Build a smarter world

Quectel Wireless Solutions

Masterclass: How to achieve IoT cybersecurity certification across the EU, US, and global markets

Oct 2025

Yoon Seungryoul (Certification Director - Quectel)
Larry Pesce (Vice President of Services - Finite State)

Quectel Certification Service

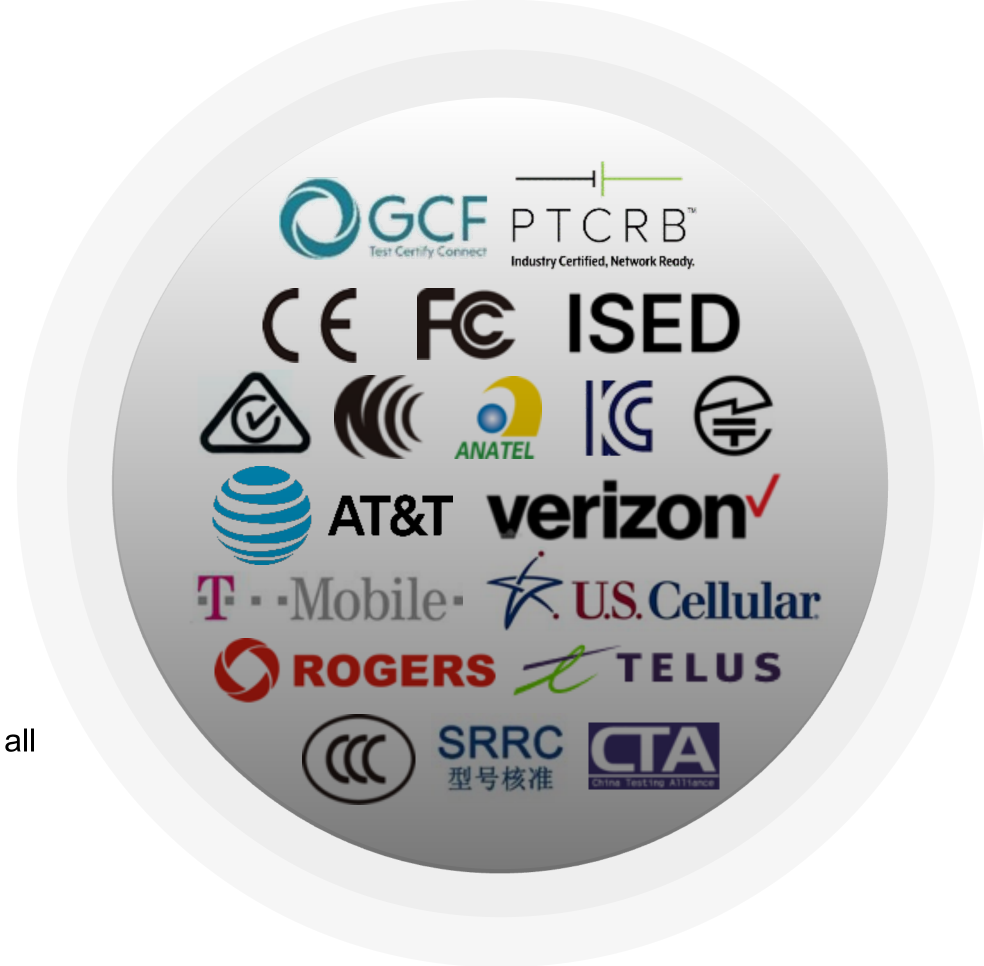
Quectel certification service

Experienced

- Larger certification team
- Global view on certification demands
- Diversified products

Professional

- Pre-scan service in owned lab
- Technical support & debugging solution
- Global on-site support



Great Cooperation

- Dedicated PM for cert project management
- Long term cooperation with all kinds of 3rd party labs
- Global team and great relationship with carriers

Efficiency

- Save labor resource
- Shorten leading time
- Reduce cost

Quectel certification service - benefits

- Project management
- All paperwork tasks
- Dealing with the labs and carriers
- Checking test scope, making minimum test scope
- Necessary onsite support
- Testing and debugging
- Quectel in-house testing for NA carrier certifications
- Fixing issues and negotiation for the waivers
- Getting certificate and provide to customer

Quectel certification service - updates in 2025

- Covers more various certifications including Industrial certifications
- Covers more country certifications (90+) including local agent support
- Testing and certifications in various locations including North America, Europe and Asia
- More capability to fix HW/SW issue related with Non-Quectel products
- More capability for in-house testing for the carrier certification requirements
- Can offer lower cost by bundling a few or more certification items
- **For Cybersecurity requirements and Cybersecurity certification service we work with Finite State team for testing/reporting in US and consulting service.**
  CE RED Article 3.3 (d)(e)(f)
  EU Cyber Resilience Act (CRA)
  Connected Vehicle Regulation
  US Cyber Trust Mark

FINITE STATE

How to achieve IoT cybersecurity certification across the EU, US, and global markets

Finite State is a leading provider of comprehensive software risk management solutions, empowering organizations to secure their digital assets and build a safer, more resilient connected world including:

Industrial/OT, IoT, Automotive, Medical, Telecom, Consumer Electronics, and more

Speakers: Matt Wyckhouse, CEO
Larry Pesce, Vice President of Services

The Regulatory Tsunami

2025–2030: Converging Global Regulations

CE RED (2025)

EU wireless device security mandate

EU Cyber Resilience Act (2027)

Lifecycle security requirements

U.S. Cyber Trust Mark

Consumer IoT labeling program

Connected Vehicle Regulations

Automotive cybersecurity standards

The IoT industry is facing what I call a "regulatory tsunami." This convergence means companies must align simultaneously with multiple regulatory bodies, each requiring slightly different approaches. Manufacturers who treat cybersecurity as optional or reactive will find themselves locked out of major markets. Early adopters will be able to move faster, reach more markets, and build consumer trust, while laggards will face product delays or outright exclusion.

From Voluntary to Mandatory

The Shift in Cybersecurity Requirements

1

Security as "Best Practice"

Guidelines and recommendations

Industry self-regulation

2

Legal Prerequisite

Mandatory for market access

Compliance builds consumer trust

Until recently, many IoT security frameworks were voluntary, serving as guidelines or industry best practices. That is changing rapidly. By 2025, compliance will be a legal prerequisite for market access in multiple regions.

This shift forces organizations to think differently about product development. Security can no longer be an afterthought bolted on at the end—it must be embedded into the design and development lifecycle. The good news is that proactive companies can use certification as a differentiator, immediately signaling quality and trustworthiness to customers, partners, and regulators.

The Compliance Imperative:

Regulations Meet Reality

- Growing insecurity driving regulation
  - Supply chain attacks, major pervasive vulnerabilities, etc.
- Emerging global mandates and standards for device security (even for low power devices)
  - EU Cyber Resilience Act (CRA), US Cyber Trust Mark, EU Radio Equipment Directive (RED), etc.
- Mandates often assume high capability (connectivity, memory, etc.)

Solution

- Map Regulatory Requirements to Device Capabilities
- Document Risk Trade-Offs
- Lean into Standards with Modular Guidance (NIST/ETSI)
- Push for Transparency Across the Supply Chain
- ***Plan for long term support, updates, and documentation***

Timeline of Key Regulations

Compliance Deadlines (2025–2030)

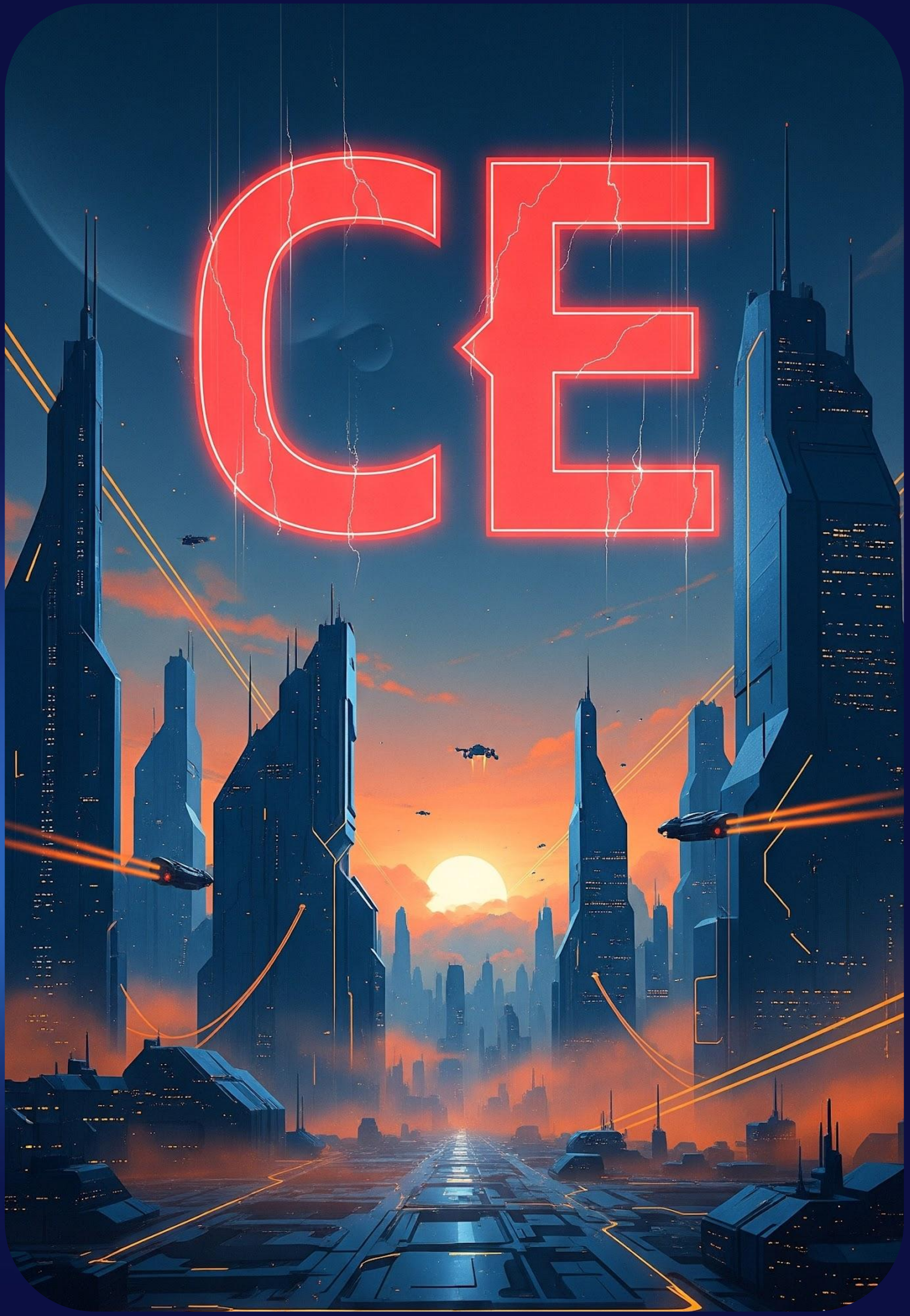
1. **2025: CE RED Article 3.3**
   EU mandatory security requirements for wireless devices become active

2. **2027: EU Cyber Resilience Act**
   Comprehensive lifecycle security requirements go live across EU

3. **U.S. Cyber Trust Mark**
   Consumer IoT labeling program (timeline pending political resolution)

4. **Connected Vehicle Regulations**
   Ongoing automotive cybersecurity compliance requirements

Mapping these requirements to your roadmap is critical. In **August 2025**, CE RED Article 3.3(d)(e)(f) goes live in the EU, requiring mandatory security, privacy, and fraud protection measures. The **Cyber Resilience Act (CRA)** expands requirements in 2027, covering the entire lifecycle of connected products. A single missed deadline could mean exclusion from a region representing millions of potential customers.



CE RED Article 3.3

FINITE STATE

EU Mandatory Requirements (2025)

Protect Networks

Safeguard infrastructure from device-based attacks and unauthorized access

Safeguard Personal Data

Implement robust privacy controls and data protection mechanisms

Prevent Fraud

Deploy anti-fraud measures and secure authentication systems

Testing + Documentation

Comprehensive validation and evidence requirements for compliance

CE RED Article 3.3(d)(e)(f) is a watershed moment requiring wireless devices to meet concrete security standards. These are not abstract goals; they come with specific test and documentation requirements including network traffic analysis, DoS resilience, and wireless penetration testing.

The key takeaway is that CE RED compliance requires early planning. Manufacturers must integrate these security assessments well before devices hit the market, making security testing a core part of the development process rather than a last-minute compliance exercise.

FINITE STATE

FINITE STATE

EU Cyber Resilience Act

Lifecycle Security (2027)

Comprehensive Coverage

- Entire device lifecycle management
- Software Bill of Materials (SBOMs) mandatory
- Continuous vulnerability management
- Incident response capabilities
- Secure-by-design development practices

Key Requirements

Ongoing Commitment: Unlike one-time certifications, CRA requires continuous security monitoring and updates.

Proactive Defense: Focus shifts from reactive patching to preventive security architecture.

The EU CRA goes beyond product launch—it requires ongoing lifecycle security including vulnerability management, incident response, and continuous monitoring. This includes SBOM generation, vulnerability enrichment, and proactive configuration assessment.

CRA compliance isn't a one-time certification. It's a continuous commitment to resilience, requiring companies to invest in processes that evolve with the threat landscape rather than viewing compliance as a "check the box" exercise.

U.S. Cyber Trust Mark

Consumer Labeling for IoT

FCC Initiative

Federal Communications Commission spearheaded program for consumer IoT security labeling and certification

Comprehensive Coverage

Software security, data protection, and network resilience requirements across device categories

Political Delays

Progress slowed due to competing political agendas and regulatory disagreements

The U.S. Cyber Trust Mark is designed to provide consumers with a recognizable label that identifies secure IoT products. While the intent is strong, progress has languished due to political overtones and competing agendas, leaving manufacturers uncertain about timelines.

Despite delays, companies should prepare now—it will eventually become a key differentiator for consumer trust. Even partial alignment with Cyber Trust Mark requirements strengthens product security and positions manufacturers favorably in the market. The mark may be delayed, but the consumer expectation it represents is already here.

Connected Vehicle Regulation

Automotive Compliance

ECU Security

Electronic Control Unit firmware analysis and vulnerability assessment across all vehicle systems

Telematics Protection

Secure communication protocols for vehicle-to-infrastructure and vehicle-to-cloud connectivity

Backend Security

Cloud infrastructure protection and API security for connected services and data management

The Connected Vehicle Regulation addresses the rapidly expanding attack surface in modern vehicles—covering ECUs, telematics, Wi-Fi, Bluetooth, and cloud backends. This includes testing in-vehicle networks like CAN bus, conducting firmware analysis, and assessing backend APIs to ensure compliance across the entire ecosystem.

For manufacturers, non-compliance can be catastrophic. Imagine an entire vehicle line unable to enter the U.S. or EU market. Proactive compliance avoids these risks while building consumer confidence in safety and resilience, protecting both revenue streams and brand reputation.

Technical Requirements

What Certification Requires

Software Bill of Materials (SBOMs)

Complete transparency into software components, dependencies, and third-party libraries for vulnerability tracking

Security & Resilience Testing

Penetration testing, firmware analysis, cryptographic assessment, and network resilience validation

Continuous Vulnerability Management

Ongoing monitoring, patch management, and incident response capabilities throughout product lifecycle

At a technical level, certification requires three core pillars: **SBOMs** provide transparency, **security testing** validates resilience, and **vulnerability management** ensures security doesn't erode post-launch.

Hardware changes are rarely required. Most certifications focus on firmware, software, and processes. However, documentation and evidence are critical; without them, compliance claims won't hold. This is where partnerships with trusted providers become essential for building reusable testing and reporting frameworks that satisfy multiple global certifications without duplicating work.

SBOMs as Foundation

Software Transparency

01

Component Discovery

Identify all software components, libraries, and dependencies within the device firmware and applications

02

Vulnerability Mapping

Map identified components to known vulnerabilities, CVEs, and security advisories for risk assessment

03

Enrichment & Analysis

Enhance SBOM data with CWEs, CPEs, and threat intelligence for comprehensive security visibility

04

Lifecycle Management

Maintain and update SBOM throughout product lifecycle for ongoing vulnerability management

The Software Bill of Materials (SBOM) is emerging as the cornerstone of cybersecurity certification, providing essential visibility into what's inside your product. This transparency enables vulnerability identification, lifecycle management, and regulatory compliance across multiple frameworks.

Specialized binary analysis and enriched SBOM generation allows manufacturers to map vulnerabilities, CWEs, and CPEs to component directories.

Think of the SBOM not as a regulatory burden, but as a strategic asset—with proper enrichment, it becomes a tool for proactive defense, supplier transparency, and accelerated certification across multiple regulatory frameworks.

Case Study: Consumer IoT

Cyber Trust Mark Alignment

Early Adoption Strategy

- Proactive alignment with Cyber Trust Mark requirements
- Comprehensive firmware and wireless testing
- SBOM generation and vulnerability management
- "Secure-by-design" reputation building

Business Impact

Marketing Advantage: Security became a key differentiator before regulatory mandate

Retail Partnerships: Won partnerships requiring stronger security baselines

Future-Proof: Ready for certification when requirements become final

The delays in U.S. rollout illustrate a key strategic point: don't wait for full political consensus. Market expectations and partner requirements often arrive faster than regulators. For this manufacturer, proactive alignment not only eased eventual certification but became a powerful marketing differentiator, helping secure retail partnerships that demanded stronger security baselines.

Case Study: Automotive

Connected Vehicle Compliance

In the automotive sector, compliance isn't optional. One OEM integrated SBOM analysis, ECU firmware testing, and backend penetration testing early in their design process, reducing certification delays by months while ensuring comprehensive security coverage.

The integrated approach validated CAN bus security, telematics resilience, and backend APIs, aligning directly with Connected Vehicle Regulation requirements. The result was accelerated market access, reduced recall risk, and stronger consumer trust. For automotive manufacturers, this represents more than compliance—it's about ensuring passenger safety and avoiding catastrophic brand damage that could result from security incidents.

ECU Firmware Testing

Comprehensive analysis of Electronic Control Unit firmware for vulnerabilities and security weaknesses

CAN Bus & Telematics Validation

In-vehicle network security testing and telematics communication protocol assessment

Backend API Security

Penetration testing of cloud services and API endpoints supporting connected vehicle features

FINITE STATE

Certification Journeys

End-to-End Support

Consulting & Planning

Regulatory landscape analysis and compliance strategy development tailored to your products and target markets

Testing & Validation

Comprehensive security testing including penetration testing, firmware analysis, and SBOM generation

Reporting & Documentation

Detailed compliance reports and evidence packages meeting regulatory requirements across jurisdictions

Certification Assistance

Guidance through submission processes and ongoing support for maintaining compliance status

Achieving certification isn't a single task: it's a comprehensive journey requiring early planning, iterative testing, thorough documentation, and sometimes retesting based on findings or regulatory updates.

An integrated service model helps manufacturers navigate this journey by combining consulting, hands-on testing, and certification assistance. This approach reduces duplication, shortens time-to-market, and ensures consistent quality across all target markets. By building certification into the product lifecycle rather than treating it as an afterthought, manufacturers can reduce costs, avoid delays, and establish security as a core competitive business advantage.

ROI of Proactive Compliance

Competitive Advantage

Faster Market Entry

Reduced time-to-market through proactive compliance planning

Cost Reduction

Lower certification costs compared to reactive compliance approaches

Revenue Protection

Avoided revenue loss from delayed or blocked product launches

Compliance is often viewed as a cost center, but the return on investment is substantial and measurable. Proactive companies avoid last-minute rushes, product delays, regulatory fines, and market exclusion. More importantly, they can leverage certification as a powerful marketing differentiator and trust signal.

Early adopters of standards like the Cyber Trust Mark can highlight consumer-friendly security labeling while competitors scramble to catch up. The same principle applies to CE RED and CRA compliance in European markets. When compliance becomes integrated into the development lifecycle, it creates operational efficiencies that extend far beyond regulatory requirements: reduced vulnerabilities, improved supplier management, faster market entry, and enhanced customer trust.

The Business Case

Why Compliance Matters

Legal Market Entry

Mandatory prerequisite for shipping products in regulated markets

Consumer Trust

Certification builds confidence and differentiates secure products

Market Leadership

Early compliance creates sustainable competitive advantages

Revenue Protection

Ensures continued access to key markets and customer segments

Certification represents far more than a legal hurdle—it has become an essential business necessity for market participation. Without proper certification, devices cannot legally ship in key markets, directly impacting revenue potential and growth opportunities.

Regulatory bodies are clearly signaling that cybersecurity is now a prerequisite for market participation, not an optional enhancement. For manufacturers, the strategic choice is straightforward: comply proactively and thrive, or delay and risk exclusion from lucrative markets. Viewed strategically, compliance ensures not just legal market access but creates sustainable competitive advantages while protecting revenue streams and enhancing brand trust in an increasingly security-conscious consumer landscape.

U.S. Political Climate

Cyber Trust Mark Challenges

Political Reality: The FCC's Cyber Trust Mark has become mired in political disagreements, with stakeholders divided on regulatory burden versus consumer protection benefits.

Current Challenges

- Political gridlock slowing federal rollout
- Competing stakeholder interests and priorities
- Uncertain timelines creating manufacturer hesitancy
- Industry confusion about requirements and scope

Market Reality

Consumer Expectations: Security labeling demand has moved ahead of policy

Retail Requirements: Distributors increasingly require security evidence

We must address the political reality: while the FCC's Cyber Trust Mark launched with strong bipartisan support, it has since become entangled in broader political disagreements about federal regulation versus industry self-governance.

This political gridlock has created uncertainty about timelines and implementation details. However, the challenge is that consumer expectations for security labeling have already evolved—retailers and distributors are beginning to require stronger evidence of security regardless of federal program delays. My recommendation: treat the Cyber Trust Mark as inevitable and build toward its requirements now. When political resolution occurs, compliant companies will have a significant first-mover advantage.

Global Alignment

Efficiency Across Markets

Avoid Duplicated Effort

Eliminate redundant testing and documentation across multiple regulatory frameworks through strategic alignment

Reuse Testing & Reports

Leverage common security testing methodologies and evidence packages across EU, US, and global certifications

Unified Compliance Framework

Implement integrated approach that satisfies multiple regulatory requirements simultaneously

One of the biggest operational challenges for global manufacturers is avoiding duplicated effort—preventing the need to test the same device multiple times for different regional requirements. This redundancy drives up costs, extends timelines, and increases the risk of inconsistent results.

The solution involves building reusable testing and reporting frameworks that strategically map across EU, US, and global certifications. This approach reduces wasted effort, ensures consistent quality across all target markets, and provides a unified view of product security posture. Global alignment isn't just about operational efficiency—it reduces the risk of conflicting compliance results, accelerates certification processes, and creates a comprehensive foundation for ongoing security management.

How Finite State Helps

Our Services

1

Penetration Testing & Analysis

Comprehensive security assessments including firmware analysis, network testing, and vulnerability identification

2

SBOM Enrichment

Advanced software bill of materials generation with vulnerability mapping, CVE analysis, and component intelligence

3

Certification Assistance

End-to-end support for regulatory compliance including documentation, submission guidance, and ongoing maintenance

Finite State provides a comprehensive suite of services specifically tailored to IoT compliance challenges. Our expertise spans penetration testing, firmware analysis, SBOM enrichment, vulnerability management, and certification assistance across multiple industry verticals.

Our team brings deep domain expertise in IoT, automotive, healthcare, and ICS/OT security environments. We've successfully helped organizations achieve compliance with CE RED, CRA, Cyber Trust Mark, FDA 524B, and numerous other regulatory frameworks across diverse industries. This breadth of experience allows us to deliver not just compliance documentation, but genuine confidence that products are secure, resilient, and trusted by both regulators and end customers.

Action Plan

What To Do Now

1 Map Deadlines to Products

Create comprehensive timeline aligning regulatory requirements with your product roadmap and release schedule

2 Start SBOMs + Enrichment

Begin software bill of materials generation and vulnerability enrichment for existing and planned products

3 Integrate Testing into Lifecycle

Embed security testing into development pipelines rather than treating it as a final compliance step

4 Prepare for CRA + Cyber Trust Mark

Align early with lifecycle security requirements and US labeling expectations despite political delays

By starting today, you avoid last-minute compliance surprises and build security into your products from the ground up. Waiting until compliance becomes mandatory is a recipe for rushed work, costly rework, and potential market exclusion.

The companies who act now will not only achieve compliance—they will establish market leadership through superior security posture, customer trust, and operational efficiency. This proactive approach transforms regulatory requirements from business obstacles into competitive advantages that drive long-term success.

FINITE STATE

Thank You – Questions?

Closing & Q&A

QUECTEL
Q1-XXXXX
BG96
MA
BG96MA-128-SGNS
SN:XXXXXXXXXXXXXXX
IMEI:XXXXXXXXXXXXXXX

Q&A Session

MASTER CLASS

INDUSTRY-LEADING IoT WEBINARS

Don’t forget to visit the Masterclass hub:

Todays Masterclass will be uploaded onto the Masterclass hub library shortly. The Library enables you to access all our previous Masterclasses : https://www.quectel.com/masterclass-library

Our dedicated team is here to serve you.
If you have any questions or need further information email us at Masterclass@Quectel.com

Thank you

For more information, please visit: quectel.com, LinkedIn, Facebook and X.
Media contact: media@quectel.com

Sales Support: **sales@quectel.com**
Technical Support: **support@quectel.com** General: **info@quectel.com**

QUECTEL