



How to Prep for a Compliance Audit Using a CMMS

Tags	CMMS Documentation	Compliance Content
	Internal Documentation	SOP
Category	Documentation & Knowledge Management	

Case Study

How I Turned CMMS Audit Prep into a Repeatable, Sanity-Saving Process

Summary

Most compliance prep relies on tribal knowledge and last-minute panic. I created a clear, repeatable checklist that mapped what needed to be verified in our CMMS and when. It helped our team avoid rework, reduce audit risk, and walk into inspections with more confidence and fewer surprises.

Context

I was working in a clinical engineering department responsible for maintaining over 1,600 medical devices. Our CMMS had scattered data, inconsistent service histories, and no clear audit-prep workflow. When Joint Commission prep rolled around, it meant pulling late nights, cross-checking bad exports, and relying on memory. Our team was capable, but the documentation was not. We didn't need better people, we needed a better process.

The Work

I started by reverse-engineering what surveyors looked for. Then I identified the fields in our CMMS that were most often incomplete, duplicated, or misused. I worked directly with our techs and managers to build a pre-audit checklist that tracked high-risk data points and timing windows.

I wrote it in plain language, stored it where the team already worked, and made sure it didn't sound like a policy manual. The checklist became something techs actually followed, not just a formality.

Impact

After we rolled it out, we shaved two to three days off audit prep. We caught bad records sooner and walked into inspections without scrambling. Our leadership team started using the checklist to train new techs and standardize expectations.

1. Run a Preventive Maintenance Status Report

- Filter by overdue, upcoming (30 days), and incomplete PMs.
- Prioritize high-risk and high-visibility equipment.
- Export to spreadsheet if necessary for sorting.

2. Audit Equipment Location and Status

- Cross-check critical equipment tags and locations against the database.
- Flag “mystery assets” or inactive devices that still appear on reports.
- Confirm any moved or loaned equipment is properly tracked.

3. Review Documentation Completeness

- Verify that all completed PMs have matching service records.
- Confirm service dates, technician names, and asset numbers match.
- Check for incomplete or handwritten notes that need digital entry.

4. Verify Recall and Alert Logs

- Confirm all recall alerts have been logged and documented.
- Make sure closure notes or follow-up actions are recorded in CMMS or SharePoint.

5. Clean Up the System View

- Ensure consistent naming conventions.
- Resolve duplicates or miscategorized assets.
- Tag incomplete items for follow-up (but don't delete).

6. Document What You Find

- Create a “pre-audit status” report to share with leadership.
- Log gaps and pending issues with estimated resolution dates.
- Note anything that requires escalation or coordination with other departments.

Final Checks

- Run your compliance checklist one last time.
- Test a sample audit path (e.g., pick a few devices and walk through their PM, service history, and location).
- Confirm your team knows where to find documentation if questioned during the audit.

Tips

- Auditors often ask for traceability, so make sure work orders reference asset IDs consistently.
- Don't assume everything in the CMMS is current without cross-checking it.
- Keep your SharePoint (or other documentation repo) folders tidy and intuitive.
- If you're short on time, focus on visibility and traceability, not perfection.