

CyberComply

Managed Cybersecurity Compliance — Operated End to End

CyberComply is not advice about compliance. Cyber Defense Advisors takes ownership of your cybersecurity compliance program and operates it — policies, controls, evidence, monitoring and audit coordination — so the burden leaves your team.

Delivered as an annual subscription scoped to organization size and compliance scope, it produces continuous audit readiness through an approval-only engagement model: your people review and approve, CDA does the work.

WHY CLIENTS BUY THIS NOW

REVENUE IS BLOCKED

An enterprise customer, a procurement team or a prime contractor has made a certification or a security review a condition of the contract.

NO INTERNAL CAPABILITY

There is no compliance function to build, and hiring one is slower and more expensive than the problem justifies.

THE PROGRAM HAS DRIFTED

Evidence is assembled by hand before each audit, controls were built for a prior examination, and nobody owns it day to day.

SERVICE TIERS AND OPTIONAL SERVICES

Four managed tiers sized to the organization, each a fully operated program rather than a project with an end date. Optional services attach to any tier.

► CyberComply Start — up to 50 employees

A managed compliance foundation for a first audit: program establishment, core policy and control framework, automated evidence, audit coordination.

► CyberComply Expand — up to 200 employees

Enterprise-scale operations across business units and environments, advanced evidence lifecycle, executive reporting, multiple concurrent frameworks.

► Security questionnaire response

Inbound customer security questionnaires answered end to end from your live compliance data.

► Compliance policy suite

Framework-aligned, audit-ready policies customized to your business, with review, approval and version management.

► Penetration testing

Delivered through CyberRecon and integrated into the compliance evidence set.

► CyberComply Growth — up to 100 employees

Multi-framework policy and control management, wider automation and evidence coverage, remediation tracking, readiness for recurring or parallel audits.

► CyberComply Enterprise — custom scope

Complex or regulated environments: CMMC, FedRAMP-aligned and multi-region obligations, dedicated compliance leadership, board and regulator reporting.

► Third-party risk management

Vendor inventory and classification, standardized vendor risk assessments, evidence collection and tracking.

► Annual risk assessment

Organizational, technical and operational risk identification and scoring, with a risk register and executive reporting.

WHAT THE PROGRAM DELIVERS

- **Operated compliance program** — CDA owns and runs it; your involvement is review and approval.
- **Policy and control framework** — implemented and maintained against the frameworks in scope.
- **Automated evidence collection** — continuous capture and validation through integrated tooling.
- **Continuous monitoring and gap identification** — issues surfaced and tracked, not discovered at audit.
- **Audit readiness and coordination** — CDA manages the lifecycle and works directly with your auditors.
- **Executive and board reporting** — control effectiveness, risk and remediation status on a standing cadence.

FRAMEWORKS SUPPORTED

STANDARD / AUTHORITY	APPLIED TO
SOC 2 (AICPA Trust Services Criteria)	Type I and Type II readiness, evidence and audit coordination
ISO/IEC 27001:2022	ISMS operation, Statement of Applicability, certification support
HIPAA Security Rule; PCI DSS	Safeguards, evidence and ongoing control operation
CMMC and NIST SP 800-171	Enterprise tier — defense-industrial-base obligations
FedRAMP-aligned requirements	Enterprise tier — federal and multi-region scope
Customer and contractual security requirements	Questionnaires, vendor reviews and flow-down clauses

DELIVERY APPROACH

1 ONBOARDING Structured kickoff, scope and objective confirmation, points of contact, tooling access. On signature	2 PROGRAM DESIGN Framework selection, control architecture, policy set, evidence model, gap baseline. Stand-up	3 IMPLEMENTATION Control and policy rollout, evidence automation, monitoring and issue tracking live. Stand-up	4 AUDIT READINESS Readiness review, evidence packaging, auditor coordination through the examination. Each cycle	5 CONTINUOUS OPERATION Ongoing monitoring, risk and remediation management, recurring audits, reporting. Annual term
--	--	--	--	--

TIMELINE Services begin immediately after onboarding; the program then operates continuously under an annual subscription term rather than concluding at a milestone. Audit cycles are managed as they arise.

WHERE AI IS USED – AND WHERE IT IS NOT

- Evidence collection and validation run continuously through integrated tooling, replacing the manual pre-audit scramble.
- Control crosswalking across frameworks is automated, so one implementation answers several standards.
- Customer security questionnaires are drafted from your live compliance data rather than rebuilt by hand.
- Monitoring and gap identification are model-assisted so issues surface early. **Every policy, control decision and audit response is reviewed and signed by a named CDA practitioner; client data is not used to train external models.**

WHO BUYS IT

CEO and founder · CTO and CIO · CISO · General Counsel · CFO · Head of Sales or Revenue where compliance is gating deals · PE operating partners

IDEAL CLIENT PROFILE

Organizations up to roughly 200 employees — SaaS and technology companies facing enterprise procurement, healthcare and healthcare-adjacent vendors, financial services and insurance, and defense-industrial-base suppliers — with no internal compliance function and no appetite to build one. Larger or regulated environments are scoped under the Enterprise tier.

WHY CDA

- ▶ **An operator, not an advisor**
Most firms tell your team how to run a compliance program. CDA runs it, and the internal lift is reduced to approvals.
- ▶ **Not a tool vendor either**
Compliance platforms track evidence; they do not design controls, write a defensible policy or argue a position with an assessor.
- ▶ **One program, several frameworks**
Work done once carries across SOC 2, ISO 27001, HIPAA and CMMC through a maintained crosswalk.
- ▶ **Independence preserved**
CDA prepares and coordinates; the audit itself is performed by an independent third-party firm. That separation is what makes the preparation credible.

SCOPE, GUARDRAILS AND RESPONSIBLE AI

CDA operates the compliance program; independent audits, attestations and certifications are performed solely by third-party audit firms. CDA provides no audit or attestation services and does not guarantee certification, audit or regulatory outcomes. Remediation execution and final decisions remain the client's. AI-assisted work is reviewed and signed by a named CDA practitioner; client data is not used to train external models.

Scope it with us.

Engagements are scoped and fixed-fee quoted to your environment. Contact us for scoping, references and a sample deliverable.

833-54-CYBER (833-542-9237)

info@cyberdefenseadvisors.com
cyberdefenseadvisors.com