AUDIT

OF

MANAGEMENT OF MICROSOFT AZURE

IN

UNDP

Report No. 2411
Issue Date: 1 November 2021
# Table of Contents

Executive Summary                               i  
I. About Microsoft Azure                        1  
II. Audit results                              1  
   A. Governance                                2  
   B. Resource security                        3  
   C. Monitoring                                4  
Definitions of audit terms - ratings and priorities 6
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
Director
Office of Audit and Investigations
I. About Microsoft Azure

Microsoft Azure (MS Azure) is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. It provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) cloud services.

MS Azure delivers computing services over the Internet by using a pay-as-you-go pricing model. It allows users of the services to lower operating costs, run their infrastructures more efficiently, and scale services based on their business needs.

UNDP started using cloud computing for enterprise services in 2014 when Microsoft Office 365 was rolled out as the enterprise cloud solution. During 2015-2016, additional Microsoft cloud tools were implemented including SharePoint 2013, Yammer, and Azure services for hosting Internet applications. In the beginning of 2016 MS Azure resources became available to UNDP Country Offices. As of June 2021, UNDP relocated most of its IT solutions and services previously hosted on-premises to the MS Azure cloud computing platform. UNDP utilizes a shared responsibility model, where core aspects of MS Azure are managed by Microsoft and resource management is handled by UNDP, specifically by the Office of Information and Technology Management (ITM). As of June 2021, ITM managed more than 100 MS Azure subscriptions covering more than 300 cloud resources, including virtual computer systems (virtual machines), databases, and applications, with an average monthly cost of $65,000.

II. Audit results

Satisfactory performance was noted in the following areas:

(a) **MS Azure network configuration and management**: ITM utilizes recommended MS Azure network security controls, which improve protection of the cloud resources from unauthorized access.

(b) **MS Azure access management**: Access to the MS Azure environment is well managed, user access is limited and based on the level of access required to perform their functions. ITM has applied recommended security policies for Azure Identity and Access Management (IAM) that helps to protect access to MS Azure applications and resources.

OAI made one recommendation ranked high (critical) and three recommendations ranked medium (important) priority.

Low priority issues/recommendations were discussed directly and agreed with the Office and are not included in this report.

**High priority recommendations**, arranged according to significance:

(a) Enable MS Azure Update Management service and perform periodical security scans of the server resources (Recommendation 3).

**Medium priority recommendations**, arranged according to significance:

(a) Review security and operational requirements for the organizational resources and where applicable create UNDP specific policies in MS Azure (Recommendation 1).

(b) Develop guidance related to areas of cloud resources design, aimed at helping organizational units improve their use of the MS Azure environment (Recommendation 2).

(c) Design and implement a MS Azure monitoring strategy and develop tools to support organizational users in monitoring their cloud resources (Recommendation 4).
The detailed assessment is presented below, per audit area

A. Governance

**Issue 1**  Suboptimal usage of MS Azure Policy tool for managing UNDP’s MS Azure resources

MS Azure includes a tool (Azure Policy) that allows users managing their MS Azure environment to create, assign, and manage policies. These policies apply and enforce rules that organizational resources need to follow to stay compliant with internal standards and service-level agreements. The policies can enforce these rules when resources are created and can be used to evaluate existing resources to give better insight into the compliance with internal standards. Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management of resources. Recommended policy definitions for these common use cases are developed by Microsoft based on best industry practices and are provided / set-up by default when resources are created.

ITM had adopted these standard Azure policies without major modifications, meaning when ITM created new resources the standard policies as defined by Microsoft would apply. As a result, the standards enforced in the UNDP MS Azure environment were not fully aligned with UNDP needs and requirements. The policy controls generated alerts which were not applicable to UNDP resources due to irrelevant compliance requirements (e.g., Payment Card Industry Data Security Standard [PCI DSS] and System and Organization Controls Trust Services Principles and Criteria [SOC TSP] regulatory standards).

<table>
<thead>
<tr>
<th>Priority</th>
<th>Medium (Important)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendation 1:</strong></td>
<td></td>
</tr>
<tr>
<td>The Office of Information and Technology Management should review security and operational requirements for the organizational resources created in the Microsoft Azure environment and where applicable configure UNDP specific policies in Ms Azure.</td>
<td></td>
</tr>
</tbody>
</table>

| Management action plan: |
| The Office of Information and Technology Management agrees with the recommendation and will develop specific policies on cloud security and operations. |

| Estimated completion date: | September 2022 |

**Issue 2**  Lack of formal guidance for the organizational users of the UNDP MS Azure services

Considering the fact that ITM is ISO 9000 certified, business processes have to be formally documented and documentation has to be updated on a regular basis. Documenting MS Azure processes will ensure consistency, efficiency, and standardization. It will also allow organizational users following them to perform at their best and deliver expected results.

ITM had developed plans and procedures for business-critical MS Azure services (including, but not limited to, change management, and incident response). However, the documentation did not cover the full implementation cycle of cloud computing initiatives, including common considerations such as resource implementation, information security risks, compliance, data location, and records management.
The consequences of incomplete documentation may include inefficiencies in cloud usage, higher costs for cloud resources and compromised safety.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Medium (Important)</th>
</tr>
</thead>
</table>

**Recommendation 2:**

The Office of Information and Technology Management should develop guidance related to areas of cloud resources design, requirements, implementation, monitoring, and end-user roles and responsibilities, aimed at helping the organizational units to lower operating costs, run their infrastructure more efficiently, and scale their business needs on demand.

**Management action plan:**

The Office of Information and Technology Management agrees with the recommendation and will strengthen its guidance to provision and manage cloud resources.

**Estimated completion date:** June 2022

### B. Resource security

**Issue 3**  
Operating system critical vulnerabilities not automatically deployed to installed virtual machines

ITM recognized that an effective software update management process is necessary to maintain operational efficiency, overcome security issues, and reduce the risks of increased cyber security threats. Furthermore, best practices suggest that 'Critical' and 'Security' software patches shall be checked for availability on a predefined schedule and, once available, automatically applied to virtual machines (VMs) hosted in the MS Azure environment.

Azure Update Management enables the installation of virtual machine patches to be executed on a routine schedule set by the enterprise with a great degree of customization and flexibility to target individuals or resource groups. Azure Security Center can also be used to identify VMs that are missing patches or are not adhering to patch update requirements.

At the time of the audit, the Azure Update Management service in the UNDP MS Azure environment was not configured and no automatic patching was implemented on the VMs used by various UNDP units.

Failure to apply software patches in a timely and consistent manner significantly increases the chances that attackers gain access to UNDP computers and systems, exploiting vulnerabilities the patches are meant to address.
Priority: High (Critical)

Recommendation 3:

The Office of Information and Technology Management should:

(a) enable Azure Update Management service on existing and newly created Virtual Machines;
(b) schedule a patch deployment that aligns with the release schedule and service window;
(c) monitor deployment status on a periodic basis; and
(d) perform periodical security scans of the server resources to identify Virtual Machines that are missing patches or are not adhering to patch update requirements.

Management action plan:

The Office of Information and Technology Management agrees with the recommendations and will:

(a) if ICT recurring costs receive adequate funding, test and enable Update Management for Azure;
(b) implement an appropriate deployment schedule;
(c) monitor development status; and
(d) study, test and implement the most adequate solution (Security Center or Update Management or Automatic VM guest patching).

Estimated completion date: October 2022

C. Monitoring

Issue 4  Lack of formal monitoring program for MS Azure cloud resources

Proper monitoring of MS Azure cloud resources allows timely identification and resolution of issues such as security risks, poor performance and system failures.

Sixty percent of UNDP cloud resources used decentralized monitoring, meaning that organizational users could access and analyse all logs in their cloud assets. However, there was no guidance to ensure consistent log analysis by the users (e.g., unified set of metrics or Azure dashboard templates). Furthermore, ITM recently started using the Microsoft Azure Sentinel solution, which allowed for the setup of a central log repository where all logs are combined, but at the time of the audit ITM did not have a clear strategy which logs should be reviewed.

A decentralized approach to monitoring can result in difficulties obtaining a holistic view on events happening in all organizational assets and in the inability to derive correlations (e.g., comparing issues in different resource groups), potentially leading to additional costs for the organization by not addressing (preventable) issues in a timely fashion.
<table>
<thead>
<tr>
<th>Priority</th>
<th>Medium (Important)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendation 4:</strong></td>
<td></td>
</tr>
<tr>
<td>The Office of Information and Technology Management should:</td>
<td></td>
</tr>
<tr>
<td>(a) design and implement a MS Azure monitoring strategy that performs end-to-end monitoring across organizational infrastructure, which should be growth-oriented, and aligned with the organizational business needs; and</td>
<td></td>
</tr>
<tr>
<td>(b) develop tools to support organizational users in monitoring their cloud resources (e.g., dashboard templates, sets of metrics, instructions, etc.).</td>
<td></td>
</tr>
<tr>
<td><strong>Management action plan:</strong></td>
<td></td>
</tr>
<tr>
<td>The Office of Information and Technology Management agrees with the recommendations and will:</td>
<td></td>
</tr>
<tr>
<td>(a) design and implement a MS Azure monitoring strategy that performs end-to-end monitoring across organizational infrastructure; and</td>
<td></td>
</tr>
<tr>
<td>(b) develop tools and guidelines to support organizational users in monitoring their cloud resources</td>
<td></td>
</tr>
<tr>
<td><strong>Estimated completion date:</strong> September 2022</td>
<td></td>
</tr>
</tbody>
</table>
Definitions of audit terms - ratings and priorities

A. AUDIT RATINGs

- Fully Satisfactory
  The assessed governance arrangements, risk management practices and controls were adequately established and functioning well. Issues identified by the audit, if any, are unlikely to affect the achievement of the objectives of the audited entity/area.

- Satisfactory / Some Improvement Needed
  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.

- Partially Satisfactory / Major Improvement Needed
  The assessed governance arrangements, risk management practices and controls were established and functioning, but need major improvement. Issues identified by the audit could significantly affect the achievement of the objectives of the audited entity/area.

- Unsatisfactory
  The assessed governance arrangements, risk management practices and controls were either not adequately established or not functioning well. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area.

B. PRIORITIES OF AUDIT RECOMMENDATIONS

- High (Critical)
  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.

- Medium (Important)
  Action is required to ensure that UNDP is not exposed to risks. Failure to take action could result in negative consequences for UNDP.

- Low
  Action is desirable and should result in enhanced control or better value for money. Low priority recommendations, if any, are dealt with by the audit team directly with the Office management, either during the exit meeting or through a separate memo subsequent to the fieldwork. Therefore, low priority recommendations are not included in this report.