Medical Device IT Audit Readiness Checklist

How to Read This Checklist

This checklist is designed to help Medical Device and Life Science organizations assess whether their IT **environment, security controls, and operational practices** are prepared to support regulatory audits.

It focuses on **IT General Controls (ITGCs)** and cybersecurity practices that auditors frequently review or request evidence for.

Each section describes:

- **What auditors expect**
- **What Tech River manages or supports**
- **What evidence can be produced during an audit**

This checklist reflects Tech River's operational approach to supporting regulated environments and should be reviewed alongside your Quality Management System (QMS) and regulatory guidance. It is intended to support audit readiness by ensuring foundational IT controls are in place and documented.

Regulatory Scope Referenced

This checklist aligns IT practices commonly associated with:

FDA 21 CFR Part 11

Electronic Records & Signatures – IT controls support

HIPAA Security Rule

Administrative, Technical, and Physical Safeguards

NIST Cybersecurity Framework

Best-practice Reference

Section 1:
Access Control & Identity Management

What auditors expect:

Controlled, documented access to systems that store or process regulated data.

How Tech River supports this:

- Centralized identity management using secure directory services
- Role-based access controls aligned to job function
- Least-privilege enforcement for users and administrators
- Multi-factor authentication (MFA) for:
  - Remote access
  - Administrative accounts
  - Cloud applications (e.g., Microsoft 365)

Audit Readiness Checklist:

- ✓ All users have unique accounts (no shared credentials)
- ✓ Role-based access controls (RBAC) are defined and documented
- ✓ MFA enforcement is documented
- ✓ User onboarding and offboarding workflows are defined
- ✓ Access is removed promptly when employees or contractors leave
- ✓ Access review evidence can be produced

Audit Evidence Tech River Can Provide:

- Access review reports
- MFA enforcement screenshots or policies
- Account lifecycle documentation

Section 2:
Endpoint & Device Security

What auditors expect:

Systems accessing regulated data are protected, monitored, and controlled.

How Tech River supports this:

- Managed endpoint protection with advanced threat detection
- Centralized monitoring and alerting
- Device inventory and lifecycle tracking
- Disk encryption and endpoint hardening
- Controls around removable media and mobile access

Audit Readiness Checklist:

- ✓ All endpoints are inventoried and tracked (laptops, desktops, servers)
- ✓ Endpoint protection (AV/EDR/MDR) is deployed and monitored on all supported systems
- ✓ Devices are encrypted
- ✓ Security alerts are reviewed and documented
- ✓ Mobile and remote access is secured

Audit Evidence Tech River Can Provide:

- Endpoint inventory reports
- Security monitoring summaries
- Encryption status verification

Section 3:
Patch Management & System Updates

What auditors expect:

Known vulnerabilities are addressed in a timely, documented manner.

How Tech River supports this:

- Centralized patch management for operating systems
- Regular patch cycles with reporting
- Exception handling for validated systems
- Visibility into patch status across the environment

Audit Readiness Checklist:

- ✔ OS patching is automated or centrally managed
- ✔ Critical patches are applied within defined timelines
- ✔ Patch exceptions are documented and approved
- ✔ Patch status reports are available

Audit Evidence Tech River Can Provide:

- Patch compliance reports
- Exception documentation
- Update schedules

Section 4:
Logging, Monitoring & Incident Response

What auditors expect:

The organization can detect, respond to, and document security incidents.

How Tech River supports this:

- 24/7 security monitoring of endpoints and systems
- Centralized alerting and escalation
- Documented incident response procedures
- Incident logging and post-incident review support

Audit Readiness Checklist:

- ✔ Security logs are enabled and retained
- ✔ Logs are retained according to documented retention policies
- ✔ Alerts are actively monitored
- ✔ An incident response plan is documented and approved
- ✔ Incident response roles are defined
- ✔ Security incidents are documented
- ✔ Evidence of response actions is retained

Audit Evidence Tech River Can Provide:

- Incident response documentation
- Security alert summaries
- Incident timelines and reports

Section 5:
Backup, Recovery & Business Continuity

What auditors expect:

Critical data can be recovered and business disruption minimized.

How Tech River supports this:

- Managed backups for critical systems
- Encrypted, offsite backup storage
- Regular backup monitoring
- Periodic recovery testing
- Ransomware-aware recovery design

Audit Readiness Checklist:

- ✔ Regular backups are performed for critical systems and data
- ✔ Backups are encrypted and protected from unauthorized access
- ✔ Restore testing is documented
- ✔ Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined

Audit Evidence Tech River Can Provide:

- Backup success reports
- Restore test documentation
- Recovery procedures

Section 6:
Cloud & Third-Party Systems

What auditors expect:

Cloud platforms and vendors are secured and overseen.

How Tech River supports this:

- Secure configuration of Microsoft 365 and cloud services
- Restricted administrative access
- Monitoring of cloud activity
- Support for vendor access reviews and risk discussions

Audit Readiness Checklist:

- ✔ Cloud environments (e.g., Microsoft 365, Azure) are secured and monitored
- ✔ Administrative access to cloud platforms is restricted and logged
- ✔ Third-party vendors with system access are identified
- ✔ Vendor access is reviewed periodically
- ✔ Cloud security controls are documented

Audit Evidence Tech River Can Provide:

- Cloud access and security reports
- Administrative role documentation
- Vendor access records

Section 7:
Documentation & Audit Evidence Readiness

What auditors expect:

Policies exist and evidence can be produced efficiently.

How Tech River supports this:

- Assistance documenting IT and security procedures
- Centralized access to audit-relevant evidence
- Support during audit preparation and questioning

Audit Readiness Checklist:

- ✔ IT policies and procedures are documented and current
- ✔ Evidence can be produced for:
  - Access reviews
  - Patch management
  - Backup verification
  - Incident response
- ✔ Audit support roles (who answers what) are clearly defined
- ✔ Documentation is stored centrally and accessible for audits

Audit Evidence Tech River Can Provide:

During audits, Tech River supports clients by:

- Assisting with IT-related auditor questions
- Providing requested documentation and reports
- Helping explain security controls and processes
- Supporting remediation if gaps are identified

This reduces stress and ensures audits remain focused and efficient.

Final Disclaimer

This checklist is provided for informational purposes only and does not constitute legal or regulatory advice. Regulatory requirements vary, and organizations should consult appropriate compliance professionals for formal audit preparation.