Regulatory Gap & Security Architecture Report

Automated Compliance Analysis & Risk Assessment

TARGET OF EVALUATION

GridForge Industrial Edge Gateway

SCOPE OF ASSESSMENT

Target Markets:	European Union, United States
Declaration Date:	13 Jan 2026
Assessment Type:	Preliminary Design Declaration (Self-Attested)

`Date of Issue: 13 Jan 2026`

Disclaimer: This report identifies potential gaps based on provided design declarations. It does not constitute a certification of conformity.

Reader's Guide

Table of Contents

About This Audit

Assessment Context & Scope

This document constitutes an automated security & regulatory gap analysis derived from the manufacturer's technical declarations. It evaluates the device's design posture against the Active Regulatory Profile (covering applicable frameworks such as EU RED/CRA, UK PSTI, NIST, or ETSI) to detect critical compliance blockers prior to official laboratory testing.

Objective: To identify "Blocker" risks preventing market entry and reducing post-market liability.

Scope: Holistic verification of Hardware, Firmware, Connectivity, and Lifecycle Management.

Limitation: Preliminary risk assessment. Not a formal Certificate of Conformity.

Input Verification: The validity of these findings relies on the accuracy of the design parameters provided. The complete record of technical declarations used for this assessment is preserved in Technical Design Declaration.

Confidentiality Notice: This report contains sensitive vulnerability data. Distribution should be limited to authorized engineering and compliance personnel.

Executive Summary

Launch Readiness

High Launch Risk

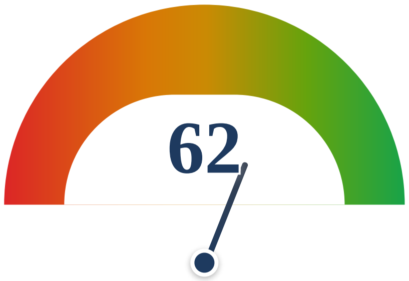
🛑 **Blocked**

Your architecture meets baseline **United States** requirements but fails specific **European Union** mandates.

Market Assessment

Market	Status	Critical Gaps
European Union	⛔ Market Blocked	1 Blocker, 1 Critical
United States	✅ Ready to Launch	None

Composite Defense Score



Aggregated score of Regulatory, Security, and Business risks.

Strategic Risk Profile

Findings grouped by business impact to justify the fix.

Regulatory

Assessment: 🔴 Critical

Risk Count: 9

Why Fix: EU Market Ban. Your configuration violates regulatory requirements.

Top Risk: EU AI Act: High-Risk Non-Compliance

Commercial

Assessment: 🔴 Critical

Risk Count: 11

Why Fix: Revenue at risk. IP or service theft vulnerabilities present.

Top Risk: AI Model Theft or Poisoning

Lifecycle

Assessment: 🟠 High

Risk Count: 7

Why Fix: Vendor support ends before device EOL. Security patches unavailable.

Top Risk: Supply Chain: Silicon EOL Mismatch

Security

Assessment: 🔴 Critical

Risk Count: 6

Why Fix: Attack Target. Critical security vulnerabilities present.

Top Risk: EU AI Act: Missing Transparency Disclosures

Compliance Horizon

Timeline of regulatory deadlines affecting your product.

Active Market Restrictions (1)

🔴 **EU AI Act (Regulation (EU) 2024/1689)** (EU)

Non-compliance with Bans manipulative AI in IoT

Upcoming Deadlines (5)

🟡 **EU Payment Services Directive 3 (PSD3)** - 01 Jun 2026 (139 days)

Strong customer authentication for IoT payments

⚪ **EU Cyber Resilience Act (CRA)** - 11 Sept 2026 (241 days)

24h/72h incident reports mandatory

⚪ **EU eIDAS 2.0 Regulation (Electronic Identification)** - 01 Dec 2026 (322 days)

Member states must offer EU Digital Identity Wallets

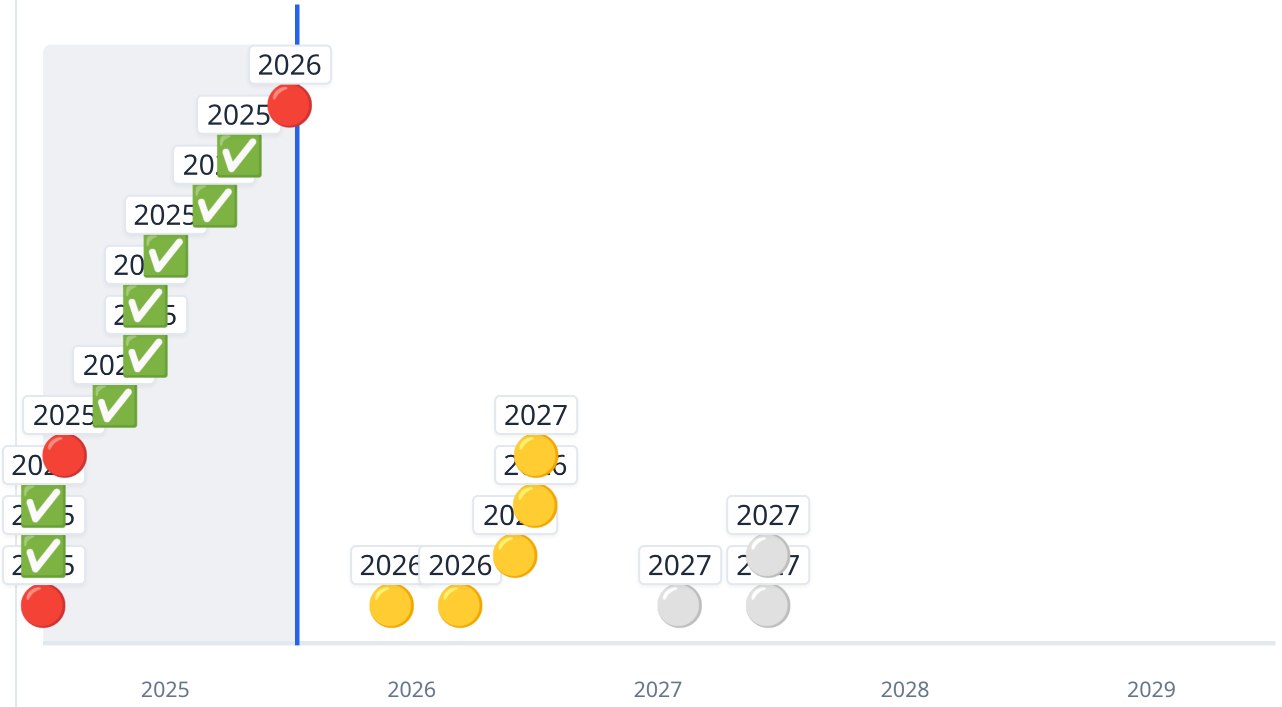
⚪ **EU Post-Quantum Cryptography Roadmap (2025)** - 31 Dec 2026 (352 days)

Inventory/assess IoT

⚪ **EU Ecodesign for Sustainable Products (ESPR) - Digital Product Passport** - 01 Jan 2027 (353 days)

DPP implementation starts - 1 gap(s)

Regulatory Enforcement Timeline (2025-2029)



Applicable Regulations

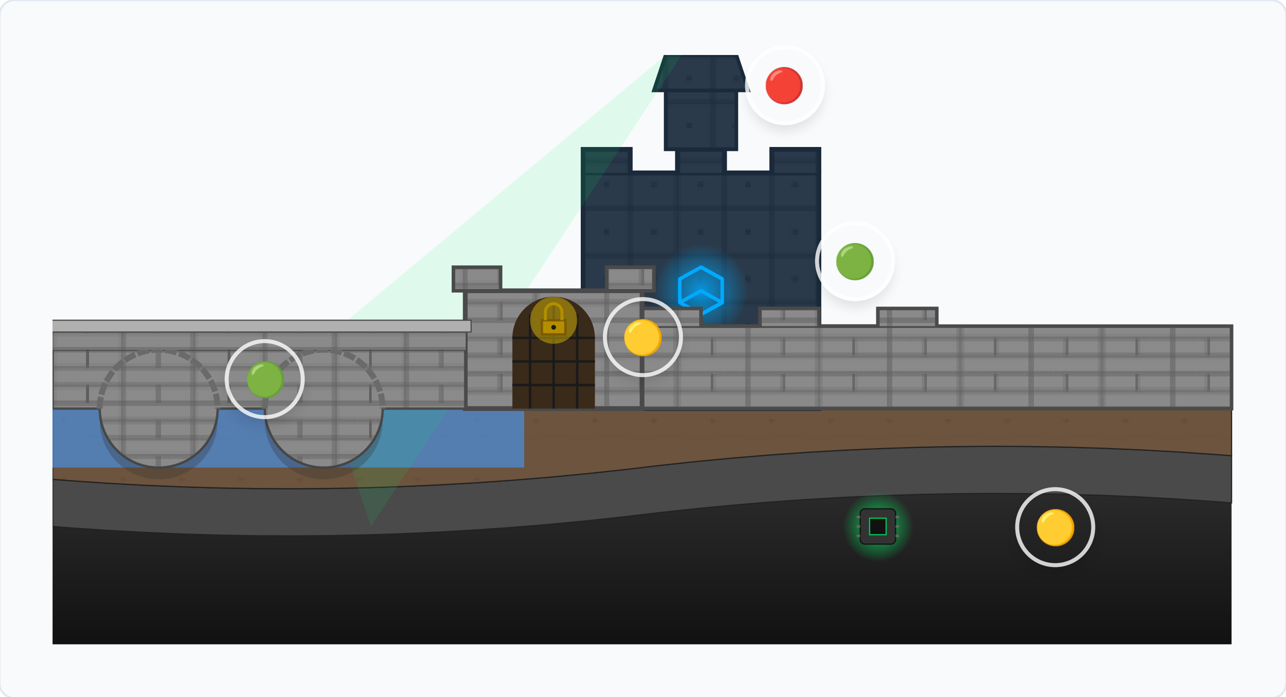
Regulation	Status	Next Deadline	Jurisdiction
EU Cyber Resilience Act (CRA)	compliant	11 Sept 2026	EU
EU CRA Supply Chain Requirements (Annex I)	compliant	11 Dec 2027	EU
NIS2 Directive (Network and Information Systems Directive 2)	compliant	Active (17 Apr 2025)	EU
EU Critical Entities Resilience Directive (CER)	compliant	Active (18 Oct 2025)	EU
EU AI Act (Regulation (EU) 2024/1689)	non_compliant	02 Aug 2027	EU
EU Data Act (Regulation (EU) 2023/2854)	compliant	Active (12 Sept 2025)	EU
EU ePrivacy Directive (Cookie Law)	compliant	Active (31 Jul 2002)	EU
EU Ecodesign for Sustainable Products (ESPR) - Digital Product Passport	at_risk	01 Jan 2027	EU
EU WEEE Directive (Waste Electrical and Electronic Equipment)	at_risk	Active (01 Jan 2026)	EU
EU Payment Services Directive 3 (PSD3)	compliant	01 Jun 2026	EU
EU Basel IV (Op Risk for Financial IoT)	compliant	Active (01 Jan 2025)	EU
EU Post-Quantum Cryptography Roadmap (2025)	compliant	31 Dec 2026	EU
US IoT Cybersecurity Improvement Act of 2020	compliant	Active (23 Sept 2022)	US
US FCC Cyber Trust Mark (Voluntary IoT Labeling)	compliant	Active (01 Jan 2025)	US
US Cybersecurity Maturity Model Certification (CMMC 2.0)	compliant	Active (01 Jun 2025)	US-DoD
California IoT Security Law (SB-327)	compliant	Active (01 Jan 2020)	US-CA
US Children's Online Privacy Protection Act (COPPA)	compliant	Active (21 Apr 2000)	US
US Oregon HB 2395 (Connected Device Security)	compliant	Active (01 Jan 2020)	US-OR
Basel Convention on Hazardous Wastes (E-Waste Amendments)	at_risk	Active (01 Jan 2025)	Global

Regulation	Status	Next Deadline	Jurisdiction
Global WEEE Extensions (UN/ITU Guidelines 2025)	compliant	Active (01 Jun 2025)	Global
EU eIDAS 2.0 Regulation (Electronic Identification)	compliant	01 Dec 2026	EU

Architectural Defense Posture

Your architecture visualized as a fortress. Each layer represents a defense domain - color shows where the architecture is broken at a glance.

Overall Health: 🔴 Critical



🔭 The Watchtower

Domain: Lifecycle & Process

Status: 🔴 At Risk (4 risks)

Finding: Critical infrastructure AI subject to mandatory conformity assessment.

📡 The Bridge

Domain: Network & Cloud

Status: 🟢 Secure (0 risks)

Finding: No issues detected in this layer.

🛡️ The Gate

Domain: Identity & Auth

Status: 🟡 Attention (1 risk)

Finding: Violation of AI Act Art. 50 (Transparency obligations). Mandatory disclosure required.

🔒 The Keep

Domain: OS Hardening & Data

Status: 🟢 Secure (1 risk)

Finding: Proprietary ML model is valuable IP.

⚙️ The Bedrock

Domain: Supply Chain & Hardware

Status: 🟡 Attention (5 risks)

Finding: WEEE and Basel Convention require EPR for electronic waste.

Critical Findings & Remediation

Top priority risks requiring immediate architectural changes.

Risk Details

#1 EU AI Act: High-Risk Non-Compliance

BLOCKER

Finding:
Critical infrastructure AI subject to mandatory conformity assessment.

Remediation:
Establish AI Risk Management System per Article 9 and implement input validation.

💰 **Estimate:** High Effort, High Cost

#2 AI Governance Maturity Gap

HIGH

Finding:
High-risk AI system without formal AI management system (ISO 42001 or equivalent).

Remediation:
Implement AI Management System aligned with ISO/IEC 42001 framework.

💰 **Estimate:** High Effort, High Cost

#3 E-Waste Supply Chain Risk

MEDIUM

Finding:
WEEE and Basel Convention require EPR for electronic waste.

Remediation:
Implement EPR program with certified recyclers.

💰 **Estimate:** Medium Effort, Medium Cost

#4 EU AI Act: Missing Transparency Disclosures

MEDIUM

Finding:
Violation of AI Act Art. 50 (Transparency obligations). Mandatory disclosure required.

Remediation:
Implement clear, easily recognizable AI interaction notices or watermarks.

💰 **Estimate:** Low Effort, Low Cost

#5 Supply Chain: Silicon EOL Mismatch

MEDIUM

Finding:
Vendor support ends before device EOL. Security patches unavailable.

Remediation:
Secure lifetime buy stock or migrate to Long-Term Support (LTS) silicon.

💰 **Estimate:** Very_high Effort, Very_high Cost

#6 Unmanaged Supply Chain

MEDIUM

Finding:
CRA requires due diligence on third-party components.

Remediation:
Implement supply chain vetting and continuous SBOM monitoring.

💰 **Estimate:** High Effort, High Cost

#7 Build Pipeline Injection

LOW

Finding:
No SAST/SCA to detect malicious dependencies.

Remediation:
Implement SLSA Level 3. Signed builds with provenance attestation.

💰 **Estimate:** High Effort, High Cost

#8 E-Waste Liability

LOW

Finding:
Short software lifecycle creates premature e-waste.

Remediation:
Design for recyclability. Implement software longevity plan.

💰 **Estimate:** Medium Effort, Medium Cost

#9 AI Model Theft or Poisoning

LOW

Finding:
Proprietary ML model is valuable IP.

Remediation:
Encrypt model at rest. Implement input sanitization and anomaly detection.

💰 **Estimate:** High Effort, High Cost

#10 No Automated Vulnerability Scanning

LOW

Finding:
Firmware shipped without continuous vulnerability scanning.

Remediation:
Integrate vulnerability scanning (e.g., Trivy, Snyk) into CI/CD pipeline.

💰 **Estimate:** Low Effort, Low Cost

#11 Critical IPR Theft Risk

LOW

Finding:
Firmware can be easily extracted and cloned by competitors.

Remediation:
Burn JTAG disable fuses and enable Hardware Readout Protection or equivalent device lifecycle locking.

💰 **Estimate:** Low Effort, Low Cost

Next Steps

Remediation & Assurance Plan

To move from this preliminary audit to a market-ready state, we recommend the following 3-step assurance cycle. This process prioritizes regulatory safety before investing in expensive physical testing.

1. Validate & Annotate

Use the **Traceability Matrix** in **Appendix B** as your working document.

- **Validate:** Review each finding against your specific implementation context.
- **Annotate:** Mark findings as "Confirmed," "False Positive," or "Risk Accepted" (where legally permissible).
- **Decision:** Clearly differentiate between *Architecture Blockers* (which require hardware changes) and *Documentation Gaps* (which require paperwork).

2. Strategic Remediation

Address the "Bedrock" issues first.

- **Hardware First:** Fix Secure Boot, Silicon EOL, and Debug Port (JTAG) issues immediately. These are expensive to fix after the PCB is finalized.
- **Re-Assess:** Once remediation is complete, re-run your compliance assessment to verify your **Composite Defense Score** has improved.
- **Lab Testing:** Only proceed to formal laboratory testing (CE/FCC) once the architectural gaps are closed.

3. Continuous Vigilance

Compliance is a snapshot in time; regulations drift.

- **Monitor:** Review the **Compliance Horizon** quarterly. New laws (like the EU Cyber Resilience Act) often introduce requirements for products already in the field.
- **Certify:** Prepare the Technical File for Notified Body review only if your specific market mandates third-party certification.

> 💡 **Auditor's Tip:**
>
> **Do not fix everything.** Focus exclusively on the **Regulatory Blockers** first. A secure device that cannot legally be sold is a failed product. Optimize for *Market Access*, then iterate for *Perfection*.

Legal Disclaimer & Limitation of Scope

1. Nature of Assessment: This document is a preliminary design audit generated by the Device Prophet Engine. Whether generated automatically or subjected to expert triage, this analysis is based exclusively on the documentation and technical declarations provided by the user. It does not constitute a physical security test, source code audit, or laboratory verification of the actual hardware.
2. Accuracy of Inputs: The validity of these findings is directly dependent on the accuracy of the input data. Device Prophet accepts no liability for false negatives resulting from incomplete, inaccurate, or misleading design declarations.
3. Regulatory Status: This report identifies potential compliance gaps for risk management purposes. It does not constitute a formal "Declaration of Conformity" (DoC), a certification by a Notified Body, or a legal guarantee of market access.
4. Expert Review: Any findings marked as "Expert Reviewed" or "Triaged" represent a validation of the logic applied to the provided data, not a validation of the physical device itself.
5. Cost & Effort Estimates: All cost and effort estimates (e.g., "Medium Effort") are relative indicators based on typical industry averages for similar device categories. They do not represent a commercial quote or guaranteed timeline. Actual implementation costs vary significantly based on existing architecture and technical debt.

Appendix A: Technical Design Declaration

The following technical parameters were formally declared and serve as the frozen basis for this gap analysis.

Declaration Date: 13 Jan 2026

Document Reference: sample-gridforge

1. Declared Specifications

Product Context

Report Name (Computed) `[q_name]`

```
GridForge Industrial Edge Gateway
```

Product Name / Reference (Optional) `[q_device_name]`

Why we ask: Correctly identifying your product in the final PDF report allows for easy sharing with stakeholders and regulators.

```
GridForge Industrial Edge Gateway
```

Where will this product be sold or deployed? `[q_market]`

Impact: Different regions have radically different rules coming into force from 2026-2028. Currently, this audit fully supports only EU, UK, and USA markets (other regions are in progress).

◉ **European Union (EU)**

○ United Kingdom (UK)

◉ **United States (USA)**

What is your primary industry sector? `[q_industry]`

Impact: Your sector determines which standards become mandatory (e.g., IEC 62443 for industrial, MDR for medical) and the severity of non-compliance fines.

○ Consumer Electronics / Wearables

○ Medical / Healthcare

● **Industrial / OT / ICS / Critical Infrastructure**

○ Automotive / Transportation

○ Smart City / Public Infrastructure

○ Telecom / Networking

○ Finance / POS / Payment

○ Maritime / Shipping / Offshore

○ Agriculture / AgTech / Farming

○ Defense / Military

○ Energy / Utilities / Smart Grid

○ Aerospace / Aviation

○ Other

Is this an EV charging station/EVSE? `[q_ev_charger]`

(Skipped)

○ Yes - AC/DC charger or EVSE

○ No

What is the primary role of the product? `[q_device_role]`

Impact: Distinguishes monitoring devices from those with physical safety implications, affecting IEC 62443, UN R155, MDR, and safety risk weighting.

(Skipped)

○ Monitoring and alerting only (no direct control)

○ Supportive/assistive (e.g., recommendations, remote disable)

○ Direct actuation/safety-critical control (e.g., braking, treatment delivery)

Planned commercial support lifespan of the product (years)? `[q_lifespan]`

Impact: Regulations require you to provide security updates for the entire expected lifespan of the product. If hardware capabilities (e.g., flash/RAM) can't support updates for 10 years, the product becomes illegal to sell.

`11`

Expected total lifetime deployed units? `[q_fleet_size]`

Impact: Large fleets are attractive targets for nation-state actors and botnets. The CRA imposes stricter reporting obligations on 'Critical' products, often defined by their deployment scale and impact.

○ Micro / Pilot (< 5k units)

○ Small Scale (5k - 50k)

● **Medium Scale (50k - 500k)**

○ Large Scale (500k - 5M)

○ Mass Market (> 5M)

Privacy & Data Handling

Does the product or cloud process personal data (IP, location, biometrics, usage)? [q_personal_data]

Impact: Processing personal data triggers GDPR (EU) and CCPA (US) obligations, including the 'Right to Erasure' and 72-hour breach notification windows, with fines up to 4% of global turnover.

◉ **No**

○ Yes, but anonymised/pseudonymised

○ Yes, identifiable PII or special-category

What is the primary target user demographic? [q_target_users]

Impact: Devices for children face extremely strict privacy limits (US COPPA, UK Children's Code, EU GDPR-K) and safety rules (EU Toy Safety Reg). Data collection must be minimized.

(Skipped)

○ General Audience (Adults)

○ Children (Under 13 or 16)

○ Mixed Audience (Likely accessed by children)

○ Professional / Industrial / Business Use

Sector-Specific Details

(Optional) Working toward UN R155 / ISO 21434 certification or CSMS? [q_automotive_unr155]

Why we ask: These regulations mandate a certified Cybersecurity Management System (CSMS) for the manufacturer. Without it, you cannot type-approve new vehicles in 60+ countries.

(Skipped)

○ Yes

○ In progress

○ No

○ Don't know these numbers

What vehicle interface access is implemented? [q_vehicle_interface]

Impact: Direct bus access increases attack surface and UN R155 scrutiny.

(Skipped)

○ OBD-II read-only diagnostics

○ Direct CAN bus access

○ Write/commands (e.g., remote disable)

○ None / wireless only

Is this product used in critical infrastructure (power grids, oil/gas, water, railways, factories)? [q_industrial_critical]

Impact: Critical infrastructure operators fall under NIS2 and CRA 'Critical Product' categories, facing the highest fines (up to €10M or 2% turnover) and mandatory 24-hour incident reporting.

○ Yes

◉ **No - general industrial/commercial**

(Optional) Targeting any additional sector-specific cybersecurity standard (e.g., IMO for maritime, FAA for drones, ISO 15118 for EV charging)? `[q_niche_regulations]`

Captures niche regulatory requirements not covered by main industry categories.

(Skipped)

○ Yes

○ No

Hardware & Software Platform

Exact SoC / MCU (Optional) `[q_exact_soc]`

Why we ask: Accurate risk analysis depends on hardware capabilities. Start typing to see suggestions (e.g., 'STM32', 'ESP32'). Identifying the chip allows us to check for known hardware vulnerabilities/errata.

```
NXP i.MX8M Plus
```

Operating System / RTOS Environment? `[q_os]`

Impact: High-level OSs (Linux/Android) have immense attack surfaces and SBOM complexity. The CRA distinguishes between 'General Purpose' and 'embedded' systems for update requirements.

○ Zephyr RTOS

○ FreeRTOS

● **Linux (Yocto/Buildroot/OpenWrt)**

○ Linux (Debian/Ubuntu/Raspbian)

○ Android (AOSP)

○ Bare Metal / No OS

○ Azure RTOS (ThreadX)

○ Other / Custom

Connectivity methods (select all that apply) `[q_connectivity]`

Impact: Every network interface is an attack vector. Unnecessary open ports on these interfaces are the #1 cause of IoT compromises.

● **Wi-Fi**

● **Bluetooth/BLE**

○ Thread / Zigbee / Matter

● **Ethernet**

● **Cellular (4G/5G/Cat-M/NB-IoT)**

○ LoRa / LoRaWAN

○ Air-gapped / no external connectivity

Does the solution include a companion mobile app or web dashboard? `[q_companion_app]`

Impact: Mobile apps and dashboards trigger additional regulations (EU Digital Services Act, ePrivacy Directive for cookies/tracking) and are common entry points for attacks.

(Skipped)

○ Yes

○ No (Device only / API only)

Is protecting firmware/algorithms from theft or cloning a core requirement? `[q_ipr_goal]`

Why we ask: If your business value is in the firmware algorithms, you need hardware-backed readout protection. Standard microcontroller 'readout protection' (aka RDP Level 1) is often trivially bypassable.

◉ **Critical - our IP is the main value**

○ Important but not critical

○ No - value is in cloud/service

Primary Power Source? `[q_power_source]`

Impact: The new EU Battery Regulation mandates a 'Battery Passport' for batteries > 2kWh, requiring digital history tracking and carbon footprint reporting.

◉ **Mains / Line Power**

○ Rechargeable Battery (> 2kWh) / EV

○ Consumer Battery / Coin Cell

○ Energy Harvesting

AI/ML Integration

Does your product use AI/ML for decision making? `[q_ai_usage]`

Impact: Using AI/ML triggers the EU AI Act. Most embedded AI is 'minimal risk,' but safety components or biometric ID systems are 'High Risk' with massive compliance burdens.

◉ **Yes**

○ No

Does the AI directly influence safety-critical or diagnostic decisions? `[q_ai_influence]`

Impact: Determines EU AI Act classification and robustness requirements.

◉ **No - insights/alerts only (minimal-risk)**

○ Supportive/recommendations (potential high-risk)

○ Direct/autonomous influence (high-risk)

What does the AI system do? (select all that apply) `[q_ai_application]`

Impact: The EU AI Act classifies AI by application. HR/education/credit scoring are HIGH-RISK (Annex III). Chatbots and content generation require transparency. Safety-critical autonomous control triggers Annex I.

(Skipped)

○ Classifies/categorizes data or images

○ Predicts outcomes or behaviors

○ Detects objects, anomalies, or patterns

○ Makes recommendations to users

○ Autonomous control/actuation decisions

○ Generates text, images, audio, or video

○ Conversational AI / Chatbot interface

○ HR/recruitment screening or decisions

○ Educational assessment or grading

○ Credit, insurance, or financial scoring

○ Biometric identification of individuals

AI model sourcing: Open-source/third-party? `[q_ai_sourcing]`

Impact: The EU AI Act places responsibility on the integrator. Using 'black box' third-party models without understanding their training data creates unmanageable liability.

○ Open Source

○ Third Party

◉ **Proprietary / In-house**

Model poisoning defenses: Input validation/sanitization? `[q_ai_poisoning]`

Why we ask: AI models can be tricked by malicious inputs ('adversarial examples'). High-risk AI systems must demonstrate 'robustness' against such attacks under the AI Act.

◉ **Yes**

○ Partial

○ No

Over-the-air AI updates segregated? `[q_ai_ota]`

Why we ask: Updating the AI model independently of the firmware allows for rapid patching of model drift or bias without risking the device's core stability.

○ Yes

◉ **No**

Federated learning for privacy? `[q_ai_federated]`

Impact: Federated learning keeps data on-device, significantly reducing GDPR exposure. It is a 'Privacy Enhancing Technology' (PET) highly favored by regulators.

○ Yes

◉ **No**

Edge AI anomaly detection enabled? `[q_ai_edge]`

Why we ask: On-device anomaly detection can catch 'zero-day' attacks or insider threats that deviate from normal operational patterns, a requirement for critical infrastructure (NIS2).

◉ **Yes**

○ No

Does the AI system logging meet EU AI Act traceability reqs? `[q_ai_logging]`

Why we ask: High-risk AI systems must automatically log events (Article 12) to enable post-market monitoring.

◉ **Yes (Automatic recording of events)**

○ No

Is human oversight built into the AI system design? `[q_ai_human_oversight]`

Why we ask: Article 14 mandates that high-risk AI tools can be overseen by natural persons to prevent or minimize risks.

◉ **Yes**

○ No

Is accuracy, robustness, and cybersecurity tested/declared? `[q_ai_accuracy]`

Why we ask: Article 15 requires high-risk AI to achieve appropriate levels of accuracy, robustness, and cybersecurity.

◉ **Yes**

○ No

Are instructions and interpretability measures in place? `[q_ai_transparency]`

Why we ask: Article 13 requires operation sufficiently transparent to enable users to interpret the system's output.

○ Yes

◉ **No**

Is technical documentation and record-keeping maintained? `[q_ai_record_keeping]`

Why we ask: Article 11 requires extensive technical documentation for conformity assessment.

◉ **Yes**

○ No

Product Security

Does the product ship with a default admin password? `[q_default_creds]`

Impact: Static passwords (e.g., 'admin/admin') are illegal in the UK (PSTI) and banned by the EU RED Delegated Act. This is the single fastest way to get your product banned from sale.

◉ **No, each unit has a unique random password**

○ Yes, but user is forced to change it on first setup

○ Yes, same password for all devices (e.g., 'admin')

○ No password / Unauthenticated

Is disk/flash encryption enabled for data-at-rest? `[q_data_at_rest_encryption]`

Impact: Mandatory for GDPR (protecting PII) and medical devices (patient data). Unencrypted flash allows attackers to desolder the chip and read all secrets in minutes.

◉ **Yes, full disk/partition encryption**

○ No

Typical physical deployment environment? `[q_physical_security]`

Why we ask: 'Physical access is total access.' If an attacker can touch the product (e.g., a smart doorbell), they can attempt side-channel power analysis or glitching attacks to extract keys.

○ Physically secure (locked cabinet)

◉ **Semi-secure (office, factory)**

○ Public or consumer home

Do you implement Secure Boot? `[q_secure_boot]`

Impact: Secure Boot ensures only YOUR signed software runs on the product. Without it, malware can persist even after a factory reset. A mandatory requirement for CRA and PSTI.

◉ **Yes**

○ Partial / vendor default

○ No

How complete is your Secure Boot chain? [q_secure_boot_depth]

Why we ask: A 'chain of trust' is only as strong as its weakest link. Securing the bootloader but not the kernel (or filesystem) leaves the system wide open to modification.

◉ **Full chain (kernel + rootfs, dm-verity/A/B)**

○ Bootloader only

○ Vendor default only

Hardware root of trust present? [q_hw_rot]

Impact: A Hardware Root of Trust (like a Secure Element or TPM) provides a safe vault for keys that even the main processor cannot read. It is the gold standard for device identity.

○ Discrete Secure Element / TPM

◉ **Integrated TEE/TrustZone/TPM**

○ SoC built-in only

○ None

How are cryptographic keys / product identity stored? [q_key_storage]

Impact: Using a shared key across all devices means one reverse-engineered device compromises your entire fleet of millions. Unique per-device keys are essential.

◉ **Hardware-backed (SE/TEE/TPM)**

○ Software but encrypted

○ Software plaintext/obfuscated

○ Shared secret (all devices same key)

○ No unique identity

Secure initial provisioning / zero-touch enrollment method? [q_provisioning]

Why we ask: Manual provisioning (typing codes, burning keys in factories) is error-prone and insecure. PKI-based 'Zero Touch' automated provisioning is the only scalable, secure way for commercial IoT.

◉ **PKI / Device Provisioning Service**

○ Manufacturer-signed device certificate

○ Manual token / activation code

○ None / open enrollment

Certificate/key revocation mechanism? [q_revocation]

Impact: If a device key is stolen, you must be able to 'revoke' it so the attacker cannot impersonate the device. The CRA explicitly mandates a working revocation process.

◉ **CRL/OCSP or automated revocation**

○ Manual (e.g., push notifications)

○ None

Firmware IPR protection method? [q_ipr_protection]

Why we ask: Standard MCU locking mechanisms are easily bypassed by cheap glitching attacks. For high-value IP, you need robust encryption or distinct secure hardware.

◉ **Hardware encrypted flash**

○ Signed only

○ Software obfuscation only

○ No protection

Post-quantum cryptography readiness: Integrated NIST-approved algorithms? [q_pqc_readiness]

Impact: Quantum computers (expected ~2030) will break current RSA/ECC crypto. If your device will be in the field then, you must plan for 'Post-Quantum Cryptography' (PQC) transitions now.

◉ **Yes**

○ Planning by 2029

○ No

Network & Access

Which local services are exposed for configuration/maintenance? [q_local_services]

Impact: Legacy protocols like Telnet and FTP send passwords in cleartext. Their presence is an automatic 'fail' for almost every modern security standard (ETSI 303 645, NIST 8259).

◉ **SSH**

◉ **Web Interface (HTTP/HTTPS)**

○ Legacy (Telnet / FTP / TFTP)

○ Android Debug Bridge (ADB)

○ UART / Serial Console only

○ None / Sealed

How is the Local Web Interface secured? [q_web_security]

Impact: HTTP is insecure. Anyone on the same Wi-Fi network can sniff admin credentials. Modern browsers and regulations demand HTTPS even for local interfaces.

◉ **HTTPS (Public/Private CA Signed)**

○ HTTPS (Self-Signed)

○ HTTP (Plaintext)

Product-to-cloud authentication method? [q_cloud_auth]

Impact: Weak cloud authentication allows attackers to control your products remotely. Static API keys are easily extracted from firmware dumps; mTLS is the industry standard.

◉ **mTLS with per-device certs**

○ mTLS but shared cert/PSK

○ Rotating JWT / token

○ Vendor proprietary (e.g., AWS/Azure keys)

○ Static API key / shared secret

○ None / open

All cloud communication encrypted with TLS 1.3 + pinning? [q_encryption_transit]

Impact: Unencrypted traffic allows valid credentials to be stolen. 'Certificate Pinning' prevents Man-in-the-Middle attacks by trusting only your specific server certificate.

◉ **Yes + certificate pinning**

○ Yes, standard TLS

○ Partial

○ No

Product network segmentation? [q_network_segmentation]

Why we ask: A 'flat' network means if one product is hacked, the attacker can talk to everything else. Segmentation isolates critical functions from potential breaches.

○ Fully isolated / zero-trust

◉ **Restricted VLAN / firewall**

○ Flat network

Security Process

Threat modeling performed? [q_threat_modeling]

Impact: You cannot secure what you don't understand. Regulations like ISO 21434 and the CRA require formal Threat Modeling (e.g., STRIDE) to prove you designed security in, not just bolted it on.

◉ **Yes, documented and reviewed annually**

○ Initial (design phase only)

○ None

Automated vulnerability scanning process? [q_vuln_scanning]

Impact: New vulnerabilities are discovered daily. The CRA mandates a process to 'continuously monitoring' your product's software stack for known CVEs.

◉ **Continuous (Integrated into CI/CD pipeline)**

○ Periodic (quarterly scans)

○ None

SBOM & vulnerability disclosure policy? [q_sbom_vdp]

Impact: You must be able to tell customers EXACTLY what software is inside your product (Software Bill of Materials). The CRA imposes fines for failing to handle vulnerability reports from researchers.

○ Full SBOM published + public vuln disclosure / PSIRT

◉ **Internal SBOM only**

○ Basic security.txt or contact

○ None

Third-party / open-source component management? [q_third_party_mgmt]

Why we ask: Modern firmware is 80-90% open source. Without automated tracking (SCA), you are unknowingly shipping vulnerabilities that others have already fixed.

◉ **Automated SCA in CI/CD + auto-updates**

○ SCA tool but manual

○ Manual review only

○ No process

FOSS license scanning automated? [q_foss_scanning]

Why we ask: Accidental inclusion of GPLv3 code ('copyleft') can legally force you to open-source your entire proprietary codebase. Automating this check prevents legal disasters.

○ Yes, automated

◉ **No**

Advanced security validation performed? `[q_security_testing]`

Why we ask: Automated scanners miss logic bugs. Fuzzing (throwing random data at inputs) and Penetration Testing are the only way to find deeper flaws. Required for higher assurance levels.

○ Continuous (fuzzing / DAST in CI/CD)

◉ **Periodic (e.g., annual pen-tests / third-party audits)**

○ None

How are firmware signing keys protected? `[q_code_signing_hsm]`

Impact: Your code signing keys are the 'Crown Jewels.' If stolen, attackers can sign their malware as your legitimate update. An HSM keeps these keys offline and secure.

○ Hardware Security Module (HSM)

◉ **Cloud-based HSM (AWS KMS, Azure Key Vault)**

○ Software keystore / encrypted file

○ No dedicated protection

Maintenance & Lifecycle

How will you deliver security updates? `[q_updates]`

Impact: Remote update capability is the #1 mandatory requirement for all new IoT laws (CRA, PSTI, RED). Without signed OTA, you cannot fix bugs, rendering the product illegal to sell once a vulnerability is found.

◉ **Signed & encrypted OTA (A/B or rollback)**

○ Signed OTA only

○ Unsigned OTA

○ Manual (USB, technician)

○ No updates

Minimum guaranteed security update period (years)? `[q_update_commitment]`

Impact: You must publicly state how long you will provide security updates (e.g., 'Software updates guaranteed until 2030'). The EU CRA requires this period to match the 'expected product lifetime' (often 5+ years).

`10`

Containerization & Runtime Security? `[q_container_usage]`

Impact: Containers allow rapid fluid updates but introduce massive attack surfaces. Running 'privileged' containers or unsigned images allows attackers to break out to the host OS. Examples: Docker/K8s/LXC (Runtime), Notary/Cosign (Signing), gVisor/Kata (Isolation).

(Skipped)

○ Yes, we use Containers

○ Images are signed & verified

○ Rootless / Privileged mode disabled

○ Runtime Isolation

○ No containers used

Does the product log security events locally? `[q_audit_logging]`

Why we ask: If an attack happens, logs are the 'black box' flight recorder. Without them, you cannot perform the forensics analysis mandated by the CRA and GDPR.

◉ **Yes (failed logins, config changes, firmware updates)**

○ Basic (only critical events)

○ No local logging

Post-market security monitoring / telemetry? `[q_telemetry]`

Impact: You cannot fix what you cannot see. Post-market monitoring is a legal requirement to detect active exploitation in the field (CRA Article 11, FDA).

◉ **Advanced (anomaly detection, fleet visibility)**

○ Basic heartbeat / status

○ None

Documented incident response and breach notification plan? `[q_incident_response]`

Impact: When a breach occurs, the clock starts ticking. The EU CRA requires notification within 24 hours. A pre-tested plan is the difference between a manageable incident and a PR disaster.

◉ **Yes, documented and tested annually**

○ Basic plan exists

○ No

End-of-Life (EOL) & Data Destruction Policy? `[q_lifecycle_eol]`

Why we ask: Making it easy for users to securely wipe data (Factory Reset) prevents privacy leaks when devices are resold or recycled. Verification of this is required by GDPR.

◉ **Secure EOL (keys revoked + crypto zeroization)**

○ Graceful (warning in app + factory reset)

○ No plan / nothing

Timeline & Organizational Scope

Target Market Launch Year? `[q_launch_year]`

Impact: Regulations like the EU CRA apply differently to 'New' products vs. 'Legacy' stock. Launching after 2027 forces full compliance immediately.

○ 2026

◉ **2027**

○ 2028+

○ Already on market (Legacy Fleet)

Organization Size Category `[q_org_size]`

This helps determine regulatory exemptions and obligations: - SME: Qualifies for CRA/AI Act SME exemptions (reduced fines, extended deadlines). Typically <250 employees or <€50M turnover. - Large: May trigger additional obligations under NIS2, CSRD (sustainability reporting for €450M+ turnover), and CSDDD (supply chain due diligence for €1.5B+ turnover). - Other: Use if unsure or prefer not to disclose. No exemptions will be applied.

◉ **SME (Small/Medium Enterprise)**

○ Large Enterprise

○ Other / Prefer not to say

Cyber Insurance Status `[q_cyber_insurance]`

Insurers increasingly mandate technical controls like SBOMs and MFA. This check helps align your architecture with those standard requirements. Select 'I don't know' if you are unsure about your organization's insurance status.

◉ **Yes, policy is active**

○ No coverage

○ I don't know

Additional Parameters

Parameters added by SoC or derived context.

Main processor class? `[q_class]`

`Mid-range (Cortex-A53/A55, RTOS+net)`

Primary SoC / MCU family? `[q_soc_vendor]`

`NXP`

2. Raw Token Data

The following raw identifiers were used for automated rule processing:

q_ai_accuracy: `yes`

q_ai_edge: `yes`

q_ai_federated: `no`

q_ai_human_oversight: `yes`

q_ai_influence: `no`

q_ai_logging: `yes`

q_ai_ota: `no`

q_ai_poisoning: `yes`

q_ai_record_keeping: `yes`

q_ai_sourcing: `proprietary`

q_ai_transparency: `no`

q_ai_usage: `yes`

q_audit_logging: `yes`

q_class: `mid`

q_cloud_auth: `mtls`

q_code_signing_hsm: `cloud_hsm`

q_connectivity: `wifi, ble, ethernet, cellular`

q_cyber_insurance: `yes`

q_data_at_rest_encryption: `yes`

q_default_creds: `unique`

q_device_name: `GridForge Industrial Edge Gateway`

q_encryption_transit: `yes_pinned`

q_exact_soc: `NXP i.MX8M Plus`

q_fleet_size: `medium`

q_foss_scanning: `no`

q_hw_rot: `integrated_tee`

q_incident_response: `yes_tested`

q_industrial_critical: `no`

q_industry: `industrial`

q_ipr_goal: `critical`

q_ipr_protection: `hw_encrypt`

q_key_storage: `hardware`

q_launch_year: `2027`

q_lifecycle_eol: `secure_eol`

q_lifespan: `11`

q_local_services: `ssh, web_ui`

q_market: `eu, usa`

q_name: `GridForge Industrial Edge Gateway`

q_network_segmentation: `restricted`

q_org_size: `sme`

q_os: `linux_yocto`

q_personal_data: `no`

q_physical_security: `semi`

q_power_source: `mains`

q_pqc_readiness: `yes`

q_provisioning: `pki_dps`

q_revocation: `crl_ocsp`

q_sbom_vdp: `internal`

q_secure_boot: `yes`

q_secure_boot_depth: `full`

q_security_testing: `periodic`

q_soc_vendor: `nxp`

q_telemetry: `advanced`

q_third_party_mgmt: `sca_cicd`

q_threat_modeling: `yes_documented`

q_update_commitment: `10`

q_updates: `ota_signed_enc`

q_vuln_scanning: `continuous`

q_web_security: `https_signed`

Appendix B: Risk Traceability Matrix

This matrix enables verification of why specific risks were triggered based on your device configuration.

EU AI Act: High-Risk Non-Compliance (risk-ai-high-risk-noncomp)

Severity: 🔴 Blocker

Triggering Inputs:

- `q_ai_usage`: yes
- `q_industry`: industrial
- `q_device_role`: N/A

Checked Exclusions (Risk NOT suppressed because):

- Tag `ai_act_compliant`: Not Present
  - *Requires:* Device meets EU AI Act High-Risk requirements (Articles 9-15)
  - *Source inputs:*
    - `q_ai_logging`: expected equals 'yes', got 'yes'
    - `q_ai_human_oversight`: expected equals 'yes', got 'yes'
    - `q_ai_accuracy`: expected equals 'yes', got 'yes'
    - `q_ai_transparency`: expected equals 'yes', got 'no'
    - `q_ai_record_keeping`: expected equals 'yes', got 'yes'
- Tag `role_monitoring`: Not Present
  - *Requires:* Device role is monitoring/alerting only
  - *Source inputs:*
    - `q_device_role`: expected equals 'monitoring_alerting', got (not answered)
- Tag `ai_influence_advisory`: Not Present
  - *Requires:* AI provides advisory/supportive output only
  - *Source inputs:*
    - `q_ai_influence`: expected in ['advisory', 'supportive', 'minimal'], got 'no'

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

AI Governance Maturity Gap (risk-ai-governance-gap)

Severity: 🟠 High

Triggering Inputs:

- `q_ai_usage`: yes
- `q_industry`: industrial
- `q_device_role`: N/A

Checked Exclusions (Risk NOT suppressed because):

- Tag `iso_42001_certified`: Not Present
  - *Requires:* Condition not met
- Tag `ai_governance_mature`: Not Present
  - *Requires:* Condition not met

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

E-Waste Supply Chain Risk (risk-supply-chain-e-waste)

Severity: 🟡 Medium

Triggering Inputs:

- `q_update_commitment`: 10
- `q_lifespan`: 11

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

EU AI Act: Missing Transparency Disclosures (risk-ai-transparency-gap)

Severity: 🟡 Medium

Triggering Inputs:

- `q_ai_usage`: yes

Checked Exclusions (Risk NOT suppressed because):

- Tag `ai_transparency_opt_in`: Not Present
  - *Requires:* Condition not met
- Tag `ai_disclaimer_present`: Not Present
  - *Requires:* Condition not met

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

Supply Chain: Silicon EOL Mismatch (risk-bus-silicon-eol)

Severity: 🟡 Medium

Triggering Inputs:

- `q_update_commitment`: 10
- `q_lifespan`: 11

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

Unmanaged Supply Chain (risk-supply-chain-unmanaged)

Severity: 🟡 Medium

Triggering Inputs:

- `q_foss_scanning`: no

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

Build Pipeline Injection (risk-comp-build-pipeline)

Severity: 🟢 Low

Triggering Inputs:

- `q_foss_scanning`: no

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

E-Waste Liability (risk-theme-ewaste)

Severity: 🟢 Low

Triggering Inputs:

- `q_update_commitment`: 10
- `q_lifespan`: 11

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

AI Model Theft or Poisoning (risk-comp-ai-model)

Severity: 🟢 Low

Triggering Inputs:

- `q_ai_usage`: yes

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

No Automated Vulnerability Scanning (risk-dev-no-vuln-scanning)

Severity: 🟢 Low

Triggering Inputs:

- `q_foss_scanning`: no

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

Critical IPR Theft Risk (risk-bus-cloning-ipr)

Severity: 🟢 Low

Triggering Inputs:

- `q_ipr_goal`: critical

Validation (For Customer Use Only):

☐ **Confidence Level:** High / Medium / Low

Notes/Comments:

Appendix C: Standards Alignment Analysis

This appendix provides an informational analysis of how this device's security posture aligns with recognized industry standards. This is supplementary information to assist with compliance planning and is not a formal conformity assessment.

21	0	4
Regulations Analyzed	Strong Alignment	Partial Alignment

⚠️ EU Cyber Resilience Act (CRA)

Jurisdiction: EU | **Status:** Conformity not demonstrated for EU Cyber Resilience Act (CRA)

Article	Standard	Coverage	Presumption
Annex I (Essential Requirements)	**std-etsi-303-645**	90%	❌ Not Granted
Annex I (Essential Requirements)	**std-iec-62443**	100%	❌ Not Granted
Annex I (Essential Requirements)	**std-nist-csf-2**	88%	❌ Not Granted

⚠️ **std-etsi-303-645 - Unaddressed Controls:** 5.13-1, 5.15-1

⚠️ **std-nist-csf-2 - Unaddressed Controls:** GV.SC-01, ID.AM-01

⚠️ NIS2 Directive (Network and Information Systems Directive 2)

Jurisdiction: EU | **Status:** Conformity not demonstrated for NIS2 Directive (Network and Information Systems Directive 2)

Article	Standard	Coverage	Presumption
Article 21 (Cybersecurity risk-management measures)	**std-iso-27001**	95%	❌ Not Granted
Article 21 (Cybersecurity risk-management measures)	**std-iec-62443**	100%	❌ Not Granted

⚠️ **std-iso-27001 - Unaddressed Controls:** A.5.19

⚠️ EU AI Act (Regulation (EU) 2024/1689)

Jurisdiction: EU | **Status:** Conformity not demonstrated for EU AI Act (Regulation (EU) 2024/1689)

Article	Standard	Coverage	Presumption
Chapter III, Section 2 (High-Risk AI Requirements)	**std-iso-42001**	44%	❌ Not Granted
Article 9 (Risk Management)	**std-nist-csf-2**	88%	❌ Not Granted

⚠️ **std-iso-42001 - Unaddressed Controls:** 5.1-01, 6.1.3-01, 6.1.4-01, 8.4-01, 10.1-01

⚠️ **std-nist-csf-2 - Unaddressed Controls:** GV.SC-01, ID.AM-01

⚠️ US FCC Cyber Trust Mark (Voluntary IoT Labeling)

Jurisdiction: US | **Status:** Partial conformity: 1/2 articles with presumption

Article	Standard	Coverage	Presumption
Labeling Criteria	**std-nist-ir-8259**	100%	✅ Granted
Labeling Criteria	**std-nist-csf-2**	88%	❌ Not Granted

⚠️ **std-nist-csf-2 - Unaddressed Controls:** GV.SC-01, ID.AM-01

Appendix D: Audit Support & Services

Methodology

Unlike generic AI scanners, this assessment was performed by the Device Prophet Expert System - a deterministic logic engine. It uses strict rule-mapping to correlate your specific architectural inputs against 30+ regulatory frameworks (EU RED, CRA, AI Act, UK PSTI, etc.) without "hallucinating" requirements.

Verification & Support

While our algorithms are rigorous, architectural context matters. If you have questions regarding the report findings, need technical verification, or wish to dispute a "False Positive" due to a specific compensating control in your design, please contact our engineering team directly:

- **Email:** info@deviceprophet.com
- **Web:** deviceprophet.com/contact

Beyond the Report

Identifying the gaps is only the first step. For teams requiring implementation support, deep-dive architectural reviews, or formal certification management, our engineering team is available to assist.

Explore our specialized services at: deviceprophet.com/solutions