Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2022/042

Audit of cloud arrangements at the Office of United Nations High Commissioner for Refugees

There was a need to strengthen cloud computing governance, security, asset and change management in UNHCR

21 September 2022
Assignment No. AR2021-166-02

Audit of cloud arrangements at the Office of United Nations High Commissioner for Refugees

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of cloud arrangements at the Office of the United Nations High Commissioner for Refugees (UNHCR). The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes for efficient and effective provision of cloud computing services in UNHCR. The audit covered the period from 1 January 2019 to 31 December 2021 and included a review of: (a) governance, risk management and compliance; (b) data management and security; (c) contract and vendor management; (d) configuration, asset management and change management; and (e) resilience and availability.

Following UNHCR's adoption of cloud computing to support its business processes, it migrated several applications to two cloud service providers in 2020 and 2021. This not only improved business continuity, visibility and scalability of applications, but also enhanced their security and transparency. To further improve efficient and effective cloud computing, UNHCR needed to strengthen arrangements for governance, security, asset and change management.

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

- Address gaps in the current framework for cloud services and formalize related guidance;
- Strengthen documentation of logging and approving requests for cloud services;
- Strengthen its processes for updating the configuration management database so it is comprehensive;
- Ensure that material changes to assets hosted in the cloud are subject to formal change management processes;
- [redacted]
- Establish a benefits realization plan for migration to the cloud against which performance can be measured.

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

CONTENTS

Audit of cloud arrangements at the Office of United Nations High Commissioner for Refugees

I. BACKGROUND

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

2. Cloud computing involves the delivery of computing services over the internet from different locations, using a shared and dynamically scalable information and communications technology (ICT) infrastructure. Cloud arrangements move operating models away from fixed utilization to more flexible ones such as 'pay-as-you-go' arrangements, thereby resulting in a transfer of costs to operating expenditure. Thus, organizations only pay for services that are required.

3. Cloud technologies provided UNHCR with new possibilities for improved computing, data storage and accessibility, increased workforce mobility and collaboration and major system enhancements. UNHCR's ICT strategy adopted a "cloud first" approach that called for new systems to be hosted on the cloud. Where appropriate, migration to cloud services would be considered to reduce susceptibility to on-premise hardware and software failures and to improve service continuity. The ICT strategy stated that UNHCR would 'buy not build' systems and services by optimizing the use of managed service providers (MSP), thereby enabling UNHCR to adapt to new opportunities and technologies.

4. The Division of Information Systems and Telecommunications (DIST) is responsible for the provision of ICT services in UNHCR. UNHCR had 'pay-as-you-go' contracts with two major cloud service providers (CSP) that offered a range of infrastructure, platforms and database software services.[1] DIST contracted an MSP to administer cloud as well as provide infrastructure services. At the time of the audit, UNHCR had 54 cloud service subscriptions, 37 of which were with one provider and the remaining 17 with another provider. The total expenditure in 2021 was $1.7 million, an increase of 42 percent from $1.2 million in 2020.

5. UNHCR is in the process of implementing a Software as a Service (SaaS) based strategic Business Transformation Programme[2] aimed at improving processes and tools to support its operations and facilitate delivery of effective services to persons of concern.

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 governance, risk management and control processes for efficient and effective provision of cloud computing services in UNHCR.

8. This audit was included in the 2021 risk-based work plan of OIOS due to the significant inherent risks associated with the management of cloud services.

---

[1] Infrastructure as a Service e.g., virtual machine, Database as a Service e.g., the SQL Database, and Platform as a Service e.g., the SQL Server.

[2] While COMPASS (Results Based Management) went live in 2021, Cloud ERP, Workday and Salesforce will be implemented by 2023. A separate OIOS audit on the Business Transformation Programme will take place in 2022.

9. OIOS conducted this audit from December 2021 to April 2022 and covered the period from 1 January 2019 to 31 December 2021. Based on an activity-level risk assessment, the audit covered high and medium risk areas pertaining to cloud arrangements which included: (a) governance, risk management and compliance; (b) data management and security[3]; (c) contract and vendor management; (d) configuration, asset management and change management; and (e) resilience and availability. All audit tests were performed on the subscriptions/resources hosted at one provider. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data from MSRP and data from the CSP; and (d) sample testing of controls.

10. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

III. AUDIT RESULTS

A. Governance, risk management and compliance

UNHCR needed to address and formalize guidance and framework gaps for cloud services

11. *Controls and assurance in the Cloud (using COBIT) by Information Systems Audit and Control Association (ISACA)* specifies that for organizations to benefit from the use of cloud computing, a clear governance strategy and management plan must be developed. The governance strategy sets the direction and objectives for cloud computing within the enterprise, and the management plan ensures that relevant objectives are achieved. DIST is responsible for developing and maintaining ICT policies, standards and guidelines that detail controls for addressing risks.

12. UNHCR did not have a formal framework, guidelines and procedures in place to reflect the changes ensuing from the introduction of cloud computing. In the document *'Cloud on-boarding framework'*, DIST proposed that a framework be developed for the deployment and configuration of resources needed to host applications. This framework referred to a basic governance structure for the cloud, as well as the general architectural, operational and security framework, but did not conform to UNHCR's guidance on policy and administrative instructions. For instance, the roles and responsibilities between cloud subscribers/customers, DIST as the internal service provider and the MSP were not clearly defined.

13. Furthermore, the whitepaper on *'Use of cloud computing in the United Nations System'* envisaged that the adoption of cloud computing changes an organization's risk profile as several ICT risks are transferred to the CSPs. Consequently, by changing to cloud systems, UNHCR had increased exposure to other types of risk such as asset management, data management, vendor performance and legal risks. These changes called for a different risk management perspective compared to the traditional arrangements for ICT (on-premises data centers). There was thus a need to perform an analysis of emerging risks and prepare plans to mitigate them. While DIST noted it had previously identified and documented cloud risks, it did not provide documentation to support this.

14. [redacted]

[3] Compliance with data protection requirements has been excluded as the topic is covered in the ongoing OIOS advisory review of data protection and privacy arrangements at UNHCR (VR2021-160-03).

15. [redacted]

(1) The UNHCR Division of Information Systems and Telecommunications should address gaps in the current framework for cloud services and formalize related guidance.

UNHCR accepted recommendation 1 and stated that DIST would review existing guidance and framework documentation and address any gaps.

Logging of cloud service requests needed improvement

16. As an organization's cloud footprint grows, more subscriptions and related resources are typically created to support applications. Effective subscription design helps organizations establish a structure to organize and manage assets during cloud adoption. Requests for cloud deployment/migrations submitted by Headquarters Divisions, Regional Bureaux or Representations were routed through an on-line service request system. The Project Services team under the Office of the Chief Information Officer, DIST was responsible for overseeing and coordinating the portfolio of all ICT projects (including cloud migrations) in UNHCR. Approved cloud initiatives, through project and change management processes, became the basis for cloud subscriptions.

17. OIOS reviewed the online system cloud migration/subscription requests log for 2020 and 2021 and the requests for changes processed during the same period. Thirty-two of the 37 subscriptions at the CSP reviewed could be linked to Biometric Identity Management System, Finance BI PROD, Population Registration and Identity Management Eco-System or to the requests for changes for Interoperability PROD, IrisGuard, and Results Based Management. However, some subscriptions originating from Representations such as JORAM BO Apps or ETHAD Digital Filing were not listed in the on-line system or requests for changes. OIOS was therefore unable to confirm that these subscriptions were established through the formal documentation or logging process.

18. Since a subscription is a credible source for establishing configurable items (such as virtual machines, operating systems, applications, storage), a consistent and formal process should be in place to log all requests. Any gaps in this process can have adverse effects on asset and configuration.

(2) The UNHCR Division of Information Systems and Telecommunications should strengthen processes related to documentation and logging of cloud initiatives from online requisition and assessment by teams to final decision.

UNHCR accepted recommendation 2 and stated that taking into consideration the existence of formal change management processes, and cloud resource request processes with appropriate validation and approval, DIST would continue to improve the effectiveness of the currently implemented processes related to documentation and logging of cloud initiatives.

B. Configuration, asset management and change management

There was a need to strengthen arrangements for configuration and asset repository

19. *Controls and assurance in the Cloud (using COBIT) by ISACA* requires that organizations have central repositories that: (i) contain all relevant information on configuration items; (ii) monitor and record

all assets and changes effected to them; and (iii) maintain a baseline of configuration items for all systems and services. This configuration data includes relationships and interdependencies between items, the history of changes as well as class and attributes (type, owner, and importance) for each item. The repository provides an organization with the information needed to make better business decisions and run efficient ICT service management processes including impact and root analyses as well as legal, compliance, incident and change management.

20. In a traditional data center setup, items in the configuration management database (CMDB) do not change very often. Every physical asset is recorded in the CMDB with related accounting and inventory records supported by purchase orders. Cloud computing has however altered these traditional parameters, with organizations expected to manage virtual assets in the cloud. In UNHCR, asset provisioning and de-provisioning in cloud arrangements (such as virtual machines and infrastructure devices) took little effort and was delinked from the conventional supply chain process. This increased the challenges of maintaining an up to date CMDB. Therefore, existing change and configuration management policies, procedures and guidelines needed updating to reflect the different change management requirements unique to the cloud computing environment.

21. Normally, an organization's CMDB should reflect all the ICT assets including the assets in the cloud. However, most assets for the CSP reviewed were not listed in the CMDB. For example, while the CSP reviewed had 2,900 resources (such as virtual machines, storage, SQL servers and other devices), the DIST CMDB had only 138 related configuration items listed. The variances were due to: (a) subscriptions which were not in the CMDB such as Interoperability PROD; VerifyPlus, ETHAD Digital Filing, JORAM BO Apps; (b) proliferation of field-based applications and services which increased the number of virtual assets that needed to be identified and tracked; and (c) resources such as public internet protocol addresses, network gateway, disks, key vaults, and network watcher that were not in the CMDB.

22. The lack of an up to date CMDB (including physical and virtual assets)[4] affected UNHCR's ability to track the impact of changes to an asset (such as a hardware or software) on other ICT assets, services, and business processes along with their security vulnerabilities. The absence of a cloud inventory also impacted the identification of assets that were non-compliant with related UNHCR policies.

(3) The UNHCR Division of Information Systems and Telecommunications should strengthen its processes for updating the configuration management database, so it is comprehensive.

UNHCR accepted recommendation 3 and stated that DIST considered that processes were already defined and in place and applications/services could be registered in the Configuration Management Database (CMDB) using the Service Catalog. Configuration management guidelines were established in 2020 and covered IAAS, PAAS, & SAAS. Nevertheless, DIST would review and strengthen processes where required.

Change management processes needed strengthening

23. *Controls and assurance in the Cloud (using COBIT) by ISACA* specifies that organizations should have formalized controls that ensure that changes to applications and systems do not disable or remove security controls. To avoid disruption to business activities, changes to production systems should only take place after necessary testing and formal approval. Similarly, any important change to the network would necessitate a review of information security risks.

[4] Infrastructure as a Service (IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS)

24. [redacted]

25. [redacted]

(4) The UNHCR Division of Information Systems and Telecommunications should strengthen existing measures to ensure that material changes to assets hosted in the cloud are subject to formal change management processes.

UNHCR accepted recommendation 4 and stated that DIST would strengthen existing measures to ensure that material changes to assets hosted in the cloud are subject to formal change management processes.

C. Data management and security

[redacted]

26. [redacted]

27. [redacted]

[redacted]

[redacted]

28. [redacted]

[redacted]

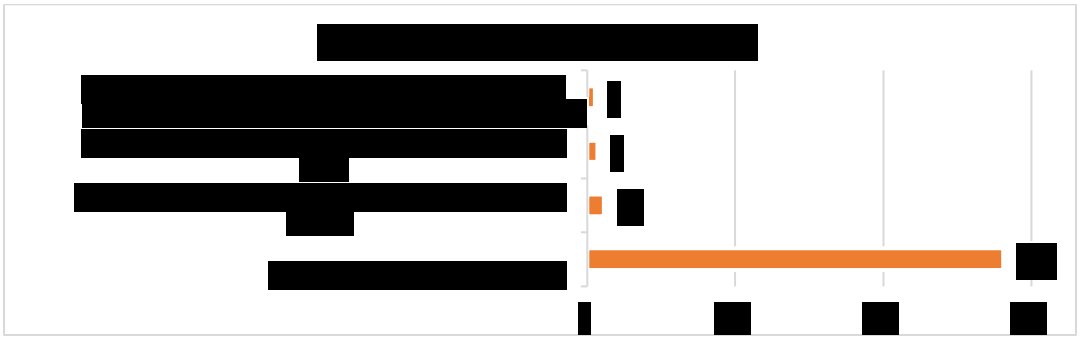
[redacted]

29. [redacted]

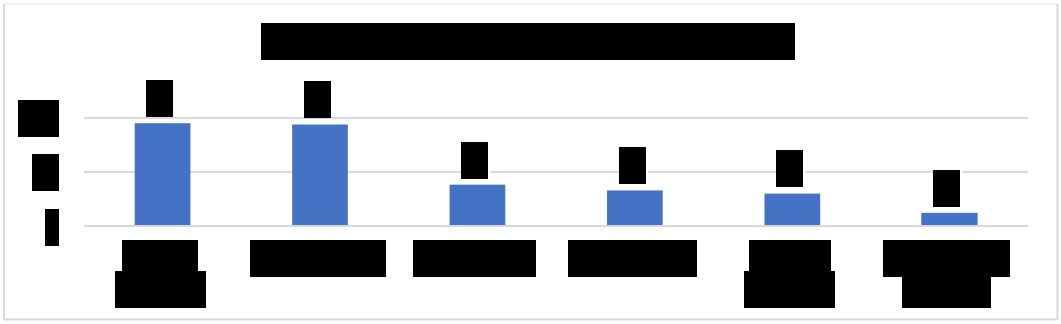
30. [redacted]

31. [redacted]

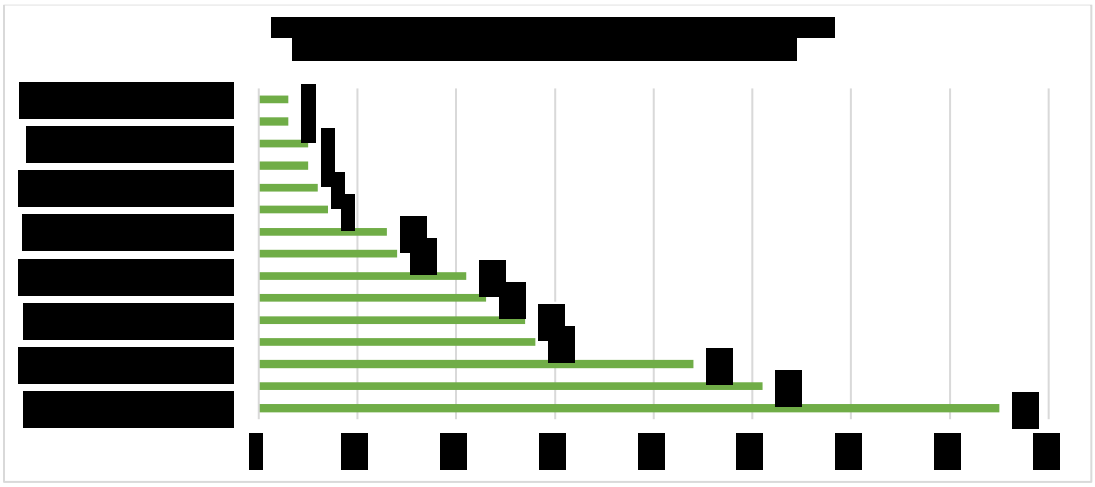
[redacted]



[redacted]



[redacted]



[redacted]

[redacted]

[redacted]

33. [redacted]

34. [redacted]

35. [redacted]

[redacted]

D. Contract and vendor management

Adequate procedures were in place for performance management

36. The whitepaper on the *Use of Cloud Computing in the United Nations System* specifies that service level agreements should be contractually enforceable. Metrics and standards for measuring performance and effectiveness of information management should be established prior to moving into the cloud. UNHCR had arrangements in place for monitoring and enforcing contract, performance metrics and service level compliance for cloud services.

Satisfactory controls were in place for human resources

37. With the steady migration and movement of platform services from UNHCR-owned assets and applications to the cloud, including provisions for the management of personnel, skills and controls became core to the responsibilities of the MSP. Schedule 15 of the agreement defined the MSP's roles and responsibilities regarding personnel matters i.e., description of key positions, vetting as part of onboarding processes and offboarding which included removing all access and disabling accounts. UNHCR also played an important role in the MSP's selection of personnel and monitoring their services through the monthly reports. OIOS obtained a list of MSP personnel from DIST and matched them to data in identity management in the CSP service and no exceptions were noted. UNHCR confirmed that it was satisfied with the skills of MSP personnel and their services and thus re-engaged them for another five years from April 2019.

E. Benefits realization, resilience and availability

There was a need to establish a benefits realization plan for cloud services

38. According to *Cloud Security Alliance (Security Guidance for Critical Areas of Focus in Cloud Computing v4.0)*, cloud computing offers tremendous potential benefits in agility, resiliency, and economy. Organizations can: (i) move faster since they don't have to purchase and provision hardware; (ii) reduce downtime; (iii) save funds due to reduced capital expenses and better demand and capacity matching; and (iv) obtain significant security benefits. The decision to use cloud arrangements should however be supported by a benefits realization plan that lists measurable factors that are used to determine whether the expected benefits are realized. These benefits include cost savings, assured scalability to meet operational needs, continued availability of the systems and efficiencies arising from the increased ability to connect, communicate and share resources outside traditional methods.

39. Migration of applications to the cloud lowered UNHCR's risks relating to continued availability, and technological obsolescence. This was in addition to other benefits such as: improved transparency/visibility and possibility to replicate good ICT initiatives to other operations; reduced local support costs; and improved security. UNHCR explained that all major projects had their own justifications, business cases and benefits realization sections as part of their respective closure reports. However, OIOS noted that there was no consistent identification of benefits across projects that employed cloud technologies. There was thus no basis against which to confirm whether the organization had realized the intended benefits of cloud deployment.

(8)	**The UNHCR Division of Information Systems and Telecommunications should incorporate standard, cloud-specific measures into project benefits realization plans and closure reports for projects implementing cloud technologies.**

UNHCR accepted recommendation 8 and emphasized that major projects had a benefits realization section as part of the project closure report. DIST would continue to strengthen the process and include the cloud specific measures into project benefits realization plans.

IV. ACKNOWLEDGEMENT

40. 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.

(*Signed*) Anne Rwego
Chief, UNHCR Audit Service
Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of cloud arrangements at the Office of United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical[7]/ Important[8]	C/ O[9]	Actions needed to close recommendation	Implementation date[10]
1	The UNHCR Division of Information Systems and Telecommunications should address gaps in the current framework for cloud services and formalize related guidance.	Important	O	Receipt of evidence of the published guidance and framework for cloud services.	
2	The UNHCR Division of Information Systems and Telecommunications should strengthen processes related to documentation and logging of cloud initiatives from online requisition and assessment by teams to final decision.	Important	O	Receipt of evidence that cloud initiatives are consistently supported by requisition and assessment processes.	
3	The UNHCR Division of Information Systems and Telecommunications should strengthen its processes for updating the configuration management database, so it is comprehensive.	Important	O	Receipt of evidence that strengthened processes are in place to identify and include resources in the configuration management database.	
4	The UNHCR Division of Information Systems and Telecommunications should strengthen existing measures to ensure that material changes to assets hosted in the cloud are subject to formal change management processes.	Important	O	Receipt of confirmation that material changes to assets hosted in cloud take place in compliance with established change management process.	
5	[redacted]	[redacted]	[redacted]	[redacted]	

[7] 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.
[8] 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.
[9] Please note the value C denotes closed recommendations whereas O refers to open recommendations.
[10] Date provided by UNHCR in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of cloud arrangements at the Office of United Nations High Commissioner for Refugees

6	[redacted]	[redacted]	[redacted]	[redacted]	
7	[redacted]	[redacted]	[redacted]	[redacted]	
8	The UNHCR Division of Information Systems and Telecommunications should incorporate standard, cloud-specific measures into project benefits realization plans and closure reports for projects implementing cloud technologies.	Important	O	Receipt of evidence confirming inclusion of cloud specific measures into benefits realization plans for projects implementing cloud technologies.	

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of cloud arrangements at the Office of United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical[11]/ Important[12]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	UNHCR comments
1	The UNHCR Division of Information Systems and Telecommunications should address gaps in the current framework for cloud services and formalize related guidance.	Important	Yes	Chief Solution Engineering Section	Q2 2023	DIST will review existing guidance and framework documentation, address any gaps, and formally issue for cloud services.
2	The UNHCR Division of Information Systems and Telecommunications should strengthen processes related to documentation and logging of cloud initiatives from online requisition, assessment by teams, to final decision.	Important	Yes	Dep. Dir IT BRMS with the support of Dep. Dir. IT Site Support and Emergency Mgmt.	Q2 2023	Taking into consideration the existence of formal change management processes, and cloud resource request processes with appropriate validation and approval, DIST will continue to improve the effectiveness of the current implemented processes related to documentation and logging of cloud initiatives
3	The UNHCR Division of Information Systems and Telecommunications should strengthen its processes for updating the configuration management database, so it is comprehensive.	Important	Yes	Head of IT Cross Functional Unit with the support of the IT Service Delivery Managers	Q2 2023	DIST considers that a process is already defined and in place, as following: • Applications/services can be registered in the Configuration Management Database (CMDB) using the Service Catalog, and • Configuration Management guidelines were established in 2020 and cover IAAS, PAAS, & SAAS.

[11] 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.

[12] 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[11]/ Important[12]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	UNHCR comments
						Nevertheless, DIST will review and strengthen the process where required.
4	The UNHCR Division of Information Systems and Telecommunications should strengthen existing measures to ensure that material changes to assets hosted in the cloud are subject to formal change management processes.	Important	Yes	Head of IT Cross Functional Unit with the support of Dep. Dir IT BRMS	Q2 2023	DIST will strengthen existing measures to ensure that material changes to assets hosted in the cloud are subject to formal change management processes.
5	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
6	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
7	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Rec. no.	Recommendation	Critical[11]/ Important[12]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	UNHCR comments
	[redacted]					[redacted]
8	The UNHCR Division of Information Systems and Telecommunications should incorporate standard, cloud-specific measures into project benefits realization plans and closure reports for projects implementing cloud technologies.	Important	Yes	Head of Project Services unit	Q2 2023	DIST would like to emphasize the following: • The "cloud -first strategy" is included in the IT Strategy in line with UN Data Strategy, • Each major project completes its own justification and business case. Furthermore, projects have a benefits realization section as part of the project closure reports. • As part of the acquisition process, DIST follows the procurement standards and uses the existent framework agreements. DIST will continue to strengthen the process and include the cloud specific measures into the project benefits realization plans.