Enterprise InfoSec Policy Compliance Gap Analysis

IT Systems vs OT/IoT Endpoints: The Hidden Compliance Crisis

WHY THIS MATTERS: 82% of enterprises cannot identify all IoT/OT devices on their network, making compliance impossible. Traditional IT security policies were designed for managed endpoints (laptops, servers) with 2-5 year lifecycles. IoT/OT devices have 10-20 year lifecycles, proprietary firmware, and often cannot be patched without vendor support—yet they must meet the same compliance standards. This gap causes audit failures, blocked deals ($2-5M), and regulatory penalties ($10M+).

24/32
Controls Applicable to IoT/OT

17/24
High/Critical Compliance Gaps

75%
Of Controls Create Audit Risk

Fully Applicable | Partially Applicable | Not Applicable | ● Critical Gap | ● High Gap | ● Medium Gap

#	InfoSec Policy Control	IT Systems	IoT/OT	IoT/OT Reality & Compliance Gap	Impact If Not Compliant	Gap Level
1. ASSET MANAGEMENT & INVENTORY						
1.1	Maintain complete asset inventory	YES	YES	**Reality:** 82% cannot identify all IoT devices. Devices auto-connect via WiFi/BLE without IT knowledge. Shadow IoT proliferates. **Gap:** No automated discovery; manual spreadsheets outdated within weeks.	Cannot prove SOC 2/ISO scope; audit failure	CRITICAL
1.2	Track device location & ownership	YES	YES	**Reality:** IoT devices span 50+ locations, no central registry. Cameras/sensors installed by facilities, not IT. **Gap:** Multi-department deployment with no ownership documentation.	Cannot demonstrate control over assets; audit finding	HIGH
1.3	Document device configurations	YES	PARTIAL	**Reality:** IoT configs stored in device firmware, not accessible. Proprietary vendor systems. **Gap:** Cannot extract or document configs without vendor tools.	Cannot prove secure configuration baseline	HIGH
2. ACCESS CONTROL & AUTHENTICATION						
2.1	Enforce strong passwords (12+ chars, complexity)	YES	PARTIAL	**Reality:** 70% of IoT devices ship with default credentials (admin/admin). Many cannot be changed. **Gap:** Hardcoded passwords in firmware; policy violation by design.	Direct violation of SOC 2 CC6.1; audit failure	CRITICAL
2.2	Implement MFA for all access	YES	NO	**Reality:** 95% of IoT devices don't support MFA. Web interfaces use basic auth only. **Gap:** Technically impossible without device replacement.	Compensating controls required; audit scrutiny	HIGH
2.3	Disable inactive accounts (90 days)	YES	PARTIAL	**Reality:** IoT devices don't integrate with AD/SSO. No account lifecycle management. **Gap:** Local accounts persist indefinitely; no deprovisioning.	Orphaned accounts = unauthorized access risk	HIGH
2.4	Implement RBAC (Role-Based Access)	YES	NO	**Reality:** Most IoT devices have 2 roles: admin or none. No granular permissions. **Gap:** Everyone has admin or no access; violates least privilege.	Excessive permissions = insider threat exposure	MEDIUM
3. VULNERABILITY & PATCH MANAGEMENT						
3.1	Patch critical vulnerabilities within 30 days	YES	PARTIAL	**Reality:** IoT vendors release patches quarterly (if at all). 40% of devices running firmware 2+ years old. **Gap:** Cannot meet 30-day SLA; dependent on vendor.	Known vulnerabilities exploitable; failed audit control	CRITICAL
3.2	Perform monthly vulnerability scans	YES	PARTIAL	**Reality:** Network scans crash IoT devices. Many behind NAT or isolated networks. **Gap:** Traditional scanners (Nessus, Qualys) incompatible with OT.	Unknown vulnerabilities; cannot prove continuous monitoring	HIGH
3.3	Maintain patch compliance >95%	YES	NO	**Reality:** Industry average: 60% of IoT devices fully patched. Maintenance windows disrupt operations. **Gap:** Cannot achieve 95% without taking production offline.	Policy violation; auditor issues finding	CRITICAL
4. NETWORK SECURITY & SEGMENTATION						
4.1	Segment networks by data sensitivity	YES	YES	**Reality:** 85% of IoT devices on flat corporate network. No micro-segmentation. **Gap:** Cameras/sensors access file servers; lateral movement risk.	Failure to contain breaches; violates Zero Trust	CRITICAL
4.2	Enforce firewall rules (deny-by-default)	YES	PARTIAL	**Reality:** IoT devices need 10-20 ports open. Firewall rules become "allow-by-exception." **Gap:** Overly permissive rules negate firewall effectiveness.	Broad attack surface; failed network controls	HIGH
4.3	Encrypt all network traffic (TLS 1.2+)	YES	PARTIAL	**Reality:** 60% of IoT traffic is unencrypted (HTTP, Telnet, FTP). Legacy protocols required. **Gap:** Cannot enforce encryption without breaking functionality.	Data in transit exposed; HIPAA/PCI violation	CRITICAL
4.4	Monitor network traffic for anomalies	YES	PARTIAL	**Reality:** IoT traffic patterns unknown. No baseline = false positives flood SOC. **Gap:** SIEM/IDS lack IoT protocol visibility (MQTT, CoAP, BACnet).	Cannot detect IoT-borne attacks; blind spot	HIGH
5. DATA PROTECTION & ENCRYPTION						
5.1	Encrypt data at rest (AES-256)	YES	NO	**Reality:** 90% of IoT devices store data unencrypted on SD cards or local storage. **Gap:** Physical theft = full data compromise.	PCI-DSS/HIPAA violation; breach notification	CRITICAL
5.2	Classify and label sensitive data	YES	PARTIAL	**Reality:** IoT data streams to cloud/servers with no classification tags. **Gap:** Cannot apply retention/handling policies to IoT data.	Data governance failure; regulatory risk	MEDIUM
5.3	Implement DLP (Data Loss Prevention)	YES	NO	**Reality:** DLP tools can't inspect IoT traffic. Proprietary protocols bypass controls. **Gap:** Data exfiltration via IoT devices undetectable.	Cannot prevent data leakage; audit gap	HIGH
6. LOGGING, MONITORING & INCIDENT RESPONSE						
6.1	Centralize logs (12-month retention)	YES	PARTIAL	**Reality:** 70% of IoT devices don't support syslog. Logs stored locally, overwritten weekly. **Gap:** Cannot meet retention requirements; forensics impossible.	Audit evidence missing; incident investigation fails	CRITICAL
6.2	Log all access attempts (success/failure)	YES	PARTIAL	**Reality:** IoT devices log sporadically or not at all. No authentication logs. **Gap:** Cannot detect unauthorized access or prove non-repudiation.	SOC 2 CC7.2 failure; no audit trail	CRITICAL
6.3	Monitor logs for security events (24/7 SOC)	YES	NO	**Reality:** IoT logs (if any) don't integrate with SIEM. Security team has no visibility. **Gap:** IoT incidents discovered days/weeks later, or never.	Breach detection delayed; increased damage	CRITICAL
6.4	Incident response plan includes all systems	YES	PARTIAL	**Reality:** IR playbooks don't cover IoT. Security team doesn't know how to isolate/remediate. **Gap:** No documented IoT incident procedures.	Slow response; regulatory reporting failure	HIGH
7. CHANGE & CONFIGURATION MANAGEMENT						
7.1	Document all configuration changes	YES	NO	**Reality:** IoT configs changed via vendor portal or on-device. No change tickets. **Gap:** Undocumented changes violate change control policy.	Audit finding; cannot prove configuration integrity	HIGH
7.2	Require change approval workflow	YES	NO	**Reality:** Facilities staff update cameras/sensors without IT approval. **Gap:** No governance over IoT changes.	Unauthorized changes = security drift	MEDIUM
7.3	Maintain configuration baselines	YES	PARTIAL	**Reality:** No tools to extract or compare IoT configs. Each vendor has proprietary format. **Gap:** Cannot detect config drift or unauthorized changes.	Unknown security posture; audit gap	HIGH
8. PHYSICAL SECURITY & DISPOSAL						
8.1	Secure physical access to devices	YES	PARTIAL	**Reality:** Cameras/sensors in public areas. Anyone can unplug, tamper, steal. **Gap:** Physical security controls weak or nonexistent.	Tampering undetected; device theft common	MEDIUM
8.2	Sanitize devices before disposal (NIST 800-88)	YES	NO	**Reality:** Old cameras/sensors tossed in dumpster with data intact. No disposal tracking. **Gap:** Data remnants on discarded devices = breach risk.	GDPR/CCPA violation; data breach notification	HIGH
9. VENDOR & THIRD-PARTY RISK MANAGEMENT						
9.1	Assess vendor security (SOC 2/ISO required)	YES	PARTIAL	**Reality:** IoT vendors (Axis, Genetec, etc.) have certs, but individual devices don't. **Gap:** Vendor security ≠ device security in deployment.	Supply chain risk unaddressed	MEDIUM
9.2	Review vendor access quarterly	YES	NO	**Reality:** Vendors have 24/7 cloud access to devices. No visibility or control. **Gap:** Cannot monitor vendor actions; backdoor access.	Unauthorized vendor access = security incident	HIGH
10. COMPLIANCE REPORTING & AUDIT READINESS						
10.1	Produce compliance reports on-demand	YES	NO	**Reality:** Audit prep takes 4-6 weeks of manual data collection from IoT. **Gap:** No automated reporting; cannot prove continuous compliance.	AUDIT FAILURE: Cannot demonstrate control effectiveness	CRITICAL
10.2	Demonstrate continuous compliance	YES	NO	**Reality:** Point-in-time snapshots only. No continuous monitoring of IoT controls. **Gap:** Cannot prove controls operated throughout audit period.	SOC 2 Type II failure; qualified opinion	CRITICAL

THE BOTTOM LINE: Of 32 standard IT InfoSec controls, 24 apply to IoT/OT devices—but 17 have HIGH or CRITICAL compliance gaps. The result: 82% of enterprises cannot pass an IoT/OT audit, leading to failed audits, blocked deals ($2-5M), and regulatory penalties ($10M+). Traditional IT security tools (EDR, SIEM, vulnerability scanners) were not designed for IoT/OT, creating a massive blind spot that auditors now scrutinize heavily. **Solution:** Purpose-built IoT compliance platforms (like SmartHub.ai) automate discovery, monitoring, and reporting—reducing audit prep from weeks to days and achieving 95%+ compliance rates.

Sources: Forescout Enterprise IoT Risk Report (82% statistic), SOC 2 Trust Services Criteria (AICPA), ISO/IEC 27001:2022 Annex A Controls, NIST Cybersecurity Framework, IEC 62443 (Industrial OT Security)