IoT Security Assessment Checklist

A Comprehensive Guide for Industrial IoT Deployments

About This Checklist

This security assessment tool covers 10 critical domains of IoT security based on industry best practices and real-world deployment experience. Use it to evaluate existing deployments, plan new projects, or conduct vendor assessments. Each item includes priority guidance and implementation notes.

Priority Levels:

- **Critical** - Must be implemented before production deployment
- **High** - Implement within first 90 days of operation
- **Medium** - Plan for implementation within first year

How to Use:

1. Print this checklist or use digitally during security assessments
2. Check the box when each control is verified and documented
3. Record findings, gaps, and remediation plans in the Notes column
4. Review quarterly to ensure controls remain effective as systems evolve

1. Network Segmentation & Isolation

✓	Security Control	Priority	Implementation Notes
☐	IoT devices are isolated in dedicated VLANs separate from corporate networks	**Critical**	*Use VLAN 20+ range for IoT, never mix with VLAN 1 or corporate VLANs*
☐	Inter-VLAN routing rules explicitly deny IoT-to-Corporate traffic by default	**Critical**	*Whitelist only necessary connections with strict firewall rules*
☐	Guest networks are completely segregated from IoT and corporate VLANs	**High**	*Use VLAN 30+ for guest access with internet-only routing*
☐	IoT VLAN traffic is monitored for anomalous lateral movement attempts	**High**	*Deploy IDS/IPS at VLAN boundaries*
☐	Physical ports connecting IoT devices are assigned to correct VLANs via 802.1X or port security	**Medium**	*Disable unused switch ports and prevent VLAN hopping*

2. Device Identity & Access Control

✓	Security Control	Priority	Implementation Notes
☐	All IoT devices have unique, non-default credentials	**Critical**	*Change default admin/admin, root/root immediately*
☐	Network Access Control (NAC) authenticates devices before granting network access	**Critical**	*Use 802.1X, MAC authentication, or certificate-based auth*
☐	Device inventory is maintained with asset IDs, MAC addresses, certificates, and firmware versions	**High**	*Use CMDB or dedicated IoT asset management platform*
☐	Strong password policies are enforced (minimum 12 characters, complexity requirements)	**High**	*Consider certificate-based authentication where possible*
☐	Multi-factor authentication is enabled for device management interfaces	**Medium**	*Especially important for gateway and controller devices*

3. Firmware & Patch Management

✓	Security Control	Priority	Implementation Notes
☐	Regular firmware update schedule is documented and followed	Critical	*Test updates in staging environment before production rollout*
☐	Automated vulnerability scanning identifies outdated firmware versions	High	*Integrate with CVE databases and vendor security advisories*
☐	Firmware updates are cryptographically signed and verified before installation	Critical	*Reject unsigned or unverified firmware packages*
☐	Rollback procedures are tested and documented for failed updates	High	*Maintain previous firmware version for emergency recovery*
☐	End-of-life (EOL) devices are identified and scheduled for replacement	Medium	*No vendor support = no security updates = replace immediately*

4. Network Traffic & Egress Filtering

✓	Security Control	Priority	Implementation Notes
☐	Outbound traffic from IoT devices is restricted to known, approved destinations	Critical	*Whitelist cloud endpoints, block all other egress by default*
☐	IoT devices cannot initiate outbound connections to arbitrary internet hosts	Critical	*Prevent command & control (C2) communication and data exfiltration*
☐	Unnecessary protocols and ports are blocked at the firewall (e.g., Telnet, FTP, SMB)	High	*Use secure alternatives: SSH, SFTP, HTTPS only*
☐	DNS queries from IoT devices are monitored for suspicious domain lookups	High	*Block known malicious domains via DNS sinkhole or firewall*
☐	Traffic inspection (DPI) is enabled to detect anomalous data patterns	Medium	*Use next-gen firewalls with application-layer inspection*

5. Remote Access & Cloud Connectivity

✓	Security Control	Priority	Implementation Notes
☐	IoT devices use private IP addressing with VPN tunnels for remote management	Critical	*Never expose IoT devices directly to the public internet*
☐	Cloud platform connections use TLS 1.2+ with mutual certificate authentication	Critical	*Disable SSLv3, TLS 1.0, and TLS 1.1*
☐	IoT SIMs use private APNs rather than public internet routing	High	*Provides network-level isolation for cellular-connected devices*
☐	Remote management interfaces are disabled when not in active use	High	*Minimize attack surface by disabling SSH, web UI, etc.*
☐	Session timeouts and automatic logout are configured for admin interfaces	Medium	*Prevent credential harvesting from abandoned sessions*

6. Monitoring, Logging & Incident Response

✓	Security Control	Priority	Implementation Notes
☐	Centralized logging captures authentication attempts, config changes, and errors	Critical	*Use syslog, SIEM, or dedicated IoT monitoring platform*
☐	Anomaly detection alerts on unusual traffic patterns, failed logins, or unauthorized access	Critical	*Establish baseline behavior and alert on deviations*
☐	Log retention policies meet compliance requirements (minimum 90 days)	High	*Longer retention for regulated industries (healthcare, finance)*
☐	Incident response playbook includes IoT-specific procedures	High	*Document steps for device quarantine, forensics, and recovery*
☐	Security events trigger automated responses (VLAN quarantine, device isolation)	Medium	*SOAR integration for rapid threat containment*

7. Physical & Environmental Security

✓	Security Control	Priority	Implementation Notes
☐	IoT devices in public areas are physically secured against tampering	High	*Use tamper-evident seals, locked enclosures, or cameras*
☐	Debug ports, USB interfaces, and JTAG connections are disabled or physically secured	High	*Prevent hardware-level attacks and firmware extraction*
☐	Devices exposed to harsh environments have appropriate ingress protection (IP rating)	Medium	*Dust, moisture, and temperature extremes can cause failures*
☐	Power supplies are protected against surges and have backup options where critical	Medium	*UPS or battery backup for life-safety and security systems*
☐	Asset disposal procedures include secure data wiping and certificate revocation	Medium	*Destroy or securely erase storage before disposal/recycling*

8. Vendor & Supply Chain Security

✓	Security Control	Priority	Implementation Notes
☐	IoT vendors provide regular security updates and have responsible disclosure policies	Critical	*Avoid vendors with poor security track records*
☐	Third-party risk assessments are conducted before deploying vendor IoT solutions	High	*Review security certifications, audit reports, and incident history*
☐	Vendor access to IoT devices is logged, time-limited, and requires approval	High	*Use jump hosts or VPN with per-session credentials*
☐	Service-level agreements (SLAs) include security incident notification requirements	Medium	*Vendors must notify you of breaches within 24-48 hours*
☐	Supply chain integrity is verified (device provenance, counterfeit detection)	Medium	*Purchase from authorized distributors with chain-of-custody*

9. Data Protection & Privacy

✓	Security Control	Priority	Implementation Notes
☐	Data in transit is encrypted using industry-standard protocols (TLS, IPsec)	**Critical**	*Never transmit sensitive data in plaintext*
☐	Data at rest on IoT devices is encrypted where feasible	**High**	*Use TPM/secure elements for key storage if available*
☐	Personally identifiable information (PII) collection is minimized and documented	**High**	*Comply with GDPR, CCPA, and other privacy regulations*
☐	Data retention policies define how long IoT data is stored and when it's deleted	**Medium**	*Delete or anonymize data that's no longer needed*
☐	Data processing agreements are in place with cloud providers and third parties	**Medium**	*Clarify data ownership, processing rights, and breach notification*

10. Resilience & Business Continuity

✓	Security Control	Priority	Implementation Notes
☐	Edge buffering and local autonomy allow devices to function during cloud outages	**High**	*Critical systems must continue operating offline*
☐	Multi-carrier SIM profiles provide network redundancy for cellular IoT	**High**	*Automatic failover if primary carrier is unavailable*
☐	Backup and recovery procedures are tested regularly (quarterly minimum)	**High**	*Validate configuration backups and disaster recovery plans*
☐	Graceful degradation strategies are defined for partial system failures	**Medium**	*Prioritize critical functions when resources are limited*
☐	Post-incident reviews document lessons learned and drive security improvements	**Medium**	*Root cause analysis and remediation tracking*

Assessment Summary & Next Steps

Completing Your Assessment:

After reviewing all 10 security domains, calculate your compliance score:

• Count the number of **Critical** controls implemented: _____ / Total Critical
• Count the number of **High** controls implemented: _____ / Total High
• Count the number of **Medium** controls implemented: _____ / Total Medium

Recommended Actions:

1. **Immediate (0-30 days):** Address all gaps in Critical controls. These represent unacceptable risks that could lead to system compromise or safety incidents.

2. **Short-term (30-90 days):** Implement High-priority controls and document compensating controls for any items that cannot be fully implemented.

3. **Medium-term (90-365 days):** Complete Medium-priority controls and establish continuous improvement processes for ongoing security monitoring.

4. **Continuous:** Re-assess quarterly, after major changes, or following security incidents. Update controls as threats evolve and new vulnerabilities emerge.

Additional Resources:

• NIST IoT Cybersecurity Framework: nist.gov/cybersecurity/iot
• IEC 62443 Industrial Security Standards: isa.org/standards-and-publications
• IoT Portal Guidance: iotportal.co.uk/what-is-iot
• OWASP IoT Top 10: owasp.org/www-project-internet-of-things/

Notes & Action Items:

_____

_____

_____

_____

_____

_____

_____