LingaTech

TRACK 1 | CYBERSECURITY + RESILIENCE

DEFEND. RESPOND. RECOVER.

The New Cyber Playbook

Cyber resilience is the ability to reduce the likelihood and impact of incidents, make sound decisions under pressure, and restore critical services with confidence.

DEFEND

Reduce exposure before the incident.

- Know critical assets, identities, data, dependencies, and third parties.
- Assess controls, cloud configurations, vulnerabilities, and operational risk.
- Prioritize actions based on mission impact and likelihood.

RESPOND

Act with speed, authority, and discipline.

- Define decision rights, escalation paths, communications, and evidence handling.
- Build practical incident playbooks for likely scenarios.
- Exercise plans before a real event exposes gaps.

RECOVER

Restore services and improve resilience.

- Sequence recovery around business priorities and critical dependencies.
- Validate system and data integrity before returning to normal operations.
- Capture lessons learned and strengthen controls, plans, and governance.

THE SHIFT IN THE PLAYBOOK

FROM Point-in-time compliance
TO Continuous risk management

FROM Perimeter-first thinking
TO Identity, data, cloud, and resilience

FROM Plans stored on a shelf
TO Rehearsed roles and decisions

FROM Uncontrolled AI experimentation
TO Governed, secure adoption

Focus Areas: Cybersecurity | Risk Management | Incident Management | Resilience

HOW LINGATECH HELPS

LingaTech helps organizations turn cybersecurity objectives into practical, prioritized action. Our work connects business risk, technology architecture, cloud and AI strategy, incident readiness, and external requirements.

SECURITY + RISK ASSESSMENTS

- Review current-state controls, architecture, identity, data handling, logging, vulnerability management, and critical dependencies.
- Identify gaps and translate findings into a risk-ranked roadmap with practical next steps.

CLOUD SECURITY + MIGRATION READINESS

- Assess security implications before a migration or the establishment of a new cloud presence.
- Help design secure foundations for identity and access, data protection, monitoring, configuration governance, segmentation, and shared-responsibility ownership.

AI ADOPTION READINESS

- Assess use cases, data sensitivity, access, vendor and tool risk, governance, privacy, human review, and operational controls.
- Establish policy and decision paths so AI adoption advances with security and accountability built in.

CXOaaS LEADERSHIP

- Provide experienced executive guidance to build incident response and recovery plans, clarify roles, establish risk governance, and lead readiness exercises.
- Support alignment with applicable external requirements, contracts, and organizational policy.

COMPLIANCE AND POLICY READINESS

LingaTech can help map applicable requirements to current controls, identify gaps, and build remediation plans. Examples include CJIS, the HIPAA Security Rule, IRS Publication 1075, Pennsylvania CHRIA, and other agency, contractual, or internal policy requirements.

CJIS · HIPAA · IRS PUB 1075 · CHRIA · AGENCY POLICY

A PRACTICAL ENGAGEMENT MODEL

1. **UNDERSTAND** — Mission, systems, data, cloud and AI goals, obligations
2. **ASSESS** — People, process, technology, controls, and dependencies
3. **PRIORITIZE** — Risk-ranked roadmap, quick wins, and investments
4. **PREPARE** — Plans, playbooks, governance, roles, and communications
5. **EXERCISE + IMPROVE** — Tabletops, lessons learned, and recurring updates

START WITH A CYBER RESILIENCE, CLOUD, OR AI READINESS ASSESSMENT.

www.lingatech.com solutions@lingatech.com

Reference frameworks and requirements: NIST Cybersecurity Framework 2.0; NIST SP 800-61 Rev. 3; NIST AI Risk Management Framework 1.0; FBI CJIS Security Policy v6.1; HHS HIPAA Security Rule; IRS Publication 1075; Pennsylvania CHRIA, 18 Pa.C.S. Ch. 91. Applicability depends on the organization, data, and legal requirements.