

# CJIS Security Support

Technical support for aligning with CJIS Security Policy requirements.

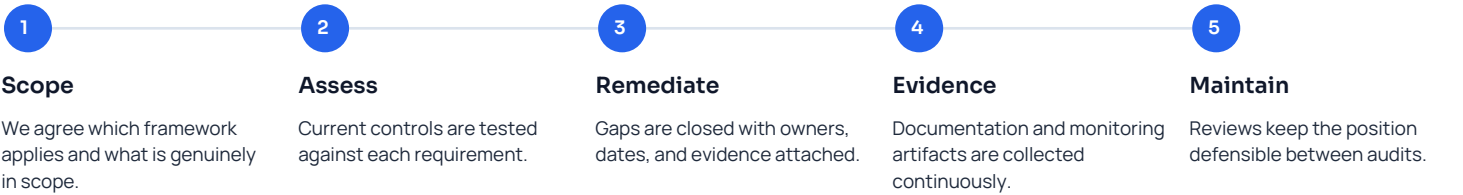


Service illustration • Compliance Governance

### What this service addresses

- Framework requirements from clients, contracts, or regulators
- Policies that are outdated or missing
- Difficulty producing evidence of controls

### A clear path to delivery



### Included capabilities & what they mean

| Capability                       | Practical detail                                                                              |
|----------------------------------|-----------------------------------------------------------------------------------------------|
| Gap and readiness assessments    | Compare the current environment with applicable framework requirements and prioritize gaps.   |
| Policy and procedure development | Translate requirements into usable policies with clear ownership and review responsibilities. |
| Control implementation support   | Help put agreed controls into operation and record the supporting evidence.                   |
| Ongoing compliance monitoring    | Review control status and evidence over time; readiness is maintained rather than assumed.    |
| Risk assessment and tracking     | Document risks, accountable owners, treatment decisions, and the remaining exposure.          |

### Business outcomes

- A clear roadmap toward framework readiness
- Documented, maintained policies
- Better-organized audit evidence

### Before we begin

Do you certify organizations? No. We provide readiness and implementation support. Certification and attestation are performed by independent, accredited assessors.

Readiness support only. Certification and attestation are performed by independent assessors; no compliance guarantee.

COMPLIANCE AND GOVERNANCE

# CJIS Security Support: a closer look

Technical support for aligning with CJIS Security Policy requirements.

## From challenge to coverage

SIGNS IT IS TIME TO ACT

- 1 Handling criminal justice information without knowing which controls apply
- 2 Audit requirements arriving with little notice
- 3 Policies written for a different environment than the one in use
- 4 Logins, privileges, and logs that can't be evidenced on request

WHAT THE SERVICE COVERS

- CJIS Security Policy gap review
- Access control and audit configuration
- Encryption and transmission review
- Policy and procedure alignment
- Evidence collection support

## CJIS alignment needs agency-specific context

| Area                 | What we review                                            | Why it matters                                                     |
|----------------------|-----------------------------------------------------------|--------------------------------------------------------------------|
| Applicability        | Agency obligations and criminal justice information flows | Confirm requirements with the responsible agency authority.        |
| Technical safeguards | Access, encryption, logging and device controls           | Identify configuration work supporting applicable requirements.    |
| Evidence             | Responsible owners and review records                     | Keep technical evidence available for the agency's review process. |

The linked tool covers SOC 2, ISO 27001 and CMMC—not CJIS. Use it only for general control awareness; CJIS needs a separate review.

## How an engagement runs

01

Discover

Review the current environment, priorities and constraints with your team.

02

Plan

Agree scope, owners, timing and how success will be reviewed.

03

Deliver

Carry out the agreed work with documented changes and checkpoints.

04

Review

Revisit results, open items and next priorities on an agreed cadence.

## What good looks like

The results this service is designed to support. Actual results depend on your environment and the agreed scope.

A clear picture of which CJIS requirements apply to you

Controls configured and documented in one place

Evidence ready to produce when asked

A defined plan for remaining gaps

## Questions clients ask

### Does this make us CJIS compliant?

No. We provide technical and documentation support. Compliance is determined by the reviewing authority, not by us.

### Where does CJIS support fit with our other frameworks?

Where controls overlap, evidence is reused. CJIS-specific requirements are handled separately so nothing is assumed.

## Your next step

### Free self-assessment

#### Compliance Readiness

Map readiness against common frameworks.

[massiveit.com/compliance-assessment](https://massiveit.com/compliance-assessment)

### Talk to an engineer

#### Book a consultation

Walk through your environment and get a scoped recommendation.

[massiveit.com/consultation](https://massiveit.com/consultation) • (813) 518-5454

### RELATED COMPLIANCE AND GOVERNANCE SERVICES

SOC 2 Readiness • CMMC Readiness • ISO 27001 Readiness • Security Governance • Risk Assessments • Compliance Monitoring

Readiness support only. Certification and attestation are performed by independent assessors; no compliance guarantee. Scope, licensing and service levels vary by environment and are confirmed in your agreement. This overview describes typical engagements, not guaranteed results.