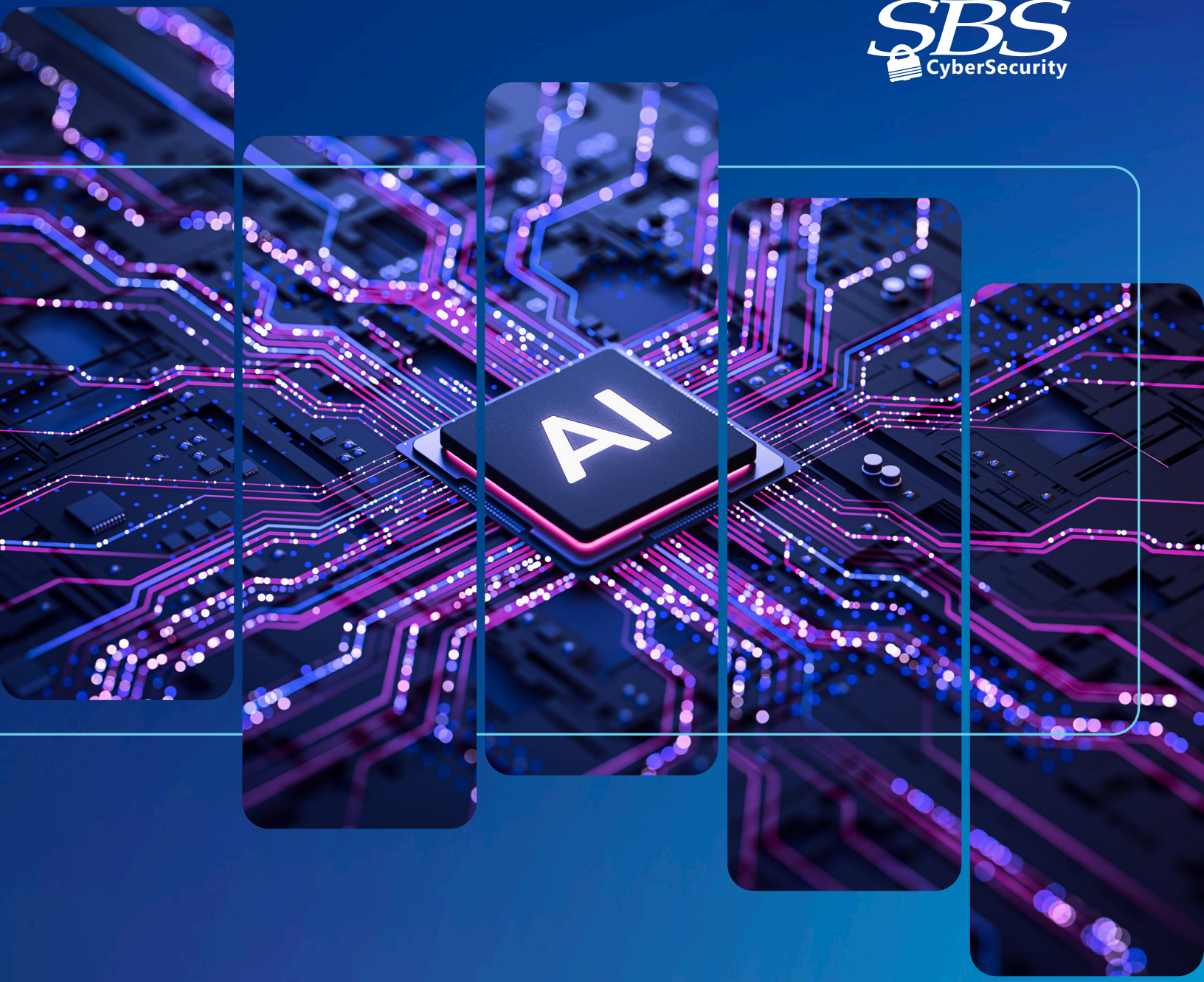
SBS CyberSecurity



AI GOVERNANCE READINESS CHECKLIST

A Practical Guide to Building Governance, Accountability, and Oversight

START WITH GOVERNANCE, Not Guesswork

Regulators are no longer asking whether financial institutions plan to use AI — they're asking whether governance, accountability, and oversight are already in place.

AI is entering organizations through vendor updates, cloud platforms, and employee experimentation, often before formal processes catch up. Without foundational governance, this creates gaps that will surface during exams, audits, and vendor reviews.

This checklist helps leaders, risk teams, and compliance staff evaluate whether foundational controls and accountability structures are in place. These basics ensure AI decisions are explainable and well-supported, enabling responsible innovation with confidence.

1 VISIBILITY AND INVENTORY

Why this matters

AI often enters institutions quietly through third-party platforms and employee workflows. Governance starts with visibility.

- Have you identified where AI exists across your organization today (including vendor tools and embedded features)?
- Do you have a process for updating that inventory as vendors add new AI capabilities?
- Can you explain how AI is currently being used if asked by an examiner?

2 EXECUTIVE OWNERSHIP AND ACCOUNTABILITY

Why this matters

Clear ownership ensures AI risks are monitored, decisions are documented, and issues are escalated appropriately. Regulators expect accountability to be explicitly defined.

- Is there a clearly named executive or role accountable for AI risk and oversight?
- Are AI responsibilities documented, not just implied?
- Do reporting and escalation paths exist for AI-related issues?

3 GOVERNANCE POLICIES AND GUARDRAILS

Why this matters

Informal or unregulated AI use, even when well-intentioned, can introduce privacy, security, or compliance risk. Policies establish boundaries and expectations for responsible use.

- Do you have written policies defining acceptable and prohibited AI use?
- Are employees given clear guidance on generative AI tools (including data handling and privacy)?
- Are policies reviewed as AI capabilities and regulations evolve?

4 DATA PROTECTION AND INFORMATION SECURITY CONTROLS

Why this matters

AI tools interact with sensitive and regulated data in new ways. Controls need to account for how data is accessed, processed, and stored to prevent exposure or misuse.

- Have you assessed how AI tools interact with sensitive or regulated data?
- Are controls in place to prevent data leakage or unauthorized data sharing?
- Does your information security program explicitly address AI-related risk?

5 VENDOR AND THIRD-PARTY RISK MANAGEMENT

Why this matters

Vendors increasingly embed AI into products and workflows. Institutions remain responsible for understanding how those features operate and ensuring appropriate oversight.

- Do you understand which vendors are using AI on your behalf and for what purpose?
- Are AI-related risks addressed during vendor due diligence and reviews?
- Do contracts and assessments reflect AI-driven processing or decision-making?

6 REGULATORY AND COMPLIANCE ALIGNMENT

Why this matters

Institutions must be able to demonstrate how AI aligns with existing regulatory requirements. Proactive involvement from compliance and legal reduces the risk of findings during exams.

- Have you mapped AI use cases to applicable regulations and guidance?
- Can you demonstrate governance, controls, and oversight during an exam?
- Are compliance, risk, and legal teams involved early in AI initiatives?

7 STRATEGIC ALIGNMENT AND ROADMAP

Why this matters

AI delivers the most value when tied to the institution's strategy. A roadmap ensures adoption is intentional, coordinated, and risk-aligned — not reactive or ad hoc.

- Is AI aligned to the institution's strategic plan?
- Do you have a prioritized, risk-aligned AI roadmap?
- Are AI decisions intentional rather than reactive?

HOW TO Interpret Your Results

CHECKED MOST BOXES

You likely have a strong foundation for scaling AI responsibly.

CHECKED SOME BOXES

You have awareness but lack structure, which is common — and fixable.

CHECKED FEW BOXES

AI may be operating without sufficient oversight, increasing regulatory and operational risk.

BRIDGE GOVERNANCE GAPS
with a vCAIO

Managing AI responsibly requires executive-level oversight — but full-time chief AI officers aren't realistic for many community banks and credit unions. SBS's Virtual Chief AI Officer (vCAIO) provides the expertise and structure to build and manage a responsible AI program without adding headcount.

A vCAIO helps institutions:

- Build an AI strategy aligned with business goals
- Establish governance, accountability, and risk management
- Train employees on responsible use
- Evaluate vendors and support AI pilot projects
- Ensure AI decisions are documented, transparent, and exam-ready

With a vCAIO in place, institutions can move forward intentionally and confidently, supported by the oversight regulators expect.

Learn how a vCAIO can help your institution manage AI responsibly.

link.sbscyber.com/vcaio

sbscyber.com