小型组织的网络安全

董事会检查清单：网络安全领导层

网络风险治理基本原则

- □ **作为集团，定期评估董事会是否能够肯定回答以下问题：**
  - 您的组织是否符合相关法定和监管要求，例如 GDPR？
  - 贵组织是否已经量化其网络暴露风险并测试其金融弹性？
  - 贵组织是否已经制定了改善计划，确保暴露风险在您约定的风险偏好之内？
  - 董事会是否定期讨论管理层提供的有关该组织网络弹性的简明、清楚和可采取行动反馈的信息？
  - 贵组织是否已经制定了事故响应计划，且最近已进行试运行演练，包括在董事会层面的演练？
  - 负责管理网络风险的关键员工的职责是否清晰，且与“三道防线”一致？
  - 您是否已就贵组织的网络风险态势取得独立的确认和保证，例如通过测试、证明或保险取得？
- □ **如果您无法肯定回答一个或多个以上问题，与您的首席执行官 (CEO)、首席信息安全官 (CISO)、相关组织人员和/或外部资源纠正该问题。**

监督

- □ **确保董事会知悉其是组织网络风险和弹性的最终责任人。**
- □ **如果必要，将监督责任委托给具体的董事会委员会。**
- □ **指定一名企业高级管理人员，通常指定为首席信息安全官 (Chief Information Security Officer, CISO) 负责汇报贵组织管理网络弹性的能力以及网络弹性目标的实施进展。**
- □ **确保该高级管理人员具备完成该等职责所需的参加常规董事会的权限、充分权限、标的控制权、经验和资源。**
- □ **每年确定贵组织的风险容忍度，确保其符合您的企业战略和风险偏好。**
- □ **确保每年对贵组织进行正式的、独立网络弹性审核。**
- □ **努力将网络弹性和风险评估纳入贵组织的整体业务战略、风险管理、预算和资源配置中。**
- □ **定期审核第三方风险。**
- □ **监督整个组织网络弹性计划的制定、实施、测试和持续改善情况，确保协调发展，且您的 CISO 或其他负责人定期向董事会报告相关情况。**
- □ **定期审核上述措施的实施情况，并考虑寻求独立建议，以持续改善。**

始终掌握情况

- □ 个人加入董事会时，确保其具备理解和管理网络威胁所带来的风险的适当能力和最新技能和知识。
- □ 就贵组织目前和未来的风险暴露、相关监管要求和风险偏好的行业和社会基准定期征询管理层的建议。计划从事：
  - 就新法规和立法产生的职责定期提供简报。
  - 董事会和执行委员会联合规划，访问网络安全届最佳从业人员和领军人物。
  - 有关威胁环境的安全简报，以及
  - 董事会层面有关治理和汇报的信息交流。
- □ 向管理层清晰表明，它们负责报告对网络风险、威胁和事件作量化和可理解的评估，作为董事会会议的常规议程。
- □ 定期与管理层和其他相关工作人员讨论有关持续存在的系统性难题的最新情况，例如供应链的薄弱环节、常见的依赖关系和信息共享上的差距。

设定语调

- □ 确保所有级别员工认可他们每个都有确保贵组织的网络弹性的重要责任。
- □ 监督管理层在培养和维护贵组织风险文化方面的职责。定期评估贵组织风险文化的有效性，考虑文化对安全和稳健性的影响，并在必要时作出改变。
- □ 明确您期望所有员工基于诚信行动，并及时上报在贵组织内外发现的不合规行为。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org