plan gets drawn up in the office, then executed in the field down to the exact square meter, precisely how much fertilizer or pesticide goes where. Every step along that chain, from key injection during manufacturing all the way through to an over the air software update landing on the machine years later, runs through the same PKI foundation, hitting the same protection goals laid out earlier in this paper, just applied to a different kind of machine.

05 | SO.. WHAT NOW?

WHAT ACTUALLY CHANGES WHEN YOU GET THIS RIGHT

Strip away the regulation for a moment and ask what the actual goal underneath all of it really is. It comes down to two things: strengthening your own organization, and strengthening the products you put out into the world. Different sides of the same coin, and both come back to the same word: trust.

Look at it from the other side of the table for a second, whether that's another company further down your supply chain or the person actually operating the machine once it ships. What they want is straightforward. A product that's genuinely secure the day it arrives. Confidence that updates will keep coming for the next four or five years. The ability to run the thing without a nagging feeling that nobody really knows what's inside it anymore.

That's really the point this whole paper has been building toward, and it holds up regardless of whether CRA or NIS2 happens to apply to your specific product. Getting your products to that level should honestly be something companies want to do for their own customers anyway, law or no law. The regulation puts a hard deadline on it. It didn't invent the reason to care in the first place.



None of it fits neatly inside one company's own walls, though. CRA compliance runs through your supply chain. NIS2 runs through your whole organization. PKI only earns its keep once every partner, every component and every connection actually plays along. Getting there alone, from a cold start, is a slow and expensive way to learn lessons other companies have already learned.



HELLO, WE ARE OPEN

That's exactly the gap the Open Industry 4.0 Alliance works on. More than 100 member companies collaborate in OI4, and Industrial Cyber Security is one of its Focus Areas. The goal is to build security into every layer from the start instead of adding it at the end. OI4 has already published a whitepaper on post-quantum cryptography, and the experts behind the Industrial Cyber Security Focus Area are available to discuss exactly the questions this paper raises.

If you're starting your CRA and PKI journey from scratch, you don't have to figure it out alone. OI4 is a good place to start.

START WITH OI4

OPEN INDUSTRY 4.0 ALLIANCE

VERSION HISTORY

VERSION	DATE	DESCRIPTION	EDITOR
1.0	August 7th 2026	Initial release	Lucas Wolf