CHECKLIST
Cybersecurity Audit Readiness

Before the Audit

Internal Audit Teams

- ☐ Understand the Cybersecurity Topical Requirement.
- ☐ Update audit plans to incorporate cybersecurity risks where applicable.
- ☐ Engage InfoSec teams to identify key risks and controls.
- ☐ Review past cybersecurity audits to establish a baseline.
- ☐ Evaluate risk management processes, incident response protocols, and disaster recovery plans.
- ☐ Confirm what cybersecurity frameworks the InfoSec team is using to manage their program.
- ☐ Choose a team member to act as the primary contact with InfoSec.
- ☐ Identify any known InfoSec issues that have not been remediated to avoid redundant testing.

InfoSec Teams

- ☐ Familiarize yourself with The IIA's guidance.
- ☐ Centralize policies, SOPs, frameworks, and evidence for audits.
- ☐ Maintain an up-to-date risk register and incident management log.
- ☐ Address potential control gaps through self-assessments.
- ☐ Align priorities and expectations, including audit scope, with internal auditors.
- ☐ Choose a team member to act as the primary contact with internal audit.
- ☐ Inform any team members involved in the audit about the need to participate proactively in the audit.

Checklist: Cybersecurity Audit Readiness *cont'd*

Governance

Internal Audit Teams	InfoSec Teams
☐ Review policies, procedures, and other relevant documentation utilized by the organization to manage daily cybersecurity responsibilities. ☐ Review roles and responsibilities to support the achievement of the cybersecurity strategy. ☐ Review materials presented to the board about cybersecurity strategy, objectives, risks, and controls. ☐ Review management's cybersecurity-related communications with relevant stakeholders. ☐ Review the analysis and communication of resource requirements by management.	☐ Provide all cybersecurity-related policies and procedures to the audit team. ☐ Verify which frameworks InfoSec uses as a basis for policies and procedures (e.g., NIST CSF, COBIT, NIST 800-53), including the version or release. ☐ Provide information related to board communications, budgets, and software used in the cybersecurity program.

Risk Management

Internal Audit Teams	InfoSec Teams
☐ Review how management initially identifies cybersecurity risks. ☐ Review how management identifies risk management team members, their qualifications, positions, and evidence of cybersecurity discussions. ☐ Review the process to update policies and procedures. ☐ Review the process for risk prioritization and escalation. ☐ Review the process for managing third-party cybersecurity risks. ☐ Review the process for communicating cybersecurity operational risks.	☐ Provide current cybersecurity risk registers and assessments, along with the risk scoring methodology. ☐ Provide a roster for the risk management team, ideally for the InfoSec team and the enterprise risk management function. ☐ Provide a list of critical applications and vendors. ☐ Provide any communications related to cybersecurity risks sent to senior management, the organization, and vendors.

Checklist: Cybersecurity Audit Readiness *cont'd*

Control Activity

Internal Audit Teams	InfoSec Teams
☐ Review the cybersecurity control strategic plan. ☐ Review management's process for control evaluation. ☐ Review the cybersecurity training and awareness program. ☐ Review the SDLC process to ensure cybersecurity is considered. ☐ Review process for protecting hardware, software, and network resources. ☐ Review controls over service delivery and third parties. ☐ Review controls over communications systems. ☐ Review incident response procedures.	☐ Provide the cybersecurity strategic plan that should include budgeting, resourcing, test plans, and vendor assessment plans for the year. ☐ Provide the annual training plan and any specific training built into the development process, such as secure coding training. ☐ Provide the current list of formal, documented controls and any operating procedures for protecting hardware, software, and networks. ☐ Provide results from tabletop incident response simulations with resulting improvement plans.

After the Audit

Internal Audit Teams	InfoSec Teams
☐ Document all findings in the audit management software with owners, dates, and action plans. ☐ Establish a follow-up frequency for corrective actions. ☐ Hold a retrospective with the InfoSec team to gather ideas for continuous improvement. ☐ Ensure cybersecurity procedures are added to applicable future audits. ☐ Draft a report highlighting the cybersecurity program's strengths and areas for improvement while supporting InfoSec's plans for future maturity. ☐ Set up a recurring touchpoint meeting with the InfoSec team to discuss findings and issues from future audits.	☐ Draft realistic action plans for all audit findings with owners and implementation dates. ☐ Communicate the action plans to appropriate members of the team and leadership. ☐ Update policies and procedures based on audit results. ☐ Create a cybersecurity maturity plan that incorporates audit results and future objectives. ☐ Meet with the internal audit team regularly to gather information from their future audits.