联合国工业发展组织

Distr.: General
20 September 2024
Chinese
Original: English

工业发展理事会
第五十二届会议
2024 年 11 月 25 日至 27 日，维也纳
临时议程项目 4(f)
总体风险管理

总体风险管理的最新情况

总干事的报告

方案和预算委员会在 2016/8 号结论中，“邀请总干事向工业发展理事会下届会议和方案和预算委员会下届会议报告工发组织总体风险管理战略的情况，并提出综合性措施，处理成员国退出本组织在财务和行政管理方面造成的影响，目的包括扭转退出趋势。”

本文件对在方案和预算委员会第四十届会议上提交的报告（IDB.52/9-PBC.40/9）作了更新，重点介绍在机构服务与运维总司下新设立的专门的风险管理和合规股，包括与网络安全有关的其他职能。

一. 导言

1. 随着经调整的《2024 年工发组织秘书处结构》（DGB/2024/03）的颁布，工发组织设立了风险管理和合规股。新单位向作为指定的工发组织机构风险管理协调人的机构服务与运维总司司长提供支持，促进制定、协调和实施工发组织的机构风险管理和信息安全风险框架。该股还积极支持高级管理层培养稳健的风险文化。除了风险管理和合规职能外，该股的任务还涉及网络安全治理。

2. 本文件重点介绍工发组织为管理和减少网络安全风险威胁而采取的行动。

请回收

二. 网络安全框架和强化措施

3. 根据联合检查组（联检组）在其题为“联合国系统各组织的网络安全”的报告（JIU/REP/2021/3）中提出的建议，工发组织全面概述了与其网络安全框架有关的已实施措施。该概要载于 IDB.52/CRP.14 号会议室文件，概述了为保护本组织免受网络威胁并确保实施强有力的安全做法而采取的关键要素和行动。

4. 工发组织在加强其网络安全框架方面取得了实质性进展，使其符合外聘审计员、联检组提出的建议和行业最佳做法。本组织通过《工发组织信息安全政策》（DGB/2023/01）以及描述确保以有效、及时和结构化的方式查明、评估、管理和减缓信息安全风险的流程的《关于信息安全风险管理流程的行政指示》（AI/2024/01），确定了治理框架并建立了信息安全管理系统（符合 ISO 27001），从而奠定了坚实的网络安全基础。

5. 随着工发组织的发展，必须针对网络安全问题维持积极主动的做法。这包括不断重新评估风险，提高技术能力，并在整个组织内培养网络安全意识文化。通过这些努力，工发组织不仅将有能力应对不断变化的网络威胁和保护其信息资产，而且还将以韧性和信心支持其更广泛的使命。

6. 在方案和预算委员会第四十届会议上提交了外聘审计员关于工发组织 2023 年 1 月 1 日至 12 月 31 日财政年度账目的报告（IDB.52/4-PBC.40/4），外聘审计员在报告中确认工发组织在网络安全方面取得进展，落实了所有五项建议，重点是设立专门的网络安全职能、开发信息安全管理系统和实施漏洞管理程序。外聘审计员查明的关键技术漏洞也已得到处理和纠正，工发组织在外部专业公司的支持下牵头进行的 2023 年安全渗透测试发现了更多问题，这些问题已列入数字化、创新和技术合作优化服务工作计划。2023 年进行的信息安全风险评估还确定了关键资产和风险，从而制定了 2023-2024 年信息安全风险处理综合计划，该计划包括 35 项活动，其中 15 项已经完成，其余活动正在进行中。本文件附件对这些活动进行了高度概括。活动成果证实，工发组织的网络安全职能在主动查明和管理风险以及加强本组织的安全和韧性方面是有效的。

7. IDB.52/CRP.14 号会议室文件对本文件作了补充，其中介绍了有助于提高本组织网络韧性的程序。

三. 需请理事会采取的行动

8. 理事会似宜注意到本文件所载信息。

附件

2023-2024 年信息安全风险处理计划的活动现状

已完成的活动

1. 渗透测试：聘请外部承包商进行全面的渗透测试，模拟具有内部访问权限的攻击者。这促成了完善控制措施，并将新活动纳入风险处理计划。

2. 对在线交流实施最新身份验证措施：对 Exchange Online 实施最新身份验证措施，加强电子邮件安全。

3. 停用 xFiles 文件共享系统：成功停用工发组织遗留的文件共享系统，并实施了基于 Microsoft 365（OneDrive）的现代共享解决方案，减少了受攻击面。

4. 改进 Microsoft Teams 的身份验证：实施 Teams 多重身份验证，降低凭据被盗风险。

5. 改进密码政策：制定并实施涵盖全面密码政策、配置和合规监控的新程序。

6. 改进身份验证、用户体验和安全性：过渡到基于 Microsoft 365 Azure AD 的单一登录，加强监控、韧性和可用性。

7. 为云系统实施多重身份验证：为所有使用云认证的服务启用多重身份验证，加强安全性。

8. 漏洞管理工具和流程：实施了漏洞管理工具，涵盖公共访问系统、关键服务器和管理员工作站等关键资源。根据外聘审计员的建议和最佳做法，还制定了额外的流程和程序。

9. 加强合规监测：根据联合国最低基线和微软最佳做法，改进对关键网络安全控制的合规监测。

10. 提高 Microsoft 365 系统的安全性：为特定 Microsoft 365 系统实施无缝单一登录，改善用户体验和安全性。

11. 对信息技术管理员进行内部专门培训：对信息技术管理员进行内部交叉培训，并为特权用户提供专门课程。

12. 审查外地办事处文件存储：完成了权限审查，并评价了将外地办事处共享迁移到 Teams 以提高安全性的问题。

13. 改进安全流程和政策：加强与访问权限、职责分工和安全配置有关的流程和政策，减少偏离标准做法的情况。

14. 优化信息安全流程：采用并调整当前信息安全方面的最佳做法，优化本组织的安全态势。

15. Teams 安全审查：审查 Teams 内部的安全设置和权限。

进行中的活动

16. 根据“需要知道”和“最低权限”原则审查账户：持续审查特权账户和服务账户、文件共享访问权限，并实施本地管理员密码解决方案等措施。

17. 实施凭据保护：正在服务器和端点上实施凭据保护安全功能，加强安全性，并降低凭据泄露的风险。

18. 在整个工发组织实施最新密码政策：根据最新密码政策程序更新密码政策和特权访问。

19. 改进补丁管理：正在努力完善补丁管理和补救流程。

20. 提高 SAP 安全性：正在采取措施处理审计发现的问题，改善 SAP 系统内的安全健康状况。

21. 改进防火墙：正在进行强化工作，包括实施零信任和全面审查防火墙架构、管理和安全政策。

22. 更换信息技术管理员密码管理工具：正在更换过时的信息技术管理员密码管理工具。

23. 零信任成熟度评估：正在对零信任成熟度进行全面评估，指导今后的改进工作。

24. 停用/替换遗留系统：持续努力停用和替换遗留系统，减少受攻击面。

25. 改进安全事件响应：正在利用内部和外部资源加强事件响应流程和工具。

26. SAP 关键控制监测：根据外聘审计员的建议，正在对 SAP 和辅助流程中的关键控制措施进行合规监测。

27. 机构资源规划系统信息技术职责分工：根据外聘审计员的建议，在资源允许的情况下，正在加强 SAP 系统信息技术的职责分工。

28. 管理员个性化账户：正在为各系统信息技术管理员实施个性化和隔离账户。

29. 试行无密码认证：正在评价和试行创新的无密码认证方法，加强安全性，同时简化访问。

3-. 审查外地办事处的互联网供应商：正在审查外地办事处互联网服务的质量和带宽。

31. 加强与外部伙伴的合作：正在探索与外部伙伴合作的机会，以便满足专业知识和安全需求。

32. 制定零信任路线图：正在根据业务优先事项和风险概况制定零信任路线图。

33. 为所有可公开访问的服务提供多重身份验证：正在对所有外部访问和特权访问实施多重身份验证。

34. 改进资产管理和发现：正在努力加强资产管理和发现工具，包括扩大服务器库存和完善补丁部署。

35. 考虑灾难恢复站点：正在规划灾难恢复和数据备份第二站点，确保业务连续性。