imprivata

2026 CJIS compliance checklist: Assessing readiness and maturity

How to use this checklist

Being CJIS compliant should be more than just checking boxes. This CJIS compliance checklist helps agencies across the spectrum of justice and public safety determine whether their CJIS controls are merely **present** – meaning they meet the minimum requirements to comply with CJIS – or truly **durable** – meaning they are set up for long-term success.

Each section compares baseline compliance with mature compliance, along with including signs your organization may be at risk.

Identity and authentication

Baseline

- MFA enabled for CJIS access
- Complex passwords are still central to access

Mature

- Identity-centric, phishing-resistant MFA everywhere
- Minimal password use
- MFA works across shared and mobile devices without personal phones

Signs you may be at risk

- MFA inconsistent across systems
- Heavy password reliance

- [ ] MFA enforced consistently across all CJIS systems
- [ ] Authentication tied to user identity, not device or password

Shared workstations and mobile devices

Baseline

- Generic login required on shared devices
- Timeouts prevent unattended access

Mature

- Fast user switching and session isolation
- Each session uniquely tied to a user
- Clear individual accountability in logs

Signs you may be at risk

- Credential sharing to save time
- Sessions persist across shifts
- Accountability depends on behavior

- [ ] Each CJIS access event maps to a unique user
- [ ] Shared devices do not rely on manual sign-out

Access control and least privilege

Baseline

- Roles defined
- Periodic access reviews

Mature

- Role-based, time-bound access
- Automatic adjustment as roles change
- Privileged access isolated and monitored

Signs you may be at risk

- Access accumulates over time
- Manual deprovisioning
- Temporary access becomes permanent

- [ ] Users only have the access they need today
- [ ] Access removed promptly when roles change

Third-party and vendor access

Baseline

- Vendors approved and documented
- Access granted as needed

Mature

- Time-bound, policy-based access
- Vendor activity logged and reviewed
- Access can be quickly enabled or revoked

Signs you may be at risk

- Broad or long-lived access
- Limited monitoring
- Shared or generic credentials for vendors

- [ ] All third parties with CJIS access are known
- [ ] Vendor activity is logged and auditable

Audit logging and visibility

Baseline

- Logs exist
- Logs exported on request

Mature

- Centralized, tamper-resistant logs
- Fast, confident audit response
- Clear view of who accessed what and when

Signs you may be at risk

- Logs scattered across systems
- Manual correlation required
- Limited visibility

- [ ] Can answer audit questions without manual log hunting

Legacy systems

Baseline

- Legacy systems documented
- Compensating controls noted

Mature

- Overlay controls enforce MFA and logging
- Consistent enforcement across old and new systems with single sign-on in place

Signs you may be at risk

- No native MFA or auditing
- Controls rely on process

- [ ] Access to legacy systems meets CJIS controls

Policy enforcement

Baseline

- CJIS policies documented
- Users are expected to comply

Mature

- Technical enforcement over policy reliance
- Exceptions are rare, documented, and time-limited
- Policies are regularly reviewed/refreshed

Signs you may be at risk

- Enforcement varies by team
- Frequent exceptions to your policy

- [ ] Enforcement consistent across systems

Training and awareness

Baseline

- Periodic CJIS training
- Policy awareness required

Mature

- Training aligned to real workflows
- Users understand the impact on audits and accountability

Signs you may be at risk

- Training is checkbox-driven
- Users have a limited understanding of why controls are in place

Users understand why controls exist

Change and scalability

Baseline

- Controls work today
- Compliance maintained manually

Mature

- Controls scale automatically
- Compliance improves as the environment grows

Signs you may be at risk

- New systems introduce gaps
- Change increases workload

Compliance improves as systems and users are added

Quick maturity check

- Where are you compliant but fragile?
- Where would an audit create stress?
- Which improvements would reduce risk fastest?

Meeting CJIS compliance requirements may be your baseline, but achieving CJIS compliance maturity means controls will hold up as people and systems change.

Click here to learn how to build lasting, durable CJIS compliance.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

3855-2026_CJIS-maturity-checklist