JupiterOne

The CISO Checklist

Continuous Controls Monitoring (CCM)

CISOs face an uphill battle

CISOs own cyber risk and are responsible for validating and improving operational resilience and agility. But CISOs lack a single pane of glass that captures the living risk landscape and provides actionable insights. As a result, you don't know what's workikng until something breaks.

JupiterOne provides continuous controls monitoring – a realtime picture of your digital environment, with all the context and data to fully understand its relationships and risks.

CISOs leading CCM adoption cut audit prep by 80%, spot drift in hours not months, and prove proactive risk management to their boards.

Adopting JupiterOne and continuous controls monitoring presents a whole new way of working. This checklist can help CISOs and teams shift from reactive scrambling to build secure systems.

Six Implementation Areas

Area	Checklist	How JupiterOne Helps
Executive Alignment	✓ Brief leadership/board on risks of manual validation ✓ Define success KPIs (audit prep time reduced, vulns remediated, etc.)	CCM dashboards provide continuous metrics for C-suite visibility.
Inventory and Integration	✓ Ensure asset inventory covers the entirety of cloud, identity, and security tools ✓ Test API integrations for data ingestion	JupiterOne graph auto-normalizes multi-source data continuously
Control Framework Mapping	✓ Identify the top 20 controls mapped to relevant frameworks ✓ Align relevant teams to security standards	JupiterOne performs unified framework mapping, noting when one control satisfies multiple frameworks
Automation Maturity	✓ Schedule regular tests for high-risk controls ✓ Connect evidence export workflows to GRC/ITSM	Automated JupiterOne queries runs and API evidence delivery eliminate manual pulls
Team and Process Readiness	✓ Train control owners on CCM and graph-powered visibility ✓ Define remediation SLAs	Drill down insights and alerting pave the way for ownership handoff
Go-Live Validation	✓ Validate that pilot dashboard shows the expected control coverage ✓ Generate mock audit evidence package	JupiterOne's always-on status and query-backed reports ensure ongoing audit readiness

JupiterOne

A CISO's Command Center for Managing Cyber Risk

Executive Risk Dashboard

- Real-time compliance posture across SOC 2, NIST, and other frameworks
- Trend analysis to spot systemic drift patterns
- Entity-level drill-downs showing blast radius

Proactive Risk Leadership

- Control tests flag gaps in hours, not quarters
- Automated alerts trigger targeted remediation
- Create automated tests for custom risks
- Minimize attack surface across complex environments

Operational Scale

- Automate evidence collection for hundreds of control tests
- Integrate ticketing workflows to close feedback-remediation loop
- Create bandwidth to spend on strategic priorities like threat hunting

Why Graph-Native Matters

Traditional tools correlate data from siloed sources; they can tell you what failed, but not why or what else is affected.

JupiterOne's graph connects assets, identities, vulnerabilities, and controls tests into a queryable model. When a control test fails, you see the blast radius instantly: which users, workloads, and data are exposed.

That's context no correlation engine can deliver.

Adopt Continuous Assurance

JupiterOne Continuous Controls Monitoring equips CISOs with a graph-powered platform built to illuminate blind spots, prioritize risk, automate evidence at scale, and deliver board-ready proof of resilience.

Contact us today to operationalize CCM and sharpen your competitive edge.

Get a Demo

JupiterOne