THIN LINE SOFTWARE
CJIS READINESS CHECKLIST

CJIS readiness checklist

Originally published: September 2026 · Last reviewed: September 2026

Printable take-away from Preparing for a CJIS audit shouldn't start when the auditor calls.

CJIS readiness checklist

Verify that the item can be produced or demonstrated. This checklist does not determine compliance. Items that organize work rather than restate a named requirement are practical readiness recommendations.

Scope and responsibility

- [ ] Current description of where CJI enters and which systems handle it can be produced
- [ ] LASO, TAC, and other applicable CJIS roles are identified
- [ ] Staff know who to contact with a CJIS or security question
- [ ] Primary owners are named; a backup is named where practical, or the single-person dependency is visible

Policies, people, and access

- [ ] Required policies can be produced and show agency-specific procedures
- [ ] Required policy reviews or approvals can be produced where applicable
- [ ] Current authorized-user list has been compared with active accounts
- [ ] Required personnel screening documentation can be produced
- [ ] Current security-awareness training records can be produced
- [ ] Former users and role changes have been removed or adjusted
- [ ] How applicable users authenticate can be demonstrated

Systems, network, and protection

- [ ] Current inventory of systems and devices that handle CJI can be produced
- [ ] Current network or system diagram can be produced and explained
- [ ] Remote and mobile access methods can be explained
- [ ] Applicable encryption or data-protection implementation can be shown
- [ ] Applicable logs can be produced
- [ ] Evidence that required log review occurred can be produced

Incidents, media, vendors, and the building

- [ ] Current incident-response plan can be produced
- [ ] Staff reporting and DPS/escalation contacts are current
- [ ] Incident-response testing, exercise, or review can be shown where applicable

- [ ] Media storage, transport, and destruction procedures can be demonstrated
- [ ] Vendors that can affect CJI are identified
- [ ] Required Security Addenda and vendor agreements can be produced
- [ ] Continuity or recovery information can be produced if a CJI system is unavailable
- [ ] Physical control of relevant areas, visitors, and displayed or printed CJI can be explained
- [ ] Prior findings and remediation evidence can be produced

Generated from the Thin Line Software resource library. Read this guide online: https://thinline.software/resources/texas-cjis-audit-readiness-checklist#pre-audit-checklist