



BlinkOps Agentic GRC

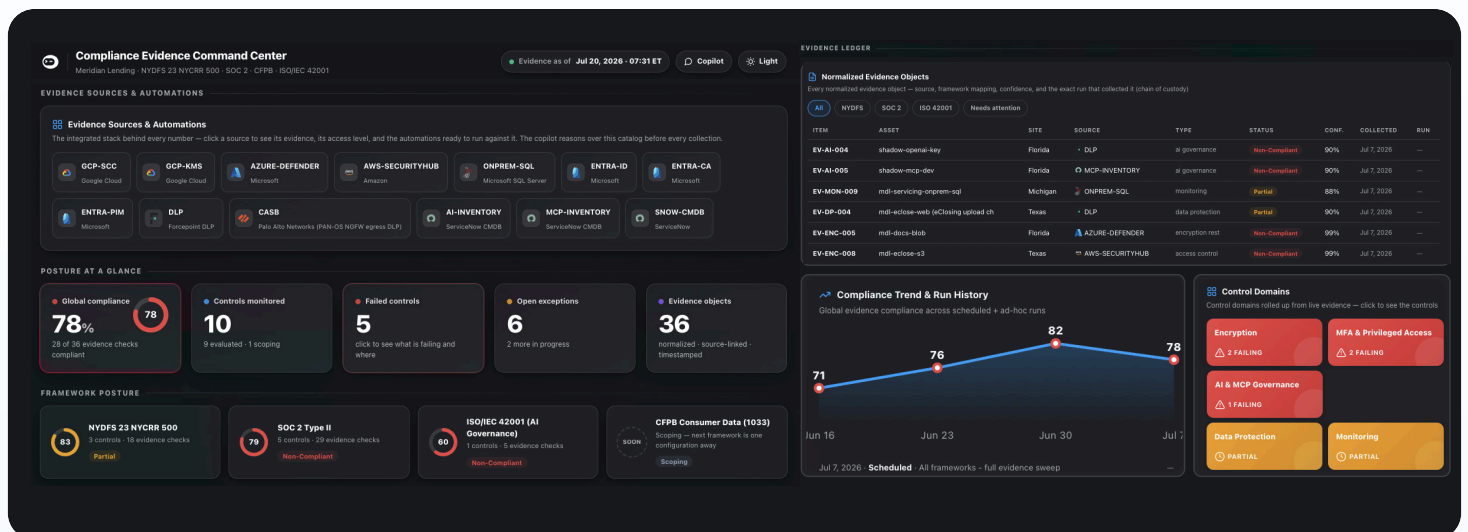
End-to-end agentic compliance operations, from control to audit package

Current State

GRC platforms track controls and frameworks, but teams still do the work of collecting evidence, chasing owners, checking whether controls are operating, and answering auditors. The same evidence gets gathered repeatedly for different frameworks, often through screenshots, spreadsheets, and email. As requirements expand, including AI governance, the workload grows while evidence becomes stale between audits. Gaps are too often discovered during audit preparation instead of when a control first fails.

Blink Solution

With BlinkOps, you can deploy agentic operators that carry GRC work through evidence collection, control mapping, gap detection, remediation, and audit response. Deterministic workflows enforce collection schedules, ownership, approvals, evidence storage, and audit trails; AI reasons over control requirements, framework mappings, gaps, and auditor questions. Operators keep evidence current, route failing controls to the right owner, track remediation to closure, and assemble cited audit packages on demand.



One operational view from control event to audit-ready package.

GRC solutions that our customers run

Evidence Collection Operator

Pulls evidence from connected systems on a schedule instead of asking owners for screenshots. Evidence is timestamped, stored, linked to the relevant control, and ready to cite when an auditor asks for it.

Control Mapping Operator

Maps each control and its evidence to the frameworks it satisfies. Teams can maintain one control library and reuse evidence across SOC 2, ISO 27001, NIST, and other applicable frameworks rather than repeating the same work for every audit.

Gap Management Operator

Continuously checks control status and evidence freshness against policy. When a control fails or evidence expires, it opens a case, routes it to the owner with context, and tracks the work through verified resolution.

Audit Response Operator

Assembles evidence packages and drafts responses grounded in the control library and source evidence. Reviewers can approve the response with its supporting citations and full history in one place.

Why Choose Blink

Work with top-tier security engineers

Blink's Forward Deployed Security Engineers help turn your control library, evidence requirements, and approval processes into working GRC solutions. They bring experience building and running security operations, so your team is not left to connect systems and design every workflow alone.

Agentify the entire security stack

With more than 30,000 integrations, Blink can gather evidence from the systems where controls actually run, identify gaps, assign work, and document resolution. The process continues from control event to audit response instead of stopping at another dashboard or reminder.

Get to value fast

Start with pre-built GRC solutions, then adapt them to your frameworks, control owners, policies, and audit process. Workflow Studio, Agent Studio, Solution Studio, and Case Management let you tailor execution, reasoning, approvals, and tracking without replacing your existing GRC stack.

Customer Proof

HUMAN Security

While preparing for ISO 27001, HUMAN Security used BlinkOps to automate audit coordination across Hyperproof, Jira, and Slack. A workflow pulled controls, created evidence-collection tasks, assigned owners, sent reminders, and returned completed documentation to Hyperproof. The company built 42 production workflows within two weeks and reported more than 100 hours of manual work eliminated during its early deployment.

About BlinkOps

With BlinkOps, security teams gain an operating layer that spans their entire security stack. From AI SOC, to vulnerability management, GRC, and IAM, Blink automates workflows from triage to remediation. One Agentic Security Operations Platform, infinite possibilities.