No Loose Ends

Year-End Risk Review Checklist for Financial Institutions

Before attention shifts to next year's priorities, take a closer look at what remains unfinished. Use this checklist to review your IT controls, technical defenses, and vendor oversight so you can start the new year with fewer unknowns.

Prove It

Have you independently validated your IT controls?

An IT audit helps validate that technology and security controls are designed and operating as intended, giving management and the board a clearer view of priorities.

- [ ] Our IT audit coverage reflects our institution's risk profile and audit plan.
- [ ] The scope accounts for significant changes to systems, services, and operations.
- [ ] Recommendations have been reviewed and prioritized.
- [ ] Remediation responsibilities and target dates are documented.
- [ ] Management can clearly report progress to the board or appropriate committee.

Test It

Have you evaluated your technical defenses?

Technical testing helps determine whether controls are working as intended. Network security assessments identify weaknesses so teams can prioritize remediation before year-end.

- [ ] Our current network environment has been independently assessed.
- [ ] Testing accounts for significant changes made during the year.
- [ ] Identified weaknesses have been validated and prioritized according to risk.
- [ ] Remediation actions have accountable owners and target dates.
- [ ] Leadership understands the business impact of significant technical results.

Check It

Does your vendor oversight reflect your current risk?

A vendor management review helps confirm critical providers receive appropriate oversight and that concerns are identified, escalated, and tracked.

- [ ] Vendors are classified according to risk and criticality.
- [ ] Critical and higher-risk vendors receive proportionate due diligence.
- [ ] Missing documentation, exceptions, and concerns are tracked.
- [ ] Reports help leadership identify vendor relationships requiring attention.
- [ ] Subcontractors and other important dependencies are considered.

Consider It

Has AI changed what you need to review?

AI can affect your environment through new tools, employee use, and vendor capabilities. Consider whether those changes should be reflected in your reviews.

- [ ] Approved AI tools and use cases are inventoried and risk-assessed.
- [ ] Vendor reviews address the use of AI and institutional data.
- [ ] Relevant policies, access controls, and responsibilities have been updated.
- [ ] Assessment providers understand how AI has changed the environment.

Start the New Year with Fewer Unknowns

Review your answers with the people responsible for executive oversight, compliance, risk, internal audit, technology, and information security.

If an IT audit, network security assessment, or vendor management review is still outstanding, SBS CyberSecurity can help you identify the right next step before year-end.

Schedule a year-end readiness discussion today.
sbscyber.com/2027-cybersecurity-readiness

SBS CyberSecurity