SUMATOSOFT

IoT Compliance & Audit-Readiness Checklist (Score 0–18)

This checklist defines the transition from "compliance as a policy" to "compliance as an engineered system." Use it to evaluate your current architecture or to vet technical partners.

Section 1: Identity and access governance

Goal: To eliminate unauthorized access and ensure non-repudiation.

- ☐ Unique device identity: Are you using per-device hardware-backed credentials (X.509 certificates) rather than shared API keys?
- ☐ Service-to-Service scoping: Are internal cloud calls restricted by short-lived tokens and scoped service accounts?
- ☐ Granular RBAC/ABAC: Is human access to regulated data (ePHI/PII) governed by Role-Based or Attribute-Based controls?

Total: _ /3

Section 2: Data protection and key sovereignty

Goal: To secure data at rest and in transit while maintaining operational continuity.

- ☐ End-to-end encryption: Is TLS 1.3 enforced for all "Northbound" (Gateway to Cloud) and "Southbound" (Cloud to Device) traffic?
- ☐ Managed key isolation: Are data encryption keys (DEKs) cryptographically separated from application secrets?
- ☐ Non-disruptive rotation: Does your Key Management System (KMS) support automated rotation without bricking field-deployed devices?

Total: _ /3

Section 3: Logging and forensic traceability

Goal: To prove "who did what and when" across a distributed stack.

- ☐ Tamper-resistant audit trails: Are logs for privileged actions and data exports streamed to an immutable, centralized repository?
- ☐ Automated retention enforcement: Is data expiry handled by technical lifecycle rules (e.g., S3 Lifecycle/TTL) rather than manual scripts?
- ☐ Cross-layer traceability: Can you trace a single data point from the physical sensor through the gateway to the final API export?

Total: _ /3

Section 4: Resilient lifecycle management (OTA)

Goal: To maintain compliance over a 5-10 year device lifespan.

- ☐ Cryptographic firmware integrity: Is the device bootloader configured to only accept firmware signed by your private PKI?
- ☐ Risk-mitigated rollouts: Does your OTA pipeline support "Canary" deployments and automated rollback upon failure?
- ☐ Security-first patching: Can you push critical security patches independently of feature updates to minimize downtime?

Total: _ /3

Section 5: Network and perimeter defense

Goal: To minimize the blast radius of a compromised node.

- ☐ Zero-trust segmentation: Are OT (Operational Tech) and IT networks separated by explicit conduits?
- ☐ Minimal surface area: Are all unnecessary device ports closed, and is "inbound" listener traffic prohibited?
- ☐ Brokered remote access: Is third-party maintenance performed via a secure, logged bastion/VPN rather than open SSH?

Total: _ /3

Section 6: Incident response and liability management

Goal: To limit legal and operational exposure during a breach.

- ☐ IoT-specific runbooks: Do you have incident response plans that cover hardware-level compromises (e.g., physical tampering)?
- ☐ Fleet-wide containment: Can you instantly revoke the credentials of a single compromised device or a specific batch?
- ☐ Continuous monitoring: Are alerts configured for anomalous data traffic patterns or unauthorized configuration changes?

Total: _ /3

Is your project audit-ready? Count the total number of checked boxes.

If you checked fewer than 15 boxes, your IoT system may have significant regulatory exposure. SumatoSoft specializes in engineering compliant-by-design IoT ecosystems that survive the scrutiny of global enterprise security teams.

Request a compliance architecture review

SUMATOSOFT

Thank you for your time!

Any questions? Drop us a line!

Headquarters

One Boston Place, Suite 2602
Boston, MA 02108, United States

Other ways to get in touch

info@sumatosoft.com
sumatosoft.com