CYBERSECURITY FOR SMALLER FINANCIAL ORGANIZATIONS

BOARD CHECKLIST: CYBERSECURITY LEADERSHIP

FUNDAMENTALS OF CYBER RISK GOVERNANCE

- ☐ As a group, periodically assess whether the board can affirmatively answer the following questions:
  - Has your organization met relevant statutory and regulatory requirements, for example, GDPR?
  - Has your organization quantified its cyber exposures and tested its financial resilience?
  - Does your organization have an improvement plan in place to ensure exposures are within your agreed-upon risk appetite?
  - Does the board regularly discuss concise, clear, and actionable information regarding the organizatoin's cyber resilience supplied by management?
  - Does your organization have incident response plans in place that have been recently dry-run exercised, including at board-level?
  - Are the roles of key people responsible for managing cyber risk clear and aligned with the three lines of defense?
  - Have you obtained independent validation and assurance of your organization's cyber risk posture, for example, via testing, certification, or insurance?
- ☐ If you cannot affirmatively answer one or more of the above, work with your CEO, CISO, relevant organization personnel, and/or external resources to correct the issue.

OVERSIGHT

- ☐ Ensure that the board is aware of its role as the ultimate responsibility-holder for your organization's cyber risk and resilience.
  - ☐ Delegate oversight to a specific board committee if deemed necessary.
- ☐ Assign one corporate officer, usually designated the chief information security officer (CISO), to be accountable for reporting on your organization's capability to manage cyber resilience and progress in implementing cyber resilience goals.
  - ☐ Ensure that this officer has regular board access, sufficient authority, command of the subject matter, experience, and resources to fulfill these duties.
- ☐ Annually define your organization's risk tolerance, ensuring it is consistent with your corporate strategy and risk appetite.
- ☐ Ensure that a formal, independent cyber resilience review of your organization is carried out annually.
- ☐ Work to integrate cyber resilience and risk assessment into your organization's overall business strategy, risk management, budgeting, and resource allocation.
- ☐ Oversee the creation, implementation, testing and ongoing improvement of cyber resilience plans, ensuring they are harmonized across your organization and that your CISO or other accountable officer regularly reports on them to the board.
- ☐ Periodically review your performance of the above and consider seeking independent advice for continuous improvement.

STAYING INFORMED

- ☐ When an individual joins the board, ensure that they have appropriate and up-to-date skills and knowledge to understand and manage the risks posed by cyber threats.
- ☐ Solicit regular advice from management on your organization's current and future risk exposure, relevant regulatory requirements, and industry and societal benchmarks for risk appetite. Plan to engage in:
  - Regular briefings on duties created by new regulations and legislation,
  - Board and executive committee joint planning and visits to best practice peers and leaders in cybersecurity,
  - Security briefings on the threat environment, and
  - Board-level exchanges of information on governance and reporting.
- ☐ Make clear to management that they are accountable for reporting a quantified and understandable assessment of cyber risks, threats, and events as a standing agenda item during board meetings.
- ☐ Regularly check in with management and other relevant personnel about developments related to ongoing systemic challenges such as supply chain vulnerabilities, common dependencies, and the gap in information sharing between boards on cyber risk governance.

SETTING THE TONE

- ☐ Ensure that staff at all levels recognize that they each have important responsibilities to ensure your organization's cyber resilience.
- ☐ Oversee management's role in fostering and maintaining your organization's risk culture. Regularly assess the effectiveness of your organization's risk culture, considering the impact of culture on safety and soundness and making changes where necessary.
- ☐ Make clear that you expect all staff to act with integrity and to promptly escalate observed non-compliance within or outside your organization.