

# 董事会层面指南:网络安全领导人

## 监督

作为贵组织的最高领导层,董事会对治理网络风险承担最终责任,因此必须监督组织在该领域的策略、政策和活动。具体而言,董事会应当:

- 对网络风险的弹性的监督承担最终责任,不管是以整体董事会的形式还是通过向特定的董事会委员会委托监督的形式。
- 指定一名企业高级管理人员,通常指定为首席信息安全官(CISO),负责汇报贵组织管理网络弹性的能力以及实施网络弹性目标的进展。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,确保其符合贵企业的战略和风险偏好。
- 确保每年对贵组织进行正式的、独立网络弹性审核。
- 监督网络弹性计划的制订、实施、测试和持续改进,确保在贵组织保持一致,且您的 CISO 或者其他负责任的高级职员定期就该等事项向董事会报告。
- 将网络弹性和风险评估融入贵组织的总体业务策略、风险管理、预算和资源分配,目标是将网络风险完全融入整体操作风险。定期审核第三方风险。
- 定期审核上述措施的实施情况,并考虑实现持续改善的独立建议。

## 不断了解情况

董事会有效的网络风险监督取决于成员对主题和最新信息的掌控情况。

- 确保参加董事会的所有个人具有理解和管理网络威胁所造成风险的适当和最新的技能与知识。
- 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。而且,就威胁的格局和监管环境、联合规划和访问网络安全最佳从业人员和领军人物以及在董事会层面进行的有关治理和报告的交流,参加有关最新动态的定期简报工作。
- 让管理层负责报告定量和可理解的网络风险、威胁和事故评估,将其作为董事会会议期间的常设议程项目。
- 不断意识到持续的系统性挑战,例如供应链薄弱环节、共同依赖以及信息分享方面的薄弱环节。

## 设定语调

董事会必须与高级管理层设定并示范贵组织的核心价值观、风险文化和关于网络弹性的预期。

- 提倡一种文化氛围,其中各级员工认识到他们在确保贵组织网络弹性方面的重要责任。以身作则。
- 监督管理层在培养和维护贵组织风险文化方面的职责。提倡、监督和评估风险文化,考虑文化对安全和稳健性的影响并在必要时作出变更。
- 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。

## 网络风险治理基本原则

确认您可以肯定地回答以下问题:

1. 贵组织是否符合相关法定和监管规定?
2. 贵组织是否已经量化其网络暴露风险并测试其金融弹性?
3. 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?
4. 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?
5. 贵组织是否已经制定了应急响应计划,且最近已进行试运行演练,包括在董事会层面的演练?
6. 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?
7. 您是否已就贵组织的网络风险态势取得独立的验证和保证?