



INTERNAL AUDIT DIVISION

REPORT 2025/087

Audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees

**UNHCR needed to strengthen the Cloud
governance framework and ensure its
provisions are implemented to improve
efficiency and achieve more cost-effective
cloud operations**

29 December 2025

Assignment No. AR2025-166-01

Audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees (UNHCR). The objective of the audit was to assess the adequacy and effectiveness of the governance, risk management and control processes for efficient and effective provision of cloud services at UNHCR. The audit covered the period from October 2023 to September 2025 and included: (a) framework to govern the cloud environment; (b) operational effectiveness of cloud services; (c) procurement and contracting of cloud services; and (d) cloud asset management.

UNHCR's transition to cloud-based infrastructure introduced both opportunities and risks, underscoring the need for UNHCR to update its IT strategy and Cloud Framework to reflect evolving cloud environments and provide adequate guidance to stakeholders. Further, cloud vendor selection criteria had inherent biases that contributed to vendor lock-in and inflexible contracting practices, which together resulted in UNHCR's inability to adjust its cloud expenditures as operational activity reduced. Also, UNHCR's inability to enforce controls in the decentralized environment resulted in field operations not complying with the Cloud Framework which curtailed the efficiencies that should have come with cloud resources. Cloud operations also needed to be further enhanced through vulnerability remediation, incident classification and asset data quality.

OIOS made seven important recommendations. To address issues identified in the audit, UNHCR needed to:

- Update cloud related guidance in IT strategy and Cloud Framework including its vendor selection methodology.
- Update the organization's guidance on data classification and retention within the cloud environment.
- Create awareness about 'cloud first' and 'reuse' principles; and address cases of violations and monitor segregation of roles in the cloud environments.
- [REDACTED]
- Include flexible clauses in cloud service provider contracts that allow adjustments in resource usage and costs as operational needs change; and establish a baseline contract template that covers essential clauses to safeguard organizational interests for all cloud-related contracts.
- Ensure that contract negotiations are based on data that reflects the most relevant operational demands, thereby improving cost estimates and securing more cost-efficient contractual terms.
- Enhance data quality of cloud assets in the configuration management database to support better decision making and management.

UNHCR accepted all recommendations and has initiated action to implement them. Actions required to close the recommendations are indicated in Annex I.

CONTENTS

I. BACKGROUND	1-2
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	2
III. AUDIT RESULTS	2-11
A. Framework to govern the cloud environment	2-6
B. Operational effectiveness of cloud services	6-9
C. Procurement and contracting of cloud services	9-10
D. Cloud asset management	10-11
IV. ACKNOWLEDGEMENT	11
ANNEX I	Status of audit recommendations
APPENDIX I	Management response

Audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees

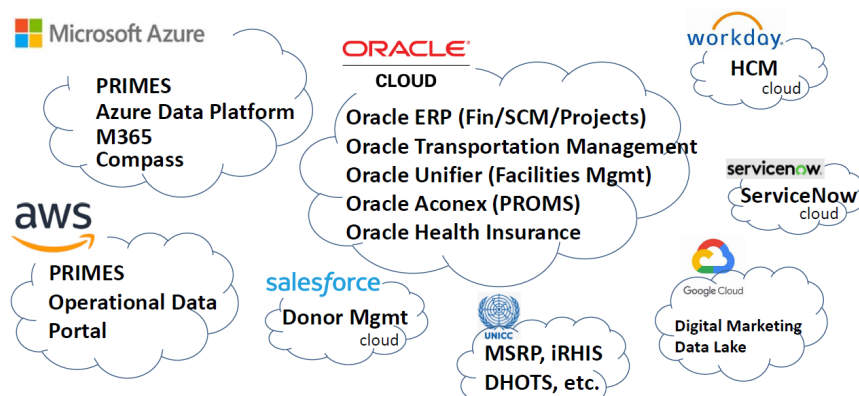
I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees (UNHCR).

2. UNHCR’s mode of operation has evolved since 2018 and this was primarily driven by the decentralization and regionalization process as well as the impact of the COVID-19 pandemic that saw teleworking come into effect. UNHCR’s ‘Cloud First’¹ strategy enabled the organization to migrate to Cloud thereby supporting remote access and improved efficiency. UNHCR relied on vendors that provided scalable, secure, and cost-effective cloud services, leaving its limited in-house IT staff to select and manage these technologies.

3. As operational demands evolved and new technologies emerged, UNHCR migrated corporate solutions such as proGres and CashAssist to the cloud and also adopted cloud-based solutions and Software as a Service (SaaS) such as Oracle’s Cloud Enterprise Resource Planning (ERP) system and Workday. UNHCR adopted a multi-cloud approach, primarily using Microsoft Azure, Amazon Web Services (AWS), and Oracle Cloud Infrastructure for general infrastructure and platform solutions as reflected in Figure 1.

Figure 1: Cloud infrastructure and systems



4. The Information Technology Service (ITS), formerly the Division of Information Systems and Telecommunications (DIST) was responsible for managing the cloud services. UNHCR’s Cloud Framework: (a) outlined its approach to cloud computing; (b) demarcated between the roles of DIST and business owners in cloud environments; and (c) established standards for secure cloud deployments. The expenditure on key cloud resources is reflected in Table 1:

Table 1: Expenditure on key cloud infrastructure between 2023 and October 2025 (\$ millions)

Cloud Service Provider (CSP)	2023	2024	2025 (up to 10/2025)	Total
Azure	2.44	3.23	3.21	8.88
Oracle Cloud Infrastructure	0.1	0.48	0.54	1.12
AWS	0.72	0.86	0.55	2.13
Total	3.26	4.57	4.30	12.13

¹ As part of the ‘cloud-first’ hosting strategy, UNHCR has progressively migrated information systems from private data centers to cloud service providers and also hosted its major enterprise software systems on cloud.

5. UNHCR relied on data management systems, including: (a) Configuration Management Data Base (CMDB) that is a centralized repository that stores information about UNHCR’s IT assets; (b) Cloud Cost Partitioning dashboard that provides visibility into how cloud expenditures are allocated across different units, projects, or services; and (c) incident management through ServiceNow.²

6. Comments provided by UNHCR are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

7. The objective of the audit was to assess the adequacy and effectiveness of the governance, risk management and control processes for efficient and effective provision of cloud services at UNHCR.

8. This audit was included in the 2025 OIOS risk-based work plan due to the risks associated with UNHCR’s increased reliance on the cloud infrastructure.

9. OIOS conducted this audit from September to November 2025. The audit covered the period from October 2023 to September 2025. Based on an activity-level risk assessment, the audit covered higher and medium risks areas which included: (a) framework to govern the cloud environment; (b) operational effectiveness of cloud services; (c) procurement and contracting of cloud services; and (d) cloud asset management.

10. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) assessment of UNHCR’s data management systems, i.e., CMDB, Cloud Cost Partitioning dashboard and ServiceNow; (d) analytical review of data on vulnerabilities, cloud cost, security incidents and cloud service requests; and (e) assessment of cloud governance and management using the Control Objectives for Information and Related Technologies (COBIT) 5 framework for Information Technology governance and management developed by the Information Systems Audit and Control Association (ISACA).

11. OIOS assessed the reliability of data related to CMDB, Cloud Cost Dashboard and Service Now by: (a) performing electronic testing, and (b) reviewing existing information about the data and interviewing ITS personnel knowledgeable about the data. Additionally, OIOS traced a random sample of data to source documents and found it sufficiently reliable for the audit objectives, although some data quality issues are noted in subsequent sections.

12. The audit was conducted in accordance with the Global Internal Audit Standards.

III. AUDIT RESULTS

A. Framework to govern the cloud environment

Need to address gaps in the cloud governance

13. UNHCR has IT strategies for 2020-22 and 2024-26, the implementation of which is supported by a Cloud Framework developed in 2023. The Framework defines UNHCR’s approach to cloud computing, helps organize information about requests and requirements for cloud services, provides explanations on roles and responsibilities for cloud environments, and describes standards for secure cloud deployments. The key cloud computing aspects include hub and spoke architecture, security configurations including

² ServiceNow portal is an information system for requesting services and support from the Global Service Desk.

network security, inter-cloud connectivity, and cloud data and integration platforms. Besides noting the presence of the aforementioned cloud governance aspects, OIOS found the following gaps:

(a) Outdated guidance on data management

14. The UNHCR IT strategy and Cloud Framework did not adequately cover data loss prevention mechanisms, i.e., how to identify, monitor, and protect sensitive data from unauthorized access, use, or transmission. This was especially important in cases where UNHCR was using public instead of private cloud resources.³ Specifically:

- UNHCR's 2010 Information Classification, Handling and Disclosure Policy had not been updated to reflect changes resulting from the organization's transition to the cloud. While the policy required information to be classified based on value, sensitivity, and criticality in line with COBIT 5, it provided no guidance on how to apply these requirements in a cloud environment.
- UNHCR's 2017 Policy on the Management of UNHCR Records and Archives identified the Electronic Document and Records Management system (e-SAFE) as the official UNHCR platform for electronic recordkeeping. This policy, however, became outdated considering the introduction of cloud-based corporate solutions such as OneDrive and SharePoint. Additionally, the policy did not provide guidance on retaining data in the cloud environment for the minimum duration required to meet operational, legal, or contractual obligations, nor on the secure disposal of data thereafter.

15. Absent of this guidance, all information in the cloud environment was handled in the same manner, which led to inefficient use of cloud resources. For instance, cloud storage for the dump of data owned by separated staff increased the expenditure on cloud resources by \$419,400 in 2025. Had the data been classified with defined retention schedules, UNHCR could have prioritized what needed to be retained resulting in more efficient use of cloud resources. Additionally, UNHCR had to incur costs totaling \$449,000 and \$431,000 in 2025 and 2024 respectively for licenses for the now-obsolete PeopleSoft ERP system. While ITS was of the view that this was a normal practice to ensure business continuity, it came at an extra cost as the non-working system would be hosted on cloud for unnecessarily long periods of time. If unaddressed in a timely manner, it would also lead to continued wastage of resources at a time when UNHCR is facing serious financial constraints.

(b) Gaps in the cloud architecture and service delivery processes

16. In line with the UNHCR's Cloud Framework, ITS prioritized the lift-and-shift migration approach which moved applications and data from on-premise infrastructure to the cloud with minimal or no code changes made. While the lift-and-shift approach allowed for faster deployment, it did not provide for the redesign and modification of applications to fully utilize cloud features.

17. Also, the migration of legacy applications with older codes without pre-migration changes resulted in the transfer of legacy inefficiencies, potential security issues and compliance mismatches with the cloud infrastructure. For example, UNHCR's Biometric Identity Management system (BIMS) application had several technical failures even after being migrated to the cloud. The UNHCR Cloud Framework needed to provide for the selection of alternatives such as re-platform/lift-tinker-and-shift⁴ when warranted to fully reap the benefits of performance, scalability, and cost-efficiency that cloud offered.

³ Public cloud is a cloud infrastructure model that is provisioned for open use by the general public. Private cloud is a cloud infrastructure used exclusively by a single organization.

⁴ Slightly modify applications to optimize for cloud (e.g., move from self-managed database to managed service).

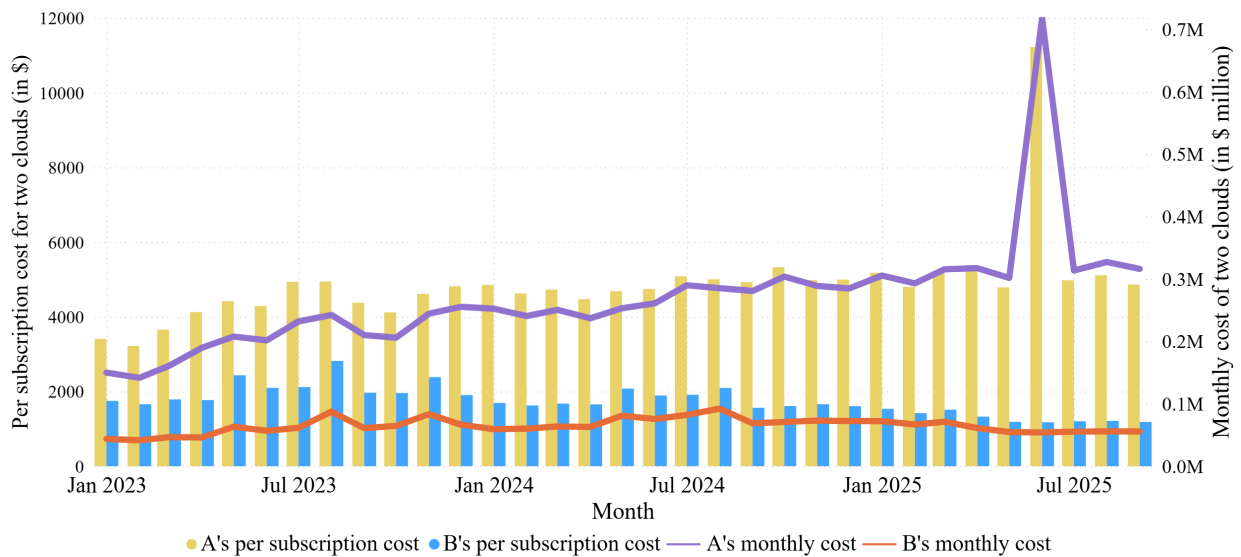
(c) Inherent bias in the recommended criteria for cloud vendor selection

18. To optimize costs and maximize value delivered, the Cloud Framework listed four criteria for the selection of CSPs, in the following order: (i) technical requirements; (ii) affinity, i.e., compatibility with existing systems; (iii) developer and support skills; and (iv) hosting costs. While it was logical to have technical requirements determine the initial supplier choice for each application, the remaining three parameters did not have to be prioritized in a fixed order but evaluated on a case-by-case basis. For instance, IT advancements now enabled interoperability across different clouds thereby reducing the need to prioritize affinity in cloud provider selection. For instance, CSP A was selected to host BIMS based on affinity and at a cost of \$ 1.75 million. However, if affinity had not been a prioritized criterion, the selection of CSP B could have resulted in a potential saving of \$1.16 million. While ITS justification was that CSP B’s architecture could not run biometric solutions such as BIMS, OIOS noted that it was providing commercial biometric solutions.

19. The interrelated nature of the criteria meant that once a vendor was chosen based on the primary criterion, the remaining criteria naturally reinforced that choice, which raised the risk of vendor lock-in. For instance, CSP A was selected for proGres on the basis that the latter relied on a certain artificial intelligence-powered ERP and customer relationship management (CRM) tool which was only available with CSP A. The second criterion, i.e., affinity, resulted in Data Port being selected on the basis that it depended on proGres which was available in CSP A.

20. An analysis of available data between January 2023 to September 2025 showed that there was an increasing reliance on CSP A even though the cost per subscription for CSP B was lower as reflected in Chart 1 below.

Chart 1: Comparison of overall monthly cost (lines) and per subscription cost (bars) for main cloud providers



21. ITS justification for this situation was the need to have all interconnected applications under one cloud provider, i.e., affinity. However, UNHCR’s heavy reliance on a couple of CSPs, with preference given to one of them, raised the risk of vendor lock-in. This complicated UNHCR’s ability to switch providers or adopt alternative solutions especially at a time when newer technologies could be available on the market. Vendor lock-in could also potentially reduce UNCHR’s negotiating power and constrain its

ability to optimize costs. ITS noted that UNHCR’s capacity to effectively mitigate vendor lock-in risk was limited, thereby accepting related risks.

22. Further, although the hosting cost was listed as the least important criterion, its prioritization could have brought possible savings. For instance, the selection of Western Europe as hosting region was not supported by a documented cost-benefit analysis but justified based on strict regional data privacy regulations and the fact that West European locations were close to UNHCR’s three Headquarter locations and UNHCR’s VSAT network. An analysis of CSP A’s costs in different regions showed that on average Western Europe region costs were 13 per cent higher as reflected in Table 2 below. Thus, the selection of a cheaper location for CSP A would have resulted in a cost saving of \$1.14 million in the period under audit.

23. ITS stated that it did not select one of the cheaper location options (say A) as the local law prevalent there required the cloud service providers to share the data stored in that location with the law enforcement agencies, if needed. The cloud supplier noted that the laws require companies based in A to share data with government authorities upon request, even if that data was stored on servers outside A. However, the cloud supplier further clarified that it could not guarantee data sovereignty for its customers and must comply with legally valid requests.

Table 2: Comparative analysis of costing between different geographical regions for three-year plan

Configuration item	Technical specifications	Western Europe cost (\$)	Cheaper cost option (\$)	Differential cost ratio
Windows Virtual Machines	Av2 Standard (A8m v2)	177.1/month	130.6/month	1.36
Blob Storage	Reserved Storage Capacity 100 TB (hot site)	1,325/month	1,217/month	1.09
SQL Database	Standard-series (Gen 5) vCORE 80	5,279.9/month	4,799.9/month	1.10
App Service on Windows	App Service Environment plan (16v2)	7,254/month	6,961/month	1.04

(d) Formal maturity assessments not conducted

24. COBIT 5 and UNHCR’s IT strategy (2024-26) required that maturity assessments of cloud management are conducted to identify ways in which related technologies could be better leveraged and costs better managed. ITS stated that formal and informal maturity assessments had been conducted but could not provide supporting evidence. ITS also indicated it did not see value in third-party assessments given resource constraints. This view, however, contradicted best practice and ITS’ own strategy, and represented a missed opportunity to identify improvements that could enhance the effectiveness, security, and efficiency of its cloud investments. Such assessments could have also helped ITS identify some of the issues identified in this report for timely remediation.

<p>(1) The UNHCR Information Technology Service should update cloud related guidance in IT strategy and Cloud Framework including its vendor selection methodology.</p> <p><i>UNHCR accepted recommendation 1 and stated that the new IT Strategy 2026 -2027 would be published soon and has a dedicated section which addressed this recommendation.</i></p> <p>(2) The UNHCR Global Data Service, in coordination with the Information Technology Service, should update the organization’s guidance on data classification and retention within the cloud-environment.</p>

UNHCR accepted recommendation 2 and stated that the new policy on the management of records and archives was under review and would be issued soon which would address the gaps related to information retention. Global Data Service would review the current data classification policy and support it with a cloud-specific guidance to address the gaps related to data classification.

B. Operational effectiveness of cloud services

Non-compliance with the Cloud Framework provisions

(a) Maintaining on-premise servers in contravention with Framework

25. In line with its cloud-first strategy, UNHCR eliminated on-premise servers at headquarters by migrating solutions to cloud infrastructure and implementing cloud-based SaaS corporate solutions. However, exceptions related to field offices retaining unauthorized on-premise servers were noted. For instance, the CMDB showed that UNHCR had 76 on-site servers, 74 of which had been acquired by Field operations between 2020 and 2025. Sixty-seven (88 per cent) of the 76 servers were in the Europe and Middle East and North Africa regions. These servers had limited scalability and were more vulnerable than cloud-based solutions to risks such as security risks, data loss and hardware failure.

26. Maintaining on-premise instead of cloud-based servers exposed UNHCR to higher costs arising from factors such as maintenance and upgrades. For example, some of these servers were updated around 200 times by the ITS field support, which was resource intensive.

27. Further, contrary to the UNHCR's "reuse, buy, or develop" requirement⁵ as mentioned in the Cloud Framework, field operations maintained/ purchased systems with functionalities that were similar to corporate solutions. These systems, some unnecessary, were hosted on the cloud and thus increased related costs. For instance, UNHCR's purchase of SurveyMonkey (a SaaS solution) when Microsoft Forms provided the same functionalities was uneconomical. Additionally, UNHCR spent \$0.5 million on hosting IrisGuard in cloud between 2023 and October 2025, an application that had similar functionality as BIMS and was used to validate bank payments using biometrics captured through BIMS.

28. ITS needed to reinforce its policies to provide disincentives for non-compliance such as robust justification and approval of exceptions, financial disincentives for non-compliance and/or flagging to senior management any flouting of policies.

(b) Inadequate segregation of roles in the development, test and production environments

29. The Cloud Framework provided for separate development, test, and production environments⁶ in cloud infrastructure to allow developers to build and test code safely without affecting live systems. While the three environments were present for most of the applications as recommended by the framework, the segregation of duties among the three environments was inadequate. For instance, 89 of 95 users that had access to CSP C production environment also had access to CSP C development environment.

30. Similarly, an analysis of user accounts for five applications in CSP B cloud revealed that several users had common roles across the three environments. For instance, six out of seven, four out of six and three out of seven users of PRIMES, DIST AOAI and RBM production environment respectively, also had

⁵ "Reuse, buy, or develop" approach encourages business owners to leverage existing systems with similar functionality rather than investing in new ones.

⁶ Developers use development environment to write and build code. Test environment is used to verify and validate code before release. Production environment is the live environment where the final application runs for end users, after testing phase.

access to development environment of these applications/ services. Also, all the eight and seven users with access to production environment of VerifyPlus and IrisGuard respectively, also had access to development environment of these applications.

31. ITS stated that segregation of roles and responsibilities between the three cloud environments was expensive. However, having the same users access the different cloud environments increased the risk of unauthorized and conflicting changes being carried out by the same user, and called for stricter monitoring as a mitigating action.

(3) The UNHCR Information Technology Service should reinforce implementation of IT strategy and Cloud Framework guidance by: (a) creating awareness about 'cloud first' and 'reuse' principles and bringing cases of violations to the notice of responsible business owners to address inefficiencies; (b) engaging the Regional Bureaux of Europe and Middle East and North Africa to reduce the high number of on-site servers; and (c) monitoring segregation of roles in the cloud environments.

UNHCR accepted recommendation 3 and stated that ITS would continue to provide regular communication to business owners and Regional Bureaux and the responsibility for the implementations lied with business owners. ITS would continue to monitor the access rights in cloud environments.

[Redacted]

(a) [Redacted]

32. [Redacted]

33. [Redacted]

34. [Redacted]

35. [Redacted]

[Redacted]

36. [Redacted]

(b) [Redacted]

37. [Redacted]

38. [Redacted]

39. [Redacted]

(4) [Redacted]

⁷ With MFA, a user is granted access after successfully presenting two or more authentication factors from independent credential categories (password / security token / biometrics etc.)

⁸ Either not tested or test to be scheduled or no evidence of testing available.



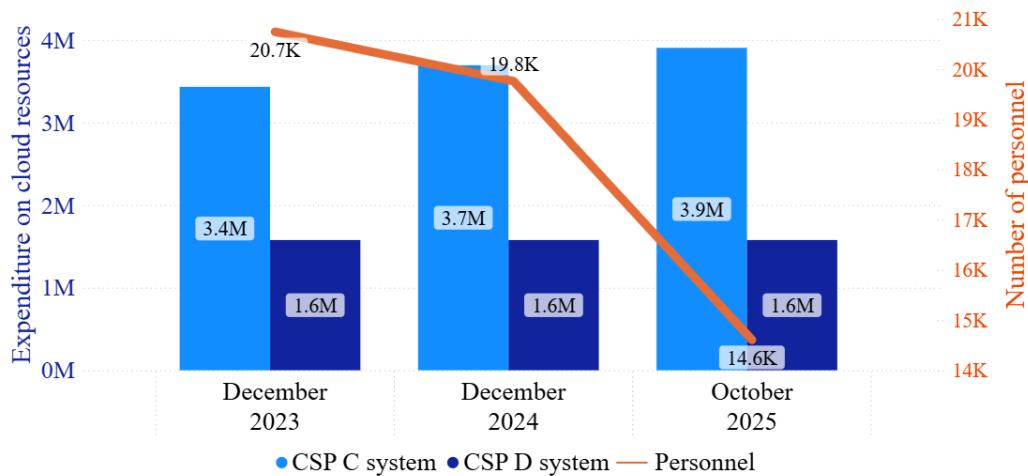
C. Procurement and contracting of cloud services

Contracts with cloud service providers needed revision

(a) Challenges in modifying cloud contracts as operational needs change

40. The benefit of cloud infrastructure being scalable was not evident, with significant reductions in UNHCR’s workforce not resulting in any corresponding decreases in cloud expenditure as noted from an analysis of expenditure on two largest resource intensive cloud-based solutions, CSP C’s system and CSP D’s system in Chart 2 below.

Chart 2: Count of personnel vis-à-vis expenditure on cloud resources (in \$)



41. ITS attributed this to contracts of these services having fixed three or five-year baselines for human resources, with no provisions for adjustments if numbers changed midway. ITS further noted that these contracts were driven by vendors and non-negotiable. In these circumstances, UNHCR continued to pay for capacity it was not using and thus did not benefit from the scalability that cloud infrastructure was supposed to bring. Considering the significant changes in operational realities, UNHCR needed to address limitations of fixed-baseline contracts by exploring alternative flexible pricing models such as tier user pricing, minimum baselines with variable add-ons and elastic subscription models. Alternatively, UNHCR could have shorter contract periods and provide for mid-term reviews. Going forward, UNHCR had reduced the CSP A’s licenses from 20,000 to 12,000 but similar reduction in other resources was awaited.

42. ITS also needed to use up to date information to inform the baselines set in contracts. For instance, the renewal of the CSP B’s contract from 1 July to 31 December 2025 was based on data from 1 January 2024 to 30 June 2025. This 18 month coverage was skewed and not reflective of current operational realities. ITS should have used the latest available usage data, aligned with overall reduced operational footprint to achieve better cost estimates from cloud providers.

(b) Contractual obligations of the CSPs needed standardization

43. There was variability in the clauses related to data protection in different cloud contracts. For example, the contract for CSP C had a clause on UNHCR’s audit rights over the data protection measures taken by the CSP but these were not there for CSP D and CSP B. Also, while the contract provided for an audit of the CSP’s compliance with the data processing agreements up to once per year or as required by the extant law, no such audit was conducted. The variability of contracts of different CSPs raised the risk of inadequate protection of sensitive information, and noncompliance with legal requirements. This may result in data loss, unauthorized access, or breaches without clear accountability.

(5) The UNHCR Legal Affairs Service, in coordination with the Information Technology Service, should: (a) include flexible clauses in cloud service provider contracts, wherever possible, that allow adjustments in resource usage and costs as operational needs change; and (b) establish a baseline contract template that covers essential clauses to safeguard organizational interests for all cloud-related contracts.

UNHCR accepted recommendation 5 and stated that the organization has established a baseline set of special conditions for cloud-based services covering essential clauses to safeguard organizational interests for cloud-related contracts. Legal Affairs Service (LAS) would review its template clauses for cloud-based services so as to provide strong basis for UNHCR negotiations. When agreed with the service provider as part of business negotiations, LAS would include flexible clauses in cloud service provider contracts that allow adjustments in resource usage and costs as operational needs change.

(6) The UNHCR Information Technology Service should ensure that contract negotiations are based on data that reflects the most relevant operational demands, thereby improving cost estimates and securing more cost-efficient contractual terms.

UNHCR accepted recommendation 6 and stated that Information Technology Service reviews the contracts using the latest data available for the negotiations and that Procurement section and Legal Affairs Service have been involved in contract negotiations.

D. Cloud asset management

Data in CMDB needed review for better cloud asset management

44. Cloud asset⁹ management includes identifying and recording, managing critical assets for reliability and availability, and managing through the lifecycle of the assets. UNHCR recorded all the cloud assets in CMDB. OIOS analyzed the CMDB containing details of the 376 operational applications hosted on cloud and observed data completeness issues for various parameters as detailed in Table 3 below, which was attributed to inadequate data-quality assurance process.

Table 3: Data completeness issues in the application database

Data field	Issue	Count
Install Status	Fields had invalid values (100/200) or were blank.	66
Backup requirements	Field read ‘Backup Requirements Unknown’	62
Application type	Field was blank.	29
Criticality	Field read ‘6 - Criticality Unknown’	20

⁹ Cloud assets refer to digital resources stored and managed in cloud environments, such as data and applications

Data field	Issue	Count
Recovery Point Objective	Field either read 'No Data' or 'To Be Advised'	19
Recovery Time Objective	Field read 'To Be Advised'	7
Install type (Cloud / On-premises etc.)	Field was blank when 'Location' field mentions it as a cloud hosted application (for example - Microsoft Azure Cloud, CLD-MSA, Site	6
Recovery plan	Field was blank.	6

(7) The UNHCR Information Technology Service should enhance data quality of cloud assets in the configuration management database to support better decision making and management.

UNHCR accepted recommendation 7 and stated that Information Technology Service (ITS) continuously enhances and monitors the quality of the configuration management database. ITS would review the processes and configuration items not used would be removed from the system. ITS would continue to monitor and demonstrate improvements, with a focus on data related to critical applications.

SLA monitoring was adequate

45. UNHCR had entered into service level agreements (SLAs) with the different CSPs to define the performance levels for availability of cloud resources, change implementation, vulnerability management, incident response and resolution, server security patching, and service request handling. These service level agreements were monitored by the Managed Service Providers (MSPs, one each for the SaaS and non-SaaS cloud resources).

46. UNHCR conducted monthly Infrastructure Operations and Managed Workplace Services Steering Committee Meetings with the MSPs. These meetings included SLA monitoring as one of the agenda items. Further, the MSP monthly reports mentioned SLA breaches. However, the target achievement for the SLA was not always mentioned. For example, in July 2025 report, Vulnerability Scanning SLA report shows RGB servers scanning percentage in red at 76.4 per cent, but the achievement target was not mentioned, to gauge the gap between target and achievement. UNHCR could guide MSPs to include target values against the actual achievement for better monitoring of these indicators.

IV. ACKNOWLEDGEMENT

47. OIOS wishes to express its appreciation to the management and staff of UNHCR for the assistance and cooperation extended to the auditors during this assignment.

Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical ¹⁰ / Important ¹¹	C/ O ¹²	Actions needed to close recommendation	Implementation date ¹³
1	The UNHCR Information Technology Service should update cloud related guidance in IT strategy and Cloud Framework including its vendor selection methodology.	Important	O	Receipt of new IT Strategy addressing the highlighted gaps.	31 March 2026
2	The UNHCR Global Data Service, in coordination with the Information Technology Service, should update the organization's guidance on data classification and retention within the cloud-environment.	Important	O	Receipt of new guidance on data classification and retention addressing the highlighted gaps.	31 December 2026
3	The UNHCR Information Technology Service should reinforce the implementation of IT strategy and Cloud Framework guidance by: (a) creating awareness about 'cloud first' and 'reuse' principles and bringing cases of violations to the notice of responsible business owners to address inefficiencies; (b) engaging the Regional Bureaux of Europe and Middle East and North Africa to reduce the high number of on-site servers; and (c) monitoring segregation of roles in the cloud environments.	Important	O	Receipt of evidence of ITS' engagement with business owners and Regional Bureaux for reinforcing the implementation of IT strategy and Cloud Framework guidance, and evidence of monitoring of access rights.	31 December 2027
4	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

¹⁰ Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

¹¹ Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

¹² Please note the value C denotes closed recommendations whereas O refers to open recommendations.

¹³ Date provided by UNHCR in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical ¹⁰ / Important ¹¹	C/ O ¹²	Actions needed to close recommendation	Implementation date ¹³
5	The UNHCR Legal Affairs Service, in coordination with the Information Technology Service, should: (a) include flexible clauses in cloud service provider contracts, wherever possible, that allow adjustments in resource usage and costs as operational needs change; and (b) establish a baseline contract template that covers essential clauses to safeguard organizational interests for all cloud-related contracts.	Important	O	Receipt of cloud service provider contracts having provision of flexible clauses, and receipt of template contract containing clauses related to audit rights.	31 December 2026
6	The UNHCR Information Technology Service should ensure that contract negotiations are based on data that reflects the most relevant operational demands, thereby improving cost estimates and securing more cost-efficient contractual terms.	Important	O	Receipt of contracts which include service usage for the relevant period while calculating expected service volume.	31 December 2027
7	The UNHCR Information Technology Service should enhance data quality of cloud assets in the configuration management database to support better decision making and management.	Important	O	Receipt of evidence demonstrating enhancement in data quality especially for the critical (Tier 0 and Tier 1) applications.	31 December 2027

APPENDIX I

Management Response

MANAGEMENT RESPONSE

Audit of optimization of cloud services in the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical ¹⁴ / Important ¹⁵	Accepted? (Yes/No)	Title of responsible individual	Implementation date	UNHCR comments
1	The UNHCR Information Technology Service should update cloud related guidance in IT strategy and Cloud Framework including its vendor selection methodology.	Important	Yes	Chief Information Officer	Q1 2026	The new IT Strategy 2016 -2017 which is under has a dedicated section which addresses the recommendation. The strategy will be published very soon.
2	The UNHCR Global Data Service, in coordination with the Information Technology Service, should update the organization's data classification and retention framework including within the cloud-environment.	Important	Yes	Head of Service, GDS / Director, ITS	31 December 2026	The new policy on the management of records and archives is under review and will be issued soon which would address the gaps related to information retention. GDS would review the current data classification policy and support it with a cloud-specific guidance to address the gaps related to data classification.
3	The UNHCR Information Technology Service should reinforce the implementation of IT strategy and Cloud Framework guidance by: (a) creating awareness about 'cloud first' and 'reuse' principles and bringing cases of violations to the notice of responsible business owners to address inefficiencies; (b) engaging the Regional Bureaux of Europe and Middle East and North Africa to reduce the high number of on-site servers; and (c) monitoring segregation of roles in the cloud environments.	Important	Yes	Chief IT Operation; Head of IT SES	Q4 2027	ITS will continue to provide regular communication to business owners and Regional Bureaux. The responsibility for the implementation lays with business owners respectively Regional Bureaux. ITS will continue to monitor the access rights in cloud environment

¹⁴ Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

¹⁵ Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

Rec. no.	Recommendation	Critical ¹⁴ / Important ¹⁵	Accepted? (Yes/No)	Title of responsible individual	Implementation date	UNHCR comments
4	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
5	The UNHCR Legal Affairs Service, in coordination with the Information Technology Service, should: (a) include flexible clauses in cloud service provider contracts, wherever possible, that allow adjustments in resource usage and costs as operational needs change; and (b) establish a baseline contract template that covers essential clauses to safeguard organizational interests for all cloud-related contracts.	Important	Yes	General Counsel and Head, LAS	31 December 2026	<p>Regarding a), LAS agrees with the recommendation for contracts that allow such adjustments. LAS will continue improving its template clauses for cloud-based services so as to provide strong basis for UNHCR negotiations and, when consulted for review of vendor templates, will pay attention to clauses that allow adjustments in resource usage and costs as operational needs change. When agreed with the service provider as part of business negotiations, UNHCR will include flexible clauses in cloud service provider contracts.</p> <p>Regarding b), LAS agrees with the recommendation and notes that</p>

Rec. no.	Recommendation	Critical ¹⁴ / Important ¹⁵	Accepted? (Yes/No)	Title of responsible individual	Implementation date	UNHCR comments
						UNHCR has already established a baseline set of 'special conditions for cloud-based services' covering essential clauses to safeguard organizational interests for cloud-related contracts, last updated in December 2024 and accessible to all UNHCR colleagues via the UNHCR Intranet, as well as a checklist and clause banks with additional/alternative clauses focusing on cybersecurity and data protection in cloud-related contracts.
6	The UNHCR Information Technology Service should ensure that contract negotiations are based on data that reflects the most relevant operational demands, thereby improving cost estimates and securing more cost-efficient contractual terms.	Important	Yes	ITS	Q4 2027	ITS reviews the contracts using the latest data available for the negotiations and Procurement section and Legal Affairs Service have been involved in the contract negotiations. As requested by OIOS, ITS will provide examples of contracts (new or renewals) which have usage for the relevant period - therefore OIOS would consider it appropriate to close the recommendation.
7	The UNHCR Information Technology Service should enhance data quality of cloud assets in the configuration management database to support better decision making and management.	Important	Yes	Deputy Director BRMS	Q4 2027	ITS continuously enhances and monitors the quality of the configuration management database. ITS will review the processes and configuration items not used will be removed. ITS will focus only on Tier 0 and Tier 1 applications and to be noted that 100 per cent compliance cannot be achieved. ITS will continue to monitor and demonstrate improvements.