

One Accountable Path

Keep work moving. Keep risk in check.

Practical IT and security support built around the work your people need to do. Layer8 connects workplace support, security improvement, useful monitoring and readiness evidence through one agreed operating plan.

Know who owns the next step, what work is covered and how the result will be checked. Each engagement has an agreed scope, responsibilities, escalation path and record of decisions.

Four Core Offerings

Managed IT

Keep people working with scoped remote support, endpoint maintenance, account lifecycle work and regular operating reviews.

Cybersecurity

Review the agreed environment, prioritize exposure and turn selected improvements into authorized changes with verification.

Resonance Monitoring

Connect devices and service signals around a maintained inventory and dependency map, with useful alert routing and an owner for the next action.

Phantom Assurance

Map the applicable requirements and boundary, review evidence, assign gaps and prepare a readiness handoff the customer can explain.

Supporting Capabilities

Network infrastructure, identity and PKI, cloud and workplace, recovery, governance and extended operating coverage are scoped beneath the applicable offering.

Scope and Operating Coverage

Support hours, included actions, escalation and data access are agreed for each engagement. Extended coverage requires verified shifts, partners, handoffs and response authority. Controlled-data work uses its separately approved personnel, locations, tools and support queues.

First conversation: Which workflow needs attention? What users, sites, platforms and support hours should the work cover?

Framework implementation experience

L8DT brings implementation experience across the frameworks and obligations below. L8DT supports scoped implementation and readiness work; the applicable version, contract, assessment route and decision authority are confirmed with the customer.

Implementation/readiness support only. L8DT does not claim QSA or C3PAO accreditation, organization certification, an assessment result or an ATO. Formal validation and authorization remain with the applicable independent body or customer authority.

PCI DSS

v4.0.1 / payment-data scope

Implementation: Map cardholder-data flows, responsibilities and evidence for agreed payment controls.

Boundary: Acquirer and qualified assessor set validation; implementation is not QSA status.

NIST Cybersecurity Framework

CSF 2.0

Implementation: Build current/target profiles, risk ownership, roadmap and operating checks.

Boundary: A CSF profile supports risk management; it is not regulatory certification.

CMMC

Contract-specific level, baseline and route

Implementation: Scope FCI/CUI, select the contract baseline, support the SSP, remediation and evidence.

Boundary: Readiness only; no C3PAO status, assessment result or certification is claimed.

NIST SP 800-171

NIST Rev. 3; contract may require Rev. 2

Implementation: Select the contract-required revision; map CUI boundary, controls and evidence.

Boundary: Assessment conclusions require the contract revision and authorized review method.

ISO/IEC 27000 series

ISO/IEC 27001:2022 and adopted amendments

Implementation: Link risk, policy, suppliers, control applicability and management review.

Boundary: Certification is determined by an independent certification body.

DFARS cybersecurity clauses

Actual contract clauses and flow-downs

Implementation: Scope contract clauses, systems and providers; prepare incident and flow-down procedures.

Boundary: Customer retains reporting/affirmation authority; counsel resolves legal interpretations.

ISO 9000 series

ISO 9001:2026 / confirm transition

Implementation: Document IT/service processes, change, corrective action and service measures.

Boundary: IT/service support only; customer retains its quality program and certification authority.

NIST SP 800-53

Rev. 5 / baseline and tailoring selected

Implementation: Map selected controls, inherited responsibility and evidence to the system boundary.

Boundary: A control mapping is not an ATO; identify the authorization authority.