



How Do I Comply? Navigating the Maze of IoT Regulations and Standards

May 30, 2019

www.securityindustry.org



VDOO

How Do I Comply?

Navigating the Maze of IoT Regulations and Standards

▶ ▶ ▶ May 30th, 2019

Agenda

Introduction

- Regulation and standardization

Regulation

- Risk and impact
- Cyber-security and privacy

Standardization

- Challenges
- Compliance process
- Automating compliance





- Security Architect with ~15 years experience, much of it in embedded.
- Currently at VDOO, working on automated firmware scanners and security requirement generation.
- Incorporating requirements from cyber-security standards such as ISA 62443, UL 2900.
- Previously at ARM, dealing with IoT security in the ARM Mbed Client and Cloud products.
- Participated in standardization forums.
- Helped certify embedded security modules to the FIPS 140-2 standard.
- Working with the SIA IoT Subcommittee on best practice guidance.

Regulation and enforcement

- Government-mandated
- Carries penalties
- May require compliance to standard



Standardization

- Tender requirements
- Customer demands
- Mandated by industry regulation
- Provides competitive advantage

Common sanctions for non-compliance with these regulations could have serious financial and reputational implications for corporations and staff, including:

- Fines
- Personal liability and imprisonment of managers or officers
- Cease and desist orders
- Erasure of data
- Public announcements and product recalls
- Binding instructions on security features

<https://www.iotsecurityfoundation.org/best-practice-guidelines/>

Regulation vs. Standardization

	Regulation	Standardization
Development pace	○○●low	○○●medium
Differs by region	●●●high	○○●low
Differs by industry	○○●medium	●●●high
Technical detail level	○○●medium	●●●high
Enforced	✓yes	?maybe
Explicit certification	?maybe	?maybe

Regulation



- Enforced by governments
 - Regional
- Created by government and legislators
 - Rarely released
 - Not very detailed
 - Different scopes by legislator
- Specific to an industry
 - Medical, automotive, critical infrastructure
- Specific to a topic
 - Safety, privacy, child protection





Overview paper from the IoT Security Foundation

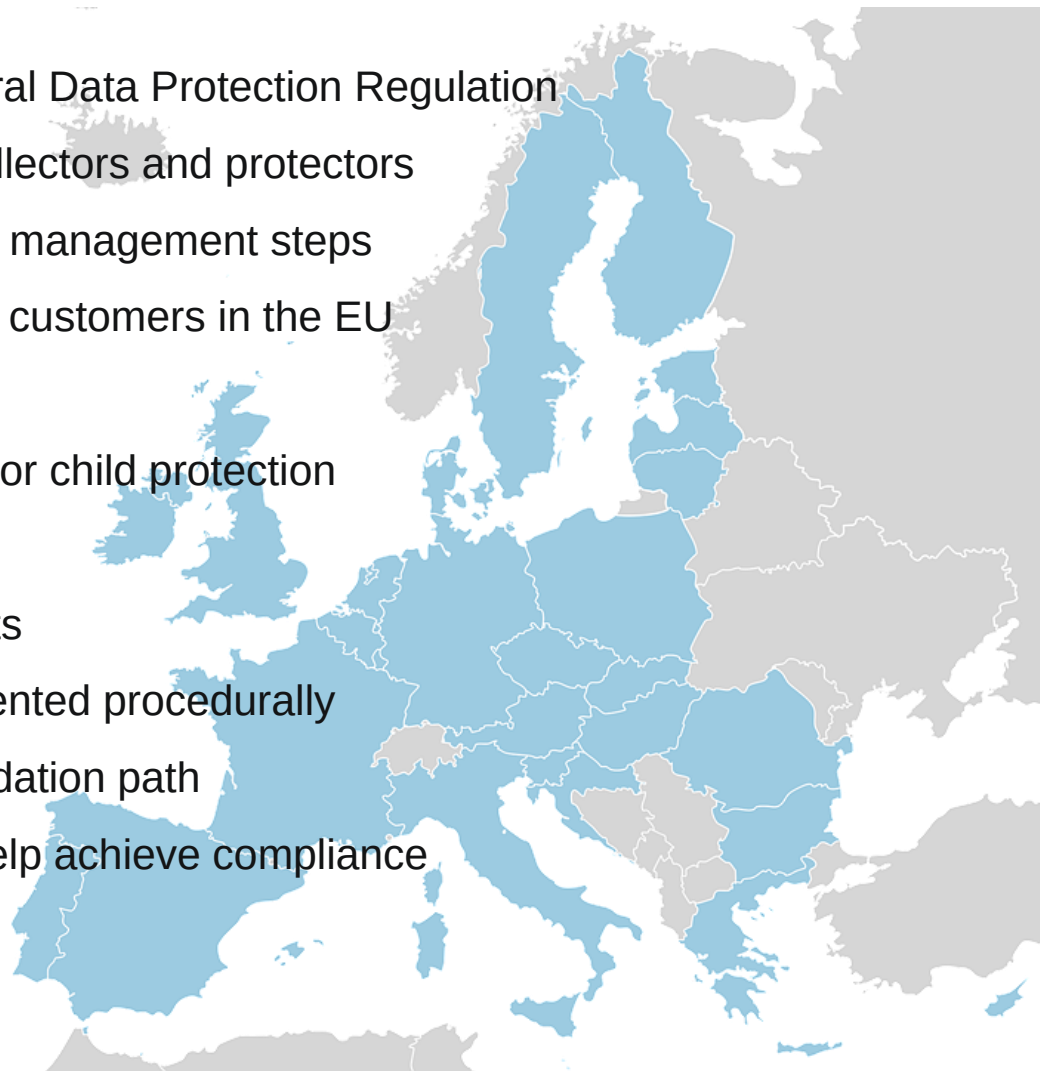
<https://www.iotsecurityfoundation.org/best-practice-guidelines/>

Regulation	Maximum Fine ³
General Data Protection Regulation (EU) [ref 13]	€10 million up to 2% global turnover or, €20 million up to 4% global turnover
Federal Trade Commission Act (USA) [ref 17]	\$41,484 (per violation, per day)
Digital Economy Act (UK) [ref37]	£20,000 a day not to exceed 10% of gross revenue
Privacy Act 1988 and Notifiable Data Breaches Acts (Australia) [ref 4]	A\$420,000 (individuals) A\$2.1 million (corporations)
Health Products Act (Singapore) [ref 33]	S\$50,000 (individuals) S\$100,000 (corporations)

Table 1 Financial Penalties

<https://www.iotsecurityfoundation.org/best-practice-guidelines/>

- The European Union's General Data Protection Regulation
- Imposes liabilities on data collectors and protectors
- Requires data protection and management steps
- Applies to all companies with customers in the EU
- May be updated legislatively
- Contains specific provisions for child protection
- Technically vague
 - No testable requirements
 - May be entirely implemented procedurally
- No official certification or validation path
- Consulting companies can help achieve compliance



FDA regulations only apply if the device intends to:

- ... Diagnose, prevent, cure, mitigate, or treat
- ... A disease or other condition
- ... That affects the structure or function of the body

FDA guidance

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- Postmarket Management of Cybersecurity in Medical Devices
- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software



<https://www.fda.gov/medical-devices/digital-health/cybersecurity>



Regulation	Sanctions
Federal Trade Commission Act	• Fines up to \$41,484 per violation, per day • Restitution for domestic and foreign victims • Audits (one-off or repeated) • Product recall or cease and desist orders • Imprisonment • Federal court and/or state civil action lawsuit • Requests for documentary evidence

Table 11 Sanctions: Federal Trade Commission Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 52: Dissemination of false advertisements (misrepresentation)	• Internationally recognised standards • Certification or conformity assessment • Adoption of security and best practice frameworks
Section 45: Unfair methods of competition unlawful; prevention by Commission (causes or is likely to cause substantial injury)	• Product lifecycle management and support • Encryption • Anonymisation and pseudonymisation
Section 50: Offenses and penalties (failure to produce documentary evidence)	• Certification or conformity assessment • Data Protection Policy • Privacy- and security-by-design policies • System or technical logs or backup files

Table 12 Treatment Examples: Federal Trade Commission Act

<https://www.iotsecurityfoundation.org/best-practice-guidelines/>



VS. **TRENDnet**



“TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were “secure.” In fact, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras’ Internet address.”

The charges were settled, with TRENDnet agreeing to:

- Stop misleading marketing
- Provide customers with free tech support over 2 years
- Establish a comprehensive information security program with third-party security audits every 2 years for 20 years.



<https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc>



VS. **ASUS**®

“ASUS marketed its routers as including numerous security features that the company claimed could “protect computers from any unauthorized access, hacking, and virus attacks” and “protect [the] local network against attacks from hackers.” Despite these claims, the FTC's complaint alleges that ASUS didn't take reasonable steps to secure the software on its routers.”

The charges were settled, with ASUS agreeing to:

- Stop misleading marketing
- A 20-year security program, subject to independent audits
- Asus will have to notify consumers about software updates



<https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>



VS. **D-Link**

The case is ongoing, with FTC seeking an injunction.

“D-Link promoted the security of its routers on the company’s website, which included materials headlined “EASY TO SECURE” and “ADVANCED NETWORK SECURITY.” But despite the claims made by D-Link, the FTC alleged, the company failed to take steps to address well-known and easily preventable security flaws”



<https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate>

- **European Union**
 - GDPR is now in effect
 - EU Cybersecurity Act – in advanced draft stages
- **UK** - Code of Practice for Consumer IoT Security
- **US** - California's Senate Bill 327
 - Requires "reasonable" security features in IoT devices
- **US** - Internet of Things (IoT) Cybersecurity Improvement Act of 2019
 - Devices sold to federal government must comply with NIST standards
- **US** - FDA Cybersecurity Guidance
- **Australia** – Consumer IoT Rating System
- **Japan** – Talks of regulation in time for the Tokyo 2020 Olympics



The trend forward is more cybersecurity regulation

Standardization



- Standards help consumers put their trust in a product
- Created by government and independent organizations
 - Government bodies (example: NIST)
 - For-profit companies (example: Underwriter Labs)
 - Non-profit organizations (example: IoT Security Foundation)
- Contain requirements
 - High level, or
 - Specific and detailed
- Scope can vary
 - Industry (example: Medical devices, Smart Grid)
 - Technology or protocol (example: Bluetooth, TCP)



Choosing relevant standards

- Which standards to comply with?

Requirement clarity and phrasing

- High-level requirements
- Deriving actionable tasks

Requirement relevance

- Match the industry, product type, and use case
- Contradictions in multiple standards

Cost and time

- Initial gap report
- Implementation
- Maintaining compliance

Verifying compliance

- Third-party testing

Selected Standard Organizations





Development pace

- Last published in 2002
- Incremental changes made to guidance documents
- To be superseded by FIPS 140-3 in 2020

Region

- Originally – US
- In fact widely influential

Industry and product class

- Originally - cryptographic modules
- In fact widely used in the entire industry

Technical detail level

- High

Enforcement

- For US government purchases only

Certification type

- Explicit - [Cryptographic Module Validation Program](#)
- Uses certification laboratories
- Involves releasing materials to the public
- Explicit re-certification program
- Many companies claim compliance without certification

By what the regulation requires

- Usually determined by region and product class

By industry vertical

- Medical
- Automotive
- Industrial control
- Children's products

By what the customers demand

- Tender requirements

By what competitors do

- Compliance can affect customer demand
- Compliance can serve as a competitive advantage

Finding out which standards and regulation apply is not a trivial task!

Compliant by declaration

- Marketing information only

Self-certification

- Questionnaire
- Documentation
- Automated tests

Third-party certification

- Certified laboratories
- Independent bodies
- Pen-testing

Requirements can be difficult to understand

- Written in “legalese”
- Use terminology from a different field
- Often too high-level
- Sometimes too specific

Some requirements can be irrelevant

- Because of product class
- Different protocols and components
- Different physical interfaces
- Depending on certification type and level

AS02.05: (Levels 1, 2, 3, and 4) All data (except status data output via the status output interface) that is output from the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another module) shall exit via the “data output” interface.

Getting help

- Consultants
- Laboratories

Going through certification

- Development
- Documentation
- Dedicated point of contact

Receiving a certificate

- Interacting with the certifying body (government or industry)

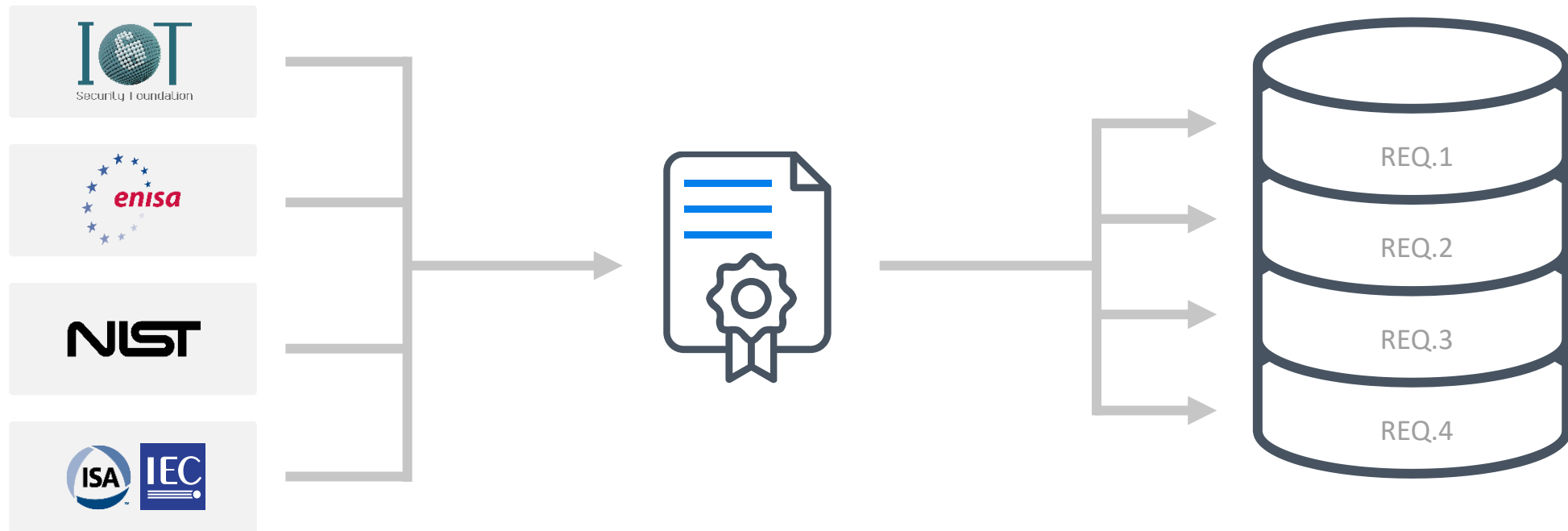
Maintaining a certificate

- Maintaining certification while patching the product
- Re-certifying your next product version
- Expiration (sunsetting)

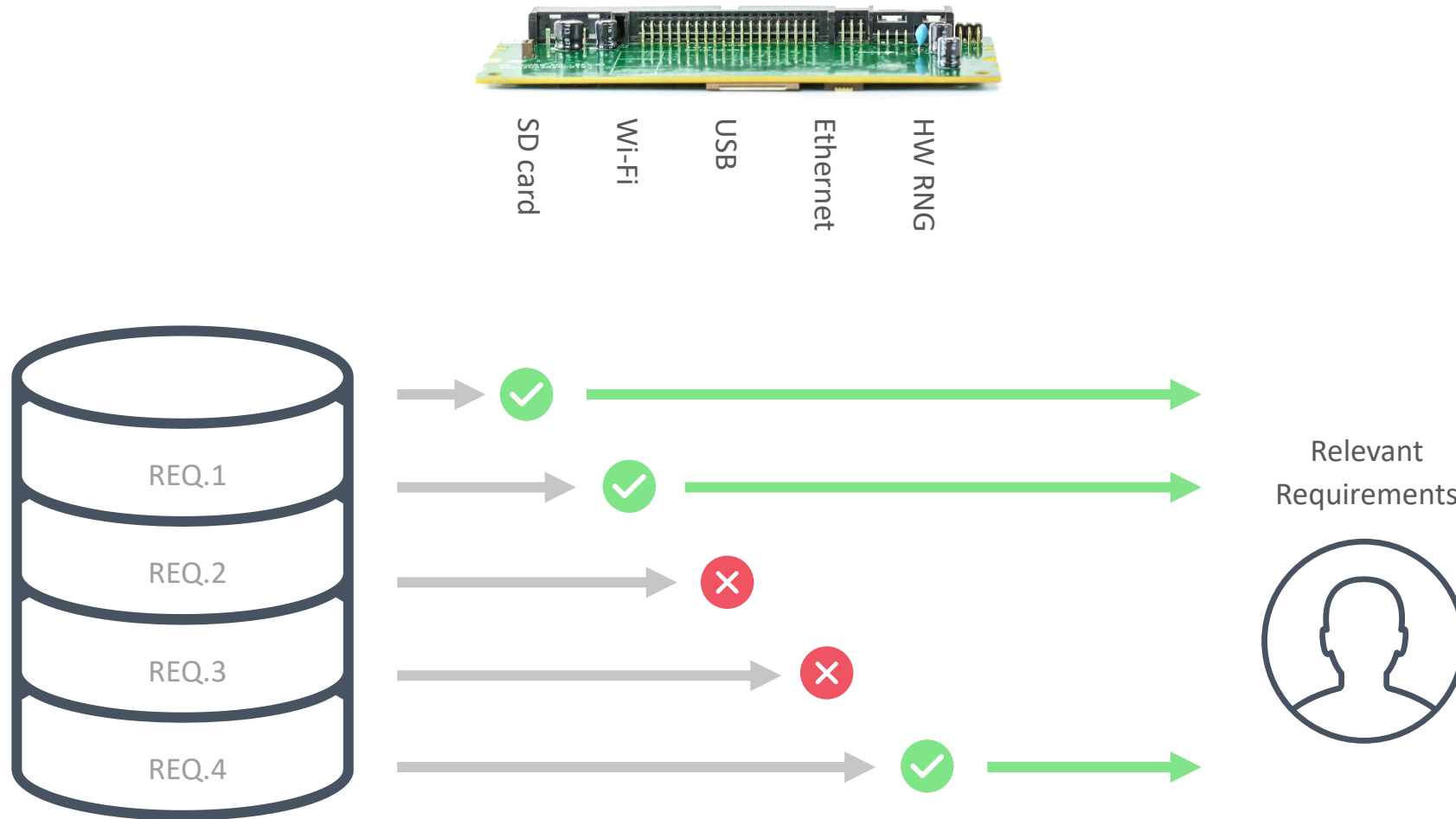
Automating Compliance



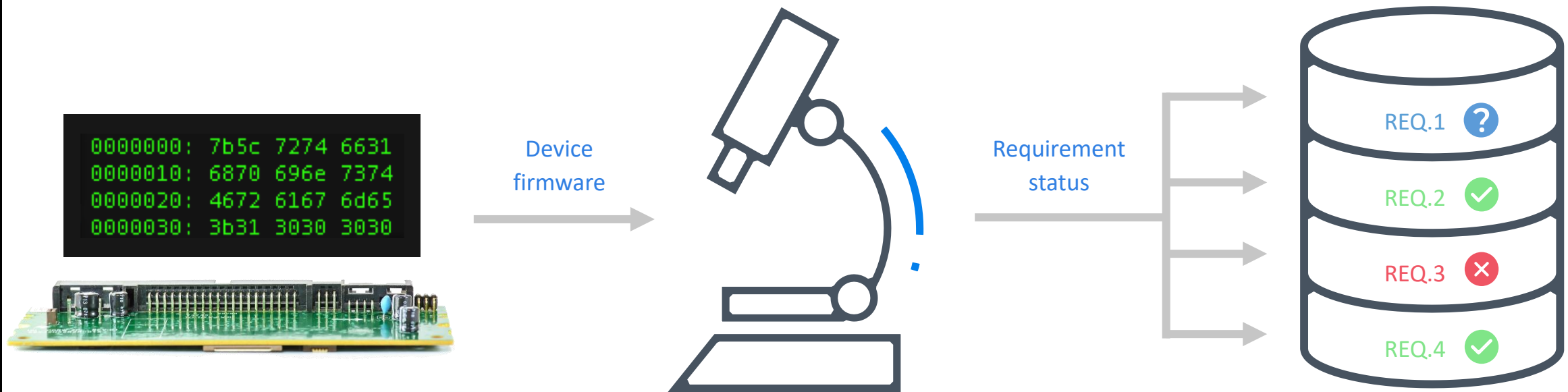
Explicitly Map Relevant Standards



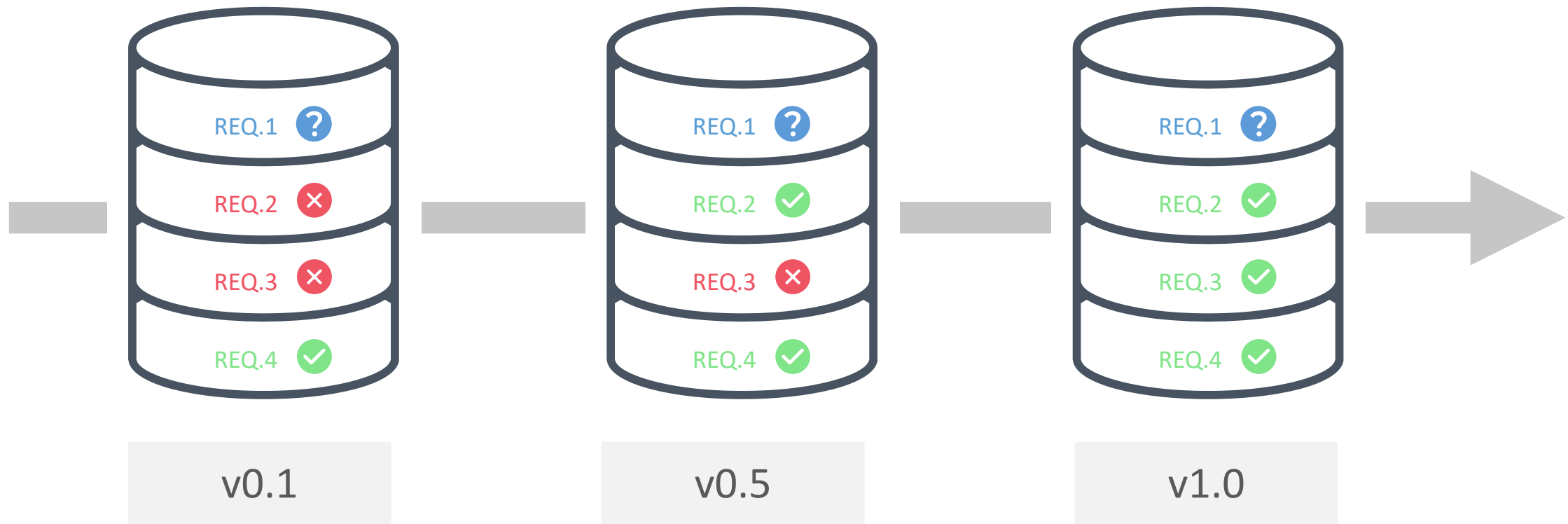
Filter For Relevant Requirements



Perform Automated Testing



Integrate with Continuous Development





VDOO

Thank you

▶ ▶ ▶ Leo Dorrendorf, Senior Security Architect
leo@vdoo.com

- Survey the regulation and standardization landscape for your product
- Examine the market drivers to compliance
- Select which standards and regulations to comply to
- Create a compliance roadmap
- Get in touch with certification laboratories or independent consultants
- Assign organizational roles and responsibilities
- Assign time to perform the necessary tasks
- Create a unified list of requirements
- Create and implement tests for compliance
- Integrate compliance with your development process
- Certify your product
- Repeat!