COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

CJIS Security Policy

Now available in Compliance Manager GRC
Purpose-built for MSPs and IT teams supporting agencies that handle Criminal Justice Information (CJI)

What is the CJIS security policy?

The **Criminal Justice Information Services (CJIS) Security Policy**, published by the FBI, establishes the minimum security requirements for protecting **Criminal Justice Information (CJI)**. It defines the technical, physical and administrative safeguards that must be in place wherever CJI is created, stored, processed or transmitted.

CJIS Security Policy:

- Aligns with **NIST SP 800-53 Rev. 5** security and privacy controls
- Covers identity and access management, authentication, encryption, incident response, auditing and more
- Applies to criminal justice agencies (CJAs), non-criminal justice agencies (NCJAs), vendors and service providers

Non-compliance can threaten public safety, derail funding and jeopardize contracts, especially when CJI is handled by external partners such as MSPs or cloud providers.

Why MSPs and agencies should care

Criminal justice systems increasingly rely on **distributed IT environments** — cloud services, SaaS apps, remote access tools and third-party IT providers. Every connection to CJI becomes a potential risk surface.

The CJIS Security Policy provides your organization and your clients with:

- A **standardized baseline** for securing CJI
- A clear set of **controls and audit expectations**
- A framework for **vendor oversight and contract obligations**
- A way to demonstrate **due diligence** to regulators, funding bodies and oversight committees

With **Compliance Manager GRC**, MSPs and agencies can turn CJIS requirements into a repeatable, documented process rather than ad-hoc checklists and spreadsheets.

Who must comply with CJIS requirements?

Organizations that create, store, access or transmit Criminal Justice Information (CJI) must comply, including:

- Federal, state and local law enforcement agencies
- Prosecutors' offices and public defenders
- Courts and justice departments
- 911 dispatch centers and public safety answering points
- IT service providers, MSPs and hosting providers that handle CJI
- Third-party vendors connected to CJI systems (e.g., records, case management or analytics platforms)

For MSPs, **your processes, tools and staff** fall within scope anytime you support systems that process CJI on behalf of an agency.

CJIS Security Policy structure

The CJIS Security Policy is organized into policy areas and requirements that address core security domains, including:

CJIS Policy Area / Domain	Example Requirements (Simplified)
Information Exchange Agreements	Define roles, responsibilities and data-sharing agreements for CJI
Security Awareness and Training	Train staff on CJI handling, incident reporting and safeguards
Incident Response	Detect, report and respond to security incidents involving CJI
Auditing and Accountability	Log access to CJI and review audit records regularly
Access Control & Authentication	Enforce strong authentication, MFA and least-privilege principles
Encryption	Encrypt CJI in transit and at rest where required
Physical and Environmental Protection	Secure facilities, workstations and server rooms
Personnel Security	Vet personnel and control access based on roles and background
Configuration & Change Management	Maintain secure configurations and track system changes

Compliance Manager GRC translates these requirements into **assessable controls, mapped evidence and automated reports** — so you can operationalize CJIS rather than just interpret the policy.

How Compliance Manager GRC streamlines CJIS compliance

Compliance Manager GRC provides a dedicated CJIS Security Policy v6.0 standard with pre-built controls, requirements and reports — plus two major sub-features that make CJIS more manageable.

1. CJIS assessments & documentation

With the CJIS standard in Compliance Manager GRC, you can:

- **Perform Rapid Baseline Assessments** to quickly identify high-risk gaps
- Conduct detailed **Controls and Requirements Assessments** aligned with CJIS and NIST 800-53 Rev. 5
- **Generate policies, procedures and operational documentation** tailored to CJIS expectations
- **Assign assessment tasks** to internal staff, agency contacts or client stakeholders
- **Produce auditor-ready reports**, including assessor checklists and CJIS assessment summaries

Everything is centralized, allowing MSPs and agencies to manage CJIS and other frameworks from one platform.

2. Compliance Monitor – Continuous device configuration monitoring

Compliance Monitor, an integrated feature of Compliance Manager GRC, extends your CJIS program beyond static questionnaires. It continuously monitors device configuration against recognized security benchmarks.

You can:

- **Deploy Discovery Agents** to endpoints in CJIS-relevant environments
- Map those agents to **CJIS and related standards** for ongoing compliance monitoring
- Use **CIS Benchmarks** (Level 1 and Level 2) to enforce secure configurations for servers, workstations and laptops
- Apply **Benchmark Exclusions and Device Exceptions** when justified, without losing visibility
- View **Compliance Readiness meters** to quickly understand how many devices meet baseline configuration requirements

For CJIS environments, Compliance Monitor helps you demonstrate:

- Secure configurations for systems that process CJI
- Continuous enforcement of baseline hardening
- Evidence that deviations from benchmarks are documented and justified

This is especially valuable for MSPs maintaining **ongoing technical assurance** on behalf of law enforcement and justice clients.

3. Risk Manager – Centralized CJIS risk management

Risk Manager in Compliance Manager GRC provides you with a dedicated dashboard for managing the risks uncovered in your CJIS assessments and technical scans. You can:

- Automatically populate the **Risk Manager dashboard** from the Plan of Actions & Milestones (POA&M)
- Assign **Risk Priority, Impact, Likelihood and Risk Response** (mitigate, accept, avoid, transfer) to CJIS-related issues
- Assign **responsibility** to specific users or roles (e.g., Agency Security Officer, MSP Security Lead)
- Visualize risks in a **Risk Heat Map**, plus summaries by status and response type
- Generate **PDF and Excel reports** for leadership, oversight boards and auditors

Risk Manager allows you to move from “we found issues” to “here’s how we’re actively managing CJIS risk”— with traceability across assessments, remediation tasks and reporting.

Key CJIS features in Compliance Manager GRC

With the CJIS Security Policy standard enabled, you can:

- **Select CJIS from the Standards Library** to launch a structured assessment
- **Perform rapid baseline, control and requirements assessments** against CJIS requirements
- **Generate CJIS-aligned policies and procedures** for agencies and vendors
- **Create and manage POA&Ms** to plan and track remediation work
- **Store evidence of compliance** (logs, screenshots, configs, documents) in a centralized repository
- **Use Compliance Monitor** to align device configurations with security expectations
- **Use Risk Manager** to prioritize and track CJIS-related risks across clients and sites
- **Produce reports** such as:
  - CJIS Assessor Checklist (.xlsx):
  - CJIS Security Policy Assessment Report (.docx)
  - Risk Manager dashboard reports and issue summaries

COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

Integrations that enhance CJIS service delivery

Compliance Manager GRC integrates with the broader Kaseya ecosystem so you can gather evidence and enforce CJIS controls more efficiently:

- **Compliance Monitor**
  Continuous configuration monitoring and benchmark alignment for CJIS-relevant devices
- **Risk Manager**
  Centralized risk scoring, tracking and reporting across all CJIS findings
- **VulScan / Network Detective Pro**
  Perform internal and external vulnerability scans to support CJIS technical controls devices
- **BullPhish ID**
  Deliver security awareness training aligned with CJIS security awareness and training requirements
- **IT Glue**
  Link system inventories, configurations and documentation directly to CJIS evidence items
- **Autotask / PSA Integrations**
  Sync POA&M tasks to your ticketing system for execution, tracking and SLA management

These integrations help you prove that CJIS controls aren't just documented — they're implemented and continuously maintained.

Value for MSPs and agencies

For **MSPs and MSSPs**, the CJIS Security Policy standard in Compliance Manager GRC enables you to:

- Launch or expand **managed CJIS** compliance services
- Differentiate in RFPs and renewals with a **documented, tool-driven methodology**
- Reduce liability through **standardized assessments, monitoring and reporting**
- Bundle CJIS services logically with other security offerings (vCISO, vulnerability management, endpoint security)

For **agencies and justice organizations**, it delivers:

- A clear, **auditor-ready compliance program** mapped to CJIS requirements
- Improved **visibility into risks, device compliance and remediation status**
- Reduced reliance on ad-hoc spreadsheets and manual document management
- Better alignment with **federal guidance, funding expectations and contract requirements**

Request a demo

CJIS Security Policy support, combined with **Compliance Monitor** and **Risk Manager**, is now available in Compliance Manager GRC.

Schedule a demo to see how quickly you can:

- Launch a new CJIS assessment
- Monitor device compliance continuously
- Prioritize and manage CJIS risks across your clients or agencies

Deliver repeatable, evidence-based CJIS compliance at scale with a platform purpose-built for IT professionals and service providers.