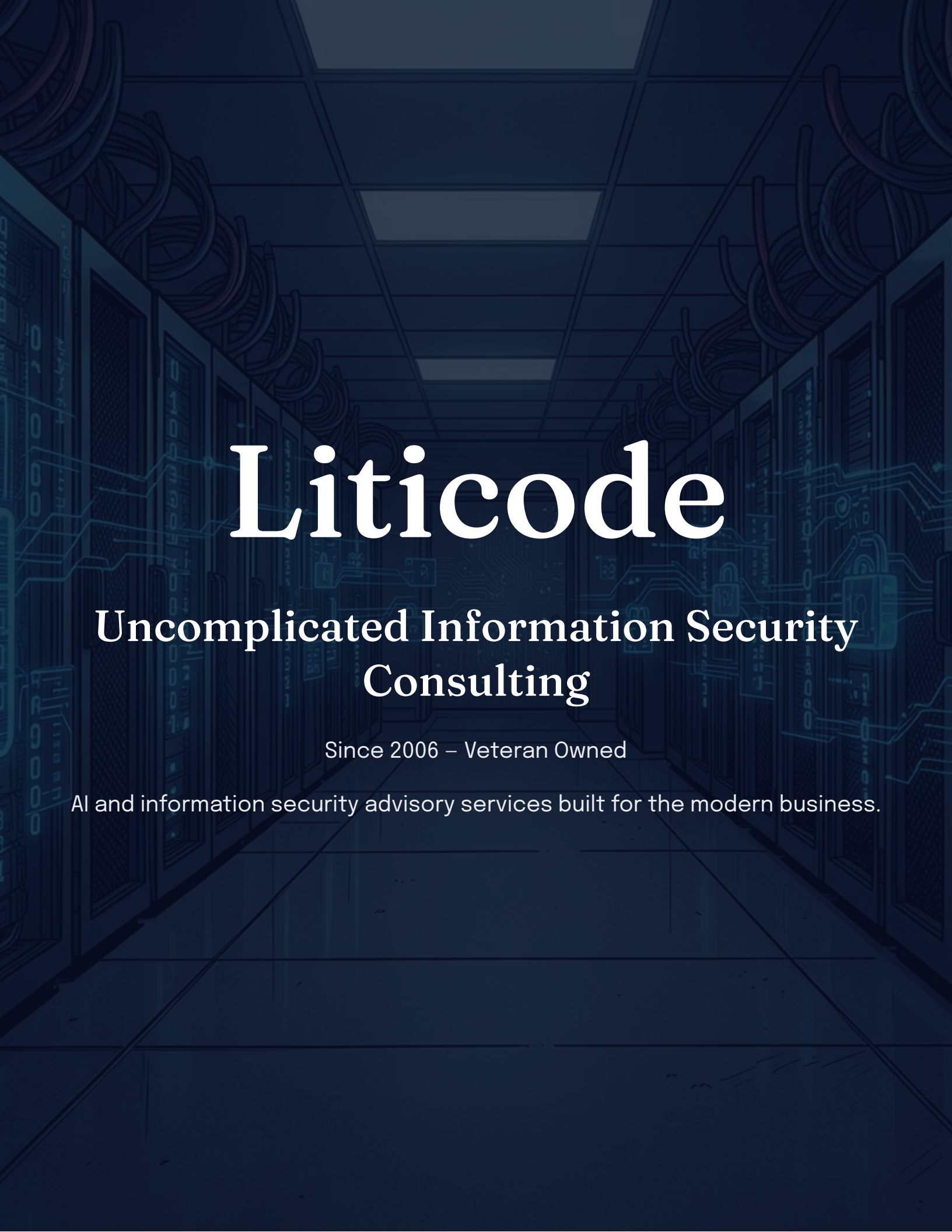


Liticode

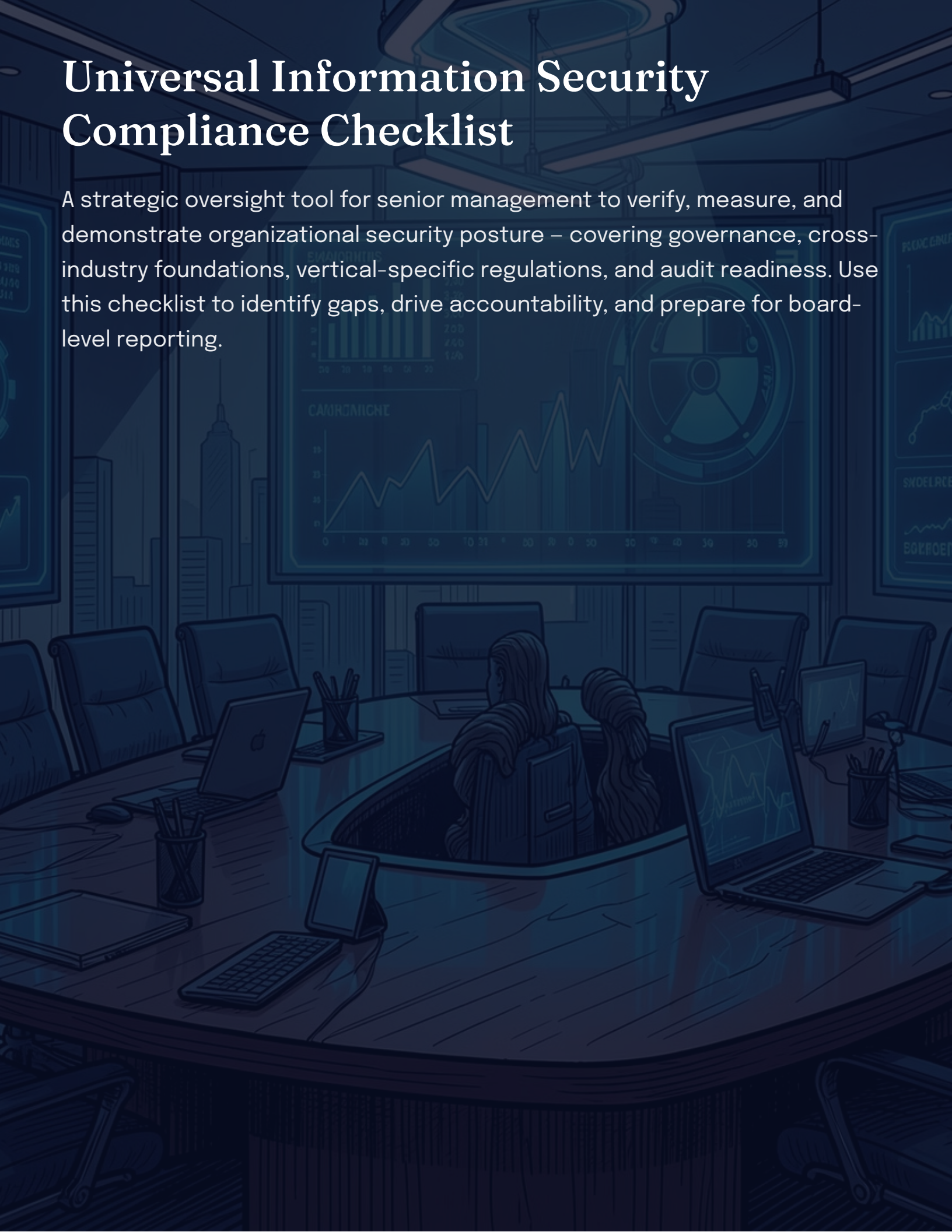
Uncomplicated Information Security Consulting

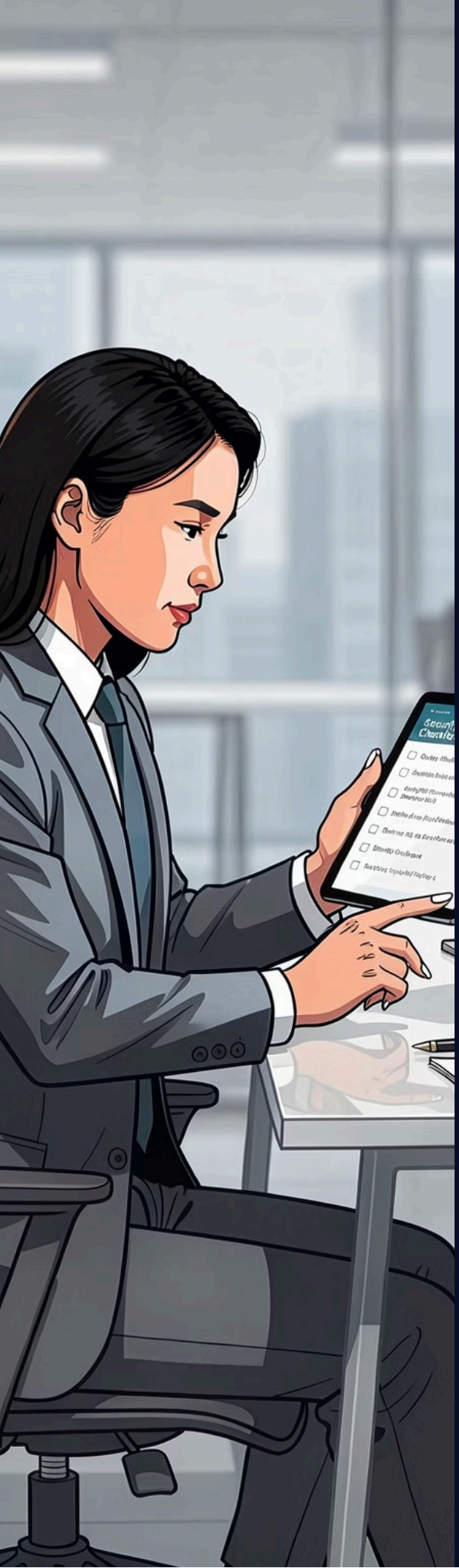
Since 2006 – Veteran Owned

AI and information security advisory services built for the modern business.

Universal Information Security Compliance Checklist

A strategic oversight tool for senior management to verify, measure, and demonstrate organizational security posture – covering governance, cross-industry foundations, vertical-specific regulations, and audit readiness. Use this checklist to identify gaps, drive accountability, and prepare for board-level reporting.





How to Use This Checklist

This document is designed for **strategic oversight** – not operational implementation. As a COO, your role is to verify that security and compliance programs *exist, are actively managed, and produce measurable outcomes*. Each section includes a visibility check to help you assess readiness for board reporting and regulatory scrutiny.

What to Verify

- Programs exist and are documented
- Controls are actively managed
- Metrics are tracked and reported
- Accountability is assigned at C-level
- Evidence is audit-ready

What This Is Not

- A technical implementation guide
- A replacement for your CISO or security team
- A one-time exercise
- A substitute for legal counsel
- A guarantee of compliance

ⓘ Regulations evolve continuously. Pair this checklist with periodic legal and regulatory horizon scanning.

1. Governance & Leadership Oversight

Security governance must be owned at the executive level. Without clear sponsorship, accountability, and board visibility, even well-designed programs fail to deliver results or demonstrate due diligence.

1

Executive Sponsorship

Designated C-level owner (e.g., CISO) with direct reporting to CEO/COO and Board. Clear accountability for security outcomes.

2

Board & C-Level Reporting

Quarterly risk briefings covering risk posture, incident summaries, compliance status, and financial exposure.

3

Policy Framework

Approved, up-to-date policies covering data classification, acceptable use, incident response, and vendor management – with annual review evidence.

4

Risk Management Program

Formal enterprise risk assessment including cyber risks, a maintained risk register, and treatment plans with ownership and timelines.

5

Budget & Resources

Dedicated security budget aligned to business risks, with metrics demonstrating ROI or risk reduction.

Visibility Check: Can you produce a one-page executive summary of current security posture for the next Board meeting?

2. Universal Cross-Industry Foundations

These controls apply broadly across all sectors and often serve as the baseline for industry-specific requirements. They represent the minimum security posture any organization should maintain and be prepared to demonstrate.

NIST CSF Adoption

Identify, Protect, Detect, Respond, Recover functions with documented control mapping.

Access & Identity

Least privilege, MFA, user provisioning/deprovisioning, and periodic access reviews.

Data Protection

Classification, encryption (at-rest/in-transit), backup testing, and DLP measures.

Incident Response

Tested IR plan, breach notification procedures, and disaster recovery capabilities.

Vendor Risk Management

Due diligence, contracts (BAAs where needed), ongoing monitoring, and SOC 2 attestations.

Training & Awareness

Regular training for all employees with phishing simulations and completion tracking.

Auditing & Monitoring

Logging, SIEM, vulnerability scanning, and penetration testing with remediation tracking.

Physical Security

Controls for facilities, equipment, and media handling.

Continuous Monitoring

KPIs: patch compliance, vulnerability remediation time, incident response times, audit pass rates.

Key Organizational Security Metrics

These metrics should be tracked consistently and reported to executive leadership and the Board. They provide the quantitative evidence needed to demonstrate program effectiveness, justify investment, and identify areas requiring intervention.

90%

Patch Compliance Target

Percentage of systems with up-to-date patches – a primary indicator of vulnerability management maturity.

30

Days to Remediate

Maximum acceptable window for high/critical vulnerabilities open before escalation to leadership.

100%

Training Completion

Target employee security training completion rate; phishing click rates should trend downward over time.

24h

Incident Detection MTTD

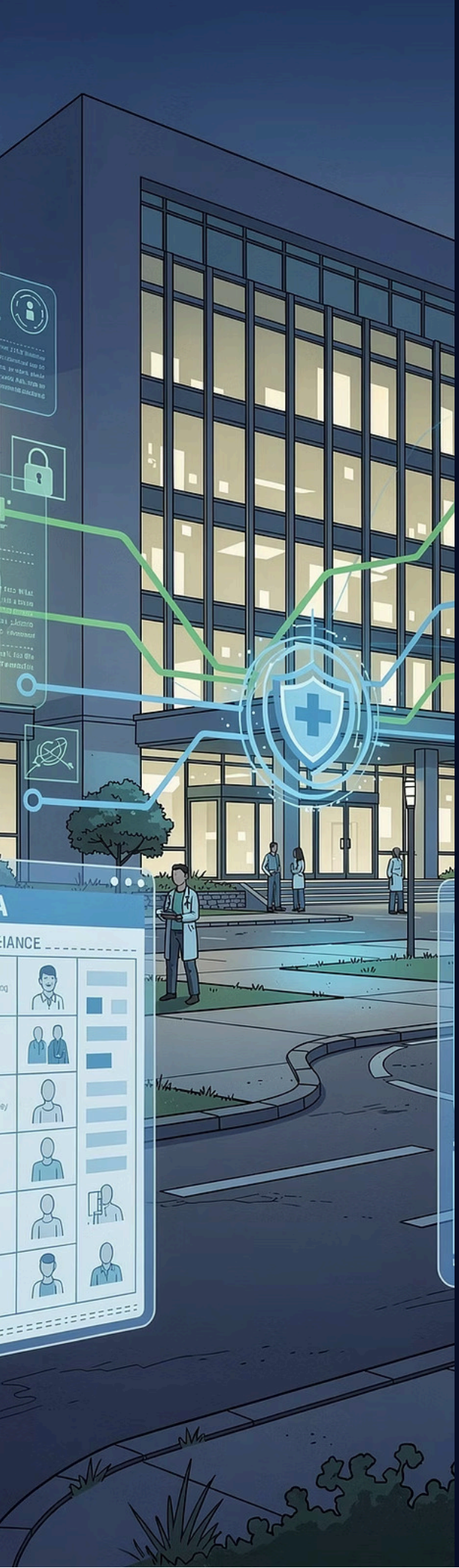
Mean time to detect incidents – a critical metric for measuring monitoring effectiveness and response readiness.

Additional Metrics to Track

- Third-party risk score summary
- Compliance adherence rate
- Audit pass rates
- Unremediated high-risk findings count
- Mean time to respond (MTTR)

Reporting Cadence

Metrics should be delivered via a **dashboard or scorecard** on a recurring basis – monthly for operational reviews, quarterly for Board reporting. Automation via AI-driven GRC tools significantly reduces manual effort and improves accuracy.



3. Industry-Specific Requirements: Healthcare & Business

Verify applicability based on your operations – data types handled, industry, contracts, and locations. Confirm that security program elements are documented, audited, and reported as required by each applicable regulation.

HEALTHCARE

HIPAA / HITECH

- Security Rule safeguards for ePHI (administrative, physical, technical)
- Business Associate Agreements (BAAs) with all vendors
- Breach notification and risk analysis requirements
- Audit logs and contingency planning

Key Metrics: PHI breach incidents, access audit trail review rates

GLBA / SOX / PCI DSS

- **GLBA:** Safeguards Rule for customer financial data protection and privacy notices
- **SOX:** Internal controls over financial reporting (ICFR) including IT general controls
- **PCI DSS:** Cardholder data environment segmentation, encryption, and annual assessments

Key Metrics: PCI compliance status, financial control effectiveness, customer data incident rates

Visibility Check: Do you have a mapping of applicable regulations to controls, with recent third-party validation (audit/attestation) and executive sign-off?

3. Manufacturing / OT-ICS

Operational Technology environments require specialized security frameworks that address the unique performance, reliability, and safety requirements of industrial systems – where downtime or compromise can have physical consequences.

IEC/ISA 62443 Series

Comprehensive controls for securing Industrial Automation and Control Systems (IACS), including security program requirements for asset owners, zone/conduit models, and security levels (SL 1-4) tailored to OT environments.

NIST SP 800-82 — OT Security Guide

Guidelines for Operational Technology (OT) security addressing unique performance, reliability, and safety requirements in ICS/SCADA environments – often used in conjunction with NIST CSF.

TISAX (Automotive Supply Chain)

VDA ISA-based information security assessment with maturity levels covering ISMS, physical security, prototype protection, and third-party data handling for suppliers to OEMs.

CMMC / NIST SP 800-171

Required for organizations handling Controlled Unclassified Information (CUI) or working with DoD/government contracts. Covers 110 security requirements across 14 families.

Additional Relevant Standards

ISO 27001 alignment, supply chain security for connected manufacturing/Industry 4.0, and sector-specific rules (e.g., chemical, energy under NERC CIP where applicable).

3. Manufacturing / OT-ICS (cont)

OT System Availability

Security uptime for ICS/SCADA systems

Segmentation Effectiveness

Zone/conduit model validation

Supplier Risk Assessments

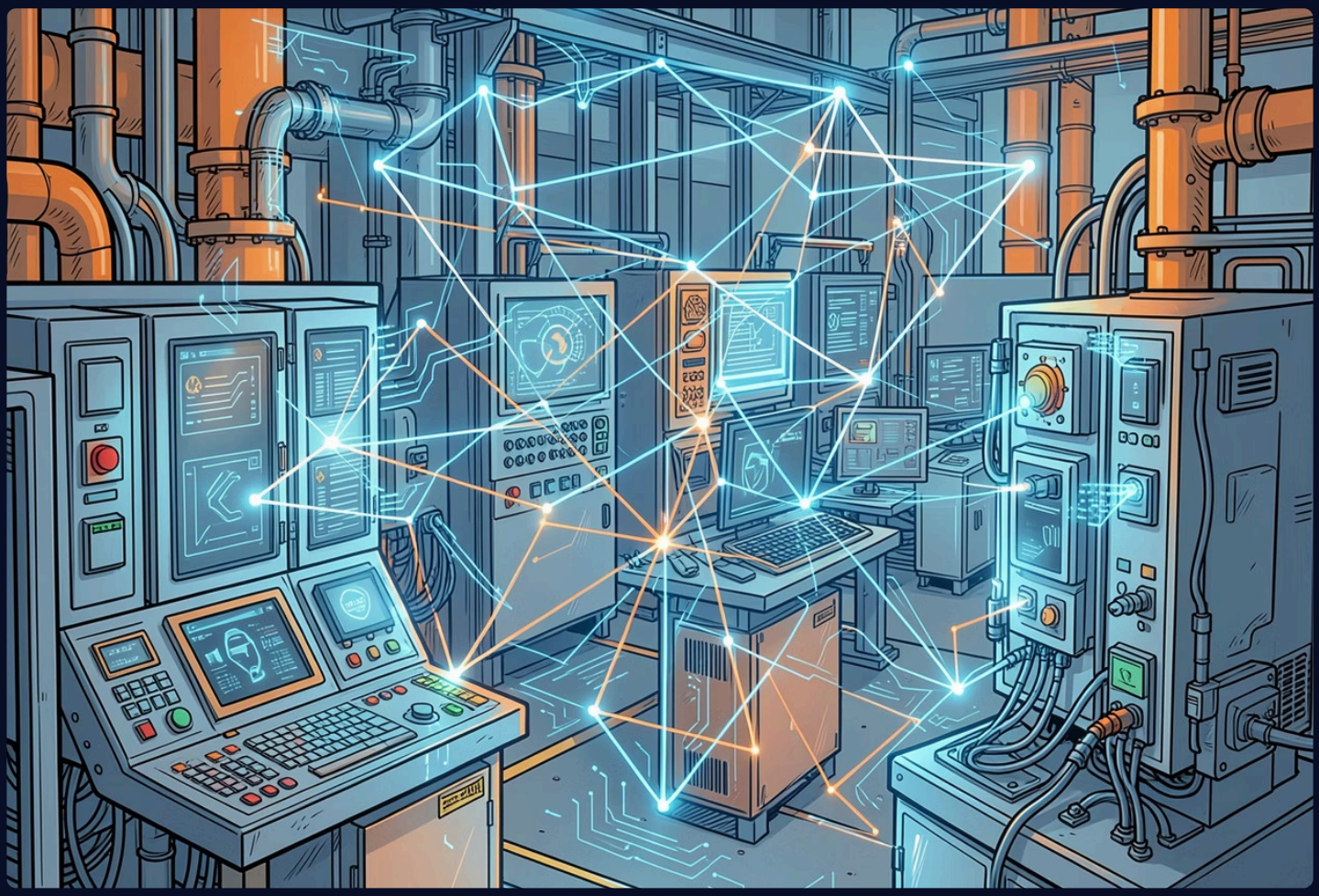
Third-party OT/ICS risk scores

Vulnerability Remediation

Closure rates for air-gapped/legacy systems

Audit Findings Closure

Industrial environment compliance rates



Visibility Check: Do you have documented mappings of your OT/ICS controls to these standards, with evidence of risk assessments, zoning, and recent third-party validations specific to manufacturing operations?

3. Public Sector, Government & General Requirements

Organizations serving government entities, handling sensitive citizen data, or operating across state lines must navigate a complex landscape of federal, state, and contractual obligations. Emerging SEC disclosure rules add another layer of accountability for public companies.

Federal Requirements

- **FISMA:** Federal Information Security Modernization Act compliance for federal agencies and contractors
- **FedRAMP:** Cloud security authorization for service providers to federal agencies
- **CMMC:** Cybersecurity Maturity Model Certification for DoD supply chain
- **DFARS:** Cybersecurity clauses for defense contractors handling CUI

GENERAL / OTHER

Broader Obligations

- **State Privacy Laws:** CCPA/CPRA (CA) and equivalents in VA, CO, CT, and emerging state legislation
- **SOC 2:** Common for service organizations serving enterprise clients – Type II preferred
- **SEC Cybersecurity Rules:** Material incident disclosure requirements for public companies (4-business-day rule)
- **GDPR:** Applicable where EU resident data is processed, regardless of company location
- **Contractual Obligations:** Customer-imposed security requirements in MSAs and DPAs

4. Audit Readiness & Continuous Improvement

Compliance is not a destination – it is a continuous discipline. Organizations that treat audits as a recurring program rather than a reactive event consistently achieve better outcomes, lower insurance premiums, and faster incident recovery.

Internal & External Audits

Maintain a scheduled cadence of compliance audits, penetration tests, and gap assessments. Track all findings to closure with documented evidence and executive sign-off.

Cyber Insurance Alignment

Review coverage annually. Ensure underwriting requirements are met – many insurers now require specific controls (MFA, EDR, incident response plans) as conditions of coverage.

Incident & Near-Miss Reporting

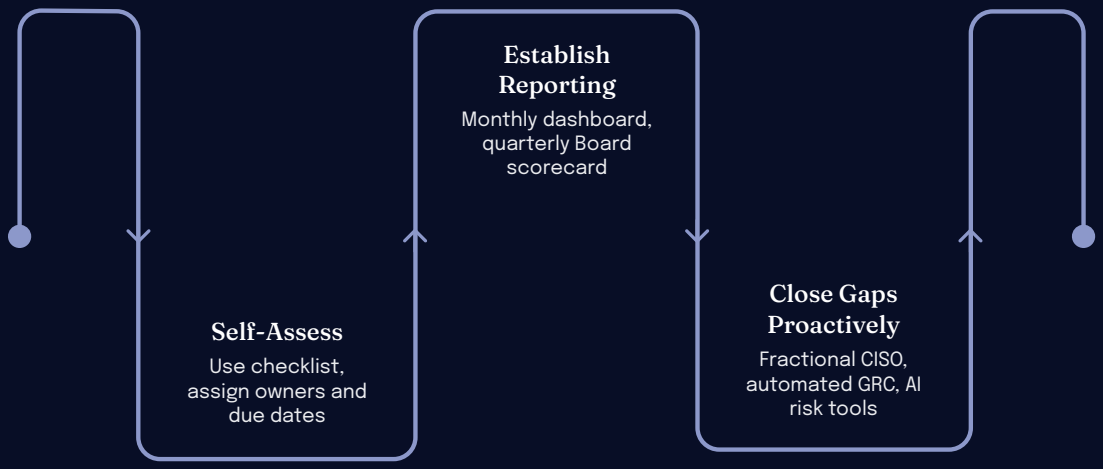
Cultivate a culture of timely escalation. Near-miss reporting surfaces systemic weaknesses before they become breaches. Leadership must model and reward transparency.

AI & Automation Integration

Where applicable, implement controls for AI systems (data governance, model security) and leverage automation for continuous compliance monitoring to reduce manual effort and accelerate audit cycles.

Next Steps for COOs

Use this checklist as your starting point – but the real value comes from turning visibility into action. The three steps below will help you move from assessment to accountability in your organization.



Organizations that operationalize these steps consistently report faster audits, lower insurance premiums, fewer incidents, and stronger board confidence in their security posture.

Partner with Liticode

Liticode's Secure Compliance & Risk Management services can help you operationalize and automate these checks – via AI-driven dashboards, risk registers, and audit-ready reporting – while integrating with your AI Systems & Automation initiatives for efficiency and ROI.

Visit Liticode.com

Key Reminders

- This checklist is a **starting point** – not a comprehensive legal or technical guide
- Regulations evolve – invest in **periodic horizon scanning**
- Security posture is a **business risk conversation**, not just an IT issue
- Board-ready reporting requires **metrics, not narratives**
- Automation and AI reduce **manual effort and accelerate ROI**

Liticode

Uncomplicated Information Security Consulting Services

Since 2006

Veteran Owned Disadvantaged Small Business

Contact Us

📍 HQ: 1636 N Cedar Crest Blvd #173, Allentown, PA 18104

📞 610.810.1727

✉️ sales@liticode.com

Locations: Allentown, PA (HQ) | Philadelphia, PA | Denver, CO | Cupertino, CA

Federal & Contract IDs

NAICS: 541519 Cybersec Cons

NAICS: 541690 Security Cons

NAICS: 541618 Mgmt Cons

SIN: 54151HACS (HACS)

SIN: 54151S (IT Pro Serv)

SIC: 8742 Mgmt Cons.

CAGE Code: 74C86

PSC/SAM: DJ01/DJ10