UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

AUDIT

OF

MANAGEMENT OF MICROSOFT AZURE

IN

UNDP

Report No. 2411

Issue Date: 1 November 2021

Report on the management of Microsoft Azure in UNDP
Executive Summary

The UNDP Office of Audit and Investigations (OAI) conducted an audit of the management of the Microsoft Azure cloud computing platform (MS Azure) from 9 June to 6 August 2021. The audit aimed to assess the adequacy and effectiveness of the governance, risk management and control processes relating to the following areas and sub-areas:

(a) Governance
(b) Network configuration and management
(c) Access management
(d) Resource security
(e) Monitoring

The audit covered the activities regarding MS Azure from 1 January 2020 to 31 May 2021. This was the first audit of MS Azure in UNDP.

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*. Due to the COVID-19 pandemic, the audit was conducted remotely. Scope limitations due to the nature of the remote audit related to the following activities:

Meetings with all parties involved in the audit were carried out virtually, which limited the audit team's understanding of auditees' working environment.

Overall audit rating

OAI assessed the Office's performance as **satisfactory/some improvement needed**, which means "The assessed governance arrangements, risk management practices and controls were generally established and functioning, but need some improvement. Issues identified by the audit do not significantly affect the achievement of the objectives of the audited entity/area."

Key recommendations: Total = **4,** high priority = **1**

The four recommendations aim to ensure the following: (a) effectiveness and efficiency of operations (Recommendations 1, 2, and 4); and (b) safeguarding of assets (Recommendation 3).

For high (critical) priority recommendations, prompt action is required to ensure that UNDP is not exposed to high risks. Failure to take action could result in major negative consequences for UNDP. The high (critical) priority recommendation is presented below:

Operating system critical vulnerabilities not automatically deployed to installed virtual machines (Issue 3)	Azure Update Management service in the UNDP MS Azure environment was not configured and no automatic patching was implemented on the Virtual Computer Systems (Machines) used by various UNDP units.

Management comments and action plan

The Chief Technology Officer accepted all four recommendations and is in the process of implementing them. Comments and/or additional information provided have been incorporated in the report, where appropriate.

Low risk issues (not included in this report) have been discussed directly with management and actions have been initiated to address them.

Helge
Osttveiten
2021.11.01
09:54:39 -04'00'

Helge S. Osttveiten
Director
Office of Audit and Investigations