United Nations Industrial Development Organization

Distr.: General
20 September 2024

Original: English

Industrial Development Board
Fifty-second session
Vienna, 25–27 November 2024
Item 4 (f) of the provisional agenda
General risk management

Update on general risk management

Report by the Director General

In its conclusion 2016/8, the Programme and Budget Committee "invited the Director General to report to the next sessions of the Industrial Development Board and the Programme and Budget Committee on UNIDO's general risk management strategy and suggest comprehensive measures for addressing the financial and administrative impact of Member States leaving the Organization including with a view to reversing the trend of withdrawal."

The present document provides an update to the report presented at the fortieth session of the Committee (IDB.52/9-PBC.40/9), highlighting the establishment of a new dedicated Risk Management and Compliance Unit, under the Directorate of Corporate Services and Operations, including additional functions related to cybersecurity.

I. Introduction

1. With the promulgation of the adjusted UNIDO Secretariat Structure 2024 (DGB/2024/03), UNIDO established the Risk Management and Compliance Unit. The new Unit supports the Managing Director of the Directorate of Corporate Services and Operations, as the designated UNIDO enterprise risk management (ERM) focal point, to further develop, coordinate and implement UNIDO's ERM and information security risk frameworks. It also actively supports senior management to foster a robust risk culture. In addition to the risk management and compliance functions, the Unit's mandate relates to cybersecurity governance.

2. This document highlights the actions taken by UNIDO to manage and reduce the threat of cybersecurity risks.

II. Cybersecurity framework and enhancements

3. In response to the Joint Inspection Unit's (JIU) recommendation contained in its report, entitled "Cybersecurity in the United Nations system organizations" (JIU/REP/2021/3), UNIDO presents a comprehensive overview of implemented

measures related to its cybersecurity framework. The overview, contained in conference room paper IDB.52/CRP.14, outlines the critical elements and actions taken to protect the Organization from cyber threats and to ensure that robust security practices are implemented.

4. UNIDO has made substantial progress in reinforcing its cybersecurity framework, aligning it with recommendations from the External Auditor, JIU and industry best practices. The Organization has established a solid cybersecurity foundation by defining the governance framework and establishing the information security management system (aligned with ISO 27001) through the UNIDO Information Security Policy (DGB/2023/01), as well as the Administrative Instruction on the Information Security Risk Management Process (AI/2024/01) which describes the process to ensure that information security risks are identified, assessed, managed, and mitigated in an effective, timely and structured manner.

5. As UNIDO progresses, it is crucial to maintain a proactive approach to cybersecurity. This includes continuously reassessing risks, enhancing technical capabilities and fostering a culture of cybersecurity awareness throughout the Organization. Through these efforts, UNIDO will not only be equipped to counter evolving cyber threats and safeguard its information assets, but also support its broader mission with resilience and confidence.

6. In the report of the External Auditor on the accounts of UNIDO for the financial year 1 January to 31 December 2023 (IDB.52/4-PBC.40/4), presented at the fortieth session of the Programme and Budget Committee, the External Auditor validated UNIDO's progress in cybersecurity by closing all five recommendations, focusing on establishing a dedicated cybersecurity function, developing the Information Security Management System and implementing a vulnerability management process. Critical technical vulnerabilities identified by the External Auditor have also been addressed and corrected, and a 2023 security penetration test led by UNIDO with the support of specialized external companies revealed additional issues that have been included in the Digitalization, Innovation and Technical Cooperation Optimization Services workplan. An information security risk assessment performed in 2023 also identified key assets and risks, leading to a comprehensive 2023–2024 information security risk treatment plan, which includes 35 activities, of which 15 have been completed and the rest are in progress. A high-level overview of these activities is presented in the annex to this document. The results confirm the effectiveness of UNIDO's cybersecurity function in proactively identifying and managing risks, as well as enhancing the security and resilience of the Organization.

7. The present document is supplemented by conference room paper IDB.52/CRP.14, which describes the processes contributing to improve the Organization's cyber resilience.

III. Action required of the Board

8. The Board may wish to take note of the information contained in the present document.

Annex

Status of activities from the 2023–2024 information security risk treatment plan

Completed activities

1. Penetration testing: engaged an external contractor to perform thorough penetration testing to simulate an attacker with internal access. This led to the refinement of controls and the inclusion of new activities in the risk treatment plan.

2. Enforce modern authentication for exchange online: implemented modern authentication for Exchange Online to enhance email security.

3. Decommission the xFiles file-sharing system: successfully decommissioned the UNIDO legacy file-sharing system and implemented a modern sharing solution based on Microsoft 365 (OneDrive), reducing the attack surface.

4. Improve authentication for Microsoft Teams: implemented multi-factor authentication for Teams to mitigate credential theft risks.

5. Improve password policies: developed and enforced new procedures covering comprehensive password policies, provisioning and compliance monitoring.

6. Improve authentication, user experience and security: transitioned to Single Sign-On (SSO) based on Microsoft 365 Azure AD, enhancing monitoring, resilience and availability.

7. Implement multi-factor authentication for cloud systems: enabled multi-factor authentication for all services utilizing cloud authentication to bolster security.

8. Vulnerability management tool and process: implemented a vulnerability management tool covering critical resources such as public-facing systems, critical servers and administrator workstations. An additional process and procedure have also been developed, in line with recommendations from the External Auditor and best practices.

9. Enhance compliance monitoring: improved compliance monitoring of key cybersecurity controls, aligning with the United Nations minimum baseline and Microsoft best practices.

10. Improve security for Microsoft 365 systems: implemented Seamless SSO for selected Microsoft 365 systems, improving user experience and security.

11. Internal dedicated training for information technology (IT) administrators: conducted internal cross-training for IT administrators and provided specialized courses for privileged users.

12. Review field office file storage: completed a review of permissions and evaluated migrating field office shares to Teams for improved security.

13. Improve security processes and policies: enhanced processes and policies related to access rights, segregation of duties and secure configurations, reducing deviations from standard practices.

14. Optimize information security processes: adopted and adapted current best practices in information security to optimize the Organization’s security posture.

15. Teams security review: conducted a review of security settings and permissions within Teams.

In-progress activities

16. Review accounts based on need-to-know and least privilege principle: continued review of privileged and service accounts, file share access rights and implementing measures such as local administrator password solution.

17. Implement credential guard: implementation of the Credential Guard security feature on both servers and endpoints is under way to enhance security and reduce the risk of credential compromise.

18. Implement latest password policies across UNIDO: update of the password policies and privileged access based on the updated password policy procedures.

19. Patch management improvements: ongoing efforts aim to refine patch management and remediation processes.

20. Improve SAP security: measures are being implemented to address audit findings and improve security hygiene within the SAP system.

21. Firewall improvements: enhancements including zero trust implementation and a full review of the firewall architecture, management and security policies are in progress.

22. Replace password management tool for IT administrators: in the process of replacing the outdated password management tool for IT administrators.

23. Zero trust maturity assessment: comprehensive assessment of the zero trust maturity is being conducted to guide future improvements.

24. Decommission/replace legacy systems: ongoing efforts to decommission and replace legacy systems to reduce the attack surface.

25. Improve security incident response: strengthening incident response processes and tools with both in-house and external resources is under way.

26. Key control monitoring for SAP: implementing compliance monitoring for key controls within SAP and supporting processes is in progress, in line with External Auditor recommendations.

27. Segregation of duties in IT for the enterprise resource planning system: enhancing segregation of duties within IT for SAP is ongoing as resources allow and in line with External Auditor recommendations.

28. Personalized accounts for administrators: implementation of personalized and separated accounts for IT administrators across various systems is progressing.

29. Pilot passwordless authentication: evaluating and piloting innovative passwordless authentication methods to enhance security while simplifying access is in progress.

30. Review Internet suppliers at field offices: reviewing the quality and bandwidth of Internet services at field offices is ongoing.

31. Enhance cooperation with external partners: exploring opportunities to collaborate with external partners for specialized knowledge and security needs is in progress.

32. Develop zero trust road map: developing a zero trust road map aligned with business priorities and risk profiles is ongoing.

33. Multi-factor authentication for all publicly accessible services: implementing multi-factor authentication for all external and privileged access is in progress.

34. Improve asset management and discovery: efforts to enhance asset management and discovery tools are in progress, including expanding server inventory and refining patch deployment.

35. Consider disaster recovery site: planning for a secondary disaster recovery and data backup site to ensure business continuity is under way.