Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2021/040

Audit of cloud services in the United Nations Secretariat

Governance, management and security of cloud services need to be strengthened

31 August 2021
Assignment No. AT2020-517-01

Audit of cloud services in the United Nations Secretariat

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of cloud services in the United Nations Secretariat. The objective of the audit was to assess the adequacy and effectiveness of the governance, risk management and control processes for efficient, effective and secure provision of cloud services in the Secretariat. The audit covered the period from January 2017 to May 2021 and included a review of: (a) governance, risk management and compliance; (b) budget, costing and cost recovery; (c) delivery strategy and architecture; (d) information and communications technology operations and support; (e) cloud change, configuration and asset management; (f) data management; and (g) data security, resilience and availability.

The audit indicated that governance, management and security of cloud services need to be strengthened. OIOS made 11 recommendations. To address the issues identified in the audit, OICT needed to, inter alia:

- Update the cloud strategy based on assessment of the Secretariat's business requirements, and implement change management mechanisms;
- Strengthen cloud governance by establishing effective oversight; ensure that the roles and responsibilities of all service providers and self-managed subscribers are clearly defined; and define metrics and mechanisms for measuring, tracking and reporting of benefits realization;
- Ensure clarity, consistency and transparency of cloud services costs, budget, cost recovery and reporting mechanisms;
- Reassess the current architecture and provide the required integration between the public and private cloud, scalability and flexibility described in the cloud strategy;
- Establish mechanisms to integrate internal and external service support to facilitate timely response and monitoring of service; and establish cloud service-level agreements with external service providers for defining service requirements and monitoring;
- Formalize and update procedures for the request, review and approval of change and configurations management, guardrails and related exceptions;
- Provide clarity to cloud service subscribers on the definition of sensitive and non-sensitive operations; assess the feasibility and develop a plan to relocate data stored in unapproved locations; and define data residency requirements, policies and procedures;
- Define the procedures for assessment, oversight and compliance with information security policies and the use of secure coding practices; and review the results of the Azure console security configurations and implement the recommendations of the independent assessment;
- Strengthen access control mechanisms by reviewing the current architecture for the use of multi-factor authentication across systems and applications; and developing guidance and defining the roles and responsibilities for use of eDiscovery;
- Ensure that all cloud subscribers define their data backup and disaster recovery requirements; and
- Establish Secretariat-wide policies and procedures for end-users to detect, report and promptly respond to data privacy and security incidents.

OICT accepted the recommendations and has undertaken to implement them.

CONTENTS

Audit of cloud services in the United Nations Secretariat

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of cloud services in the United Nations Secretariat.

2. Cloud computing involves the delivery of computing services over the Internet (the cloud) from geographically disparate locations, using a shared and dynamically scalable information and communications technology (ICT) infrastructure. The cloud allows the Secretariat to augment data centre capacity and take advantage of economies of scale, high availability, capacity management, scalability and agility of ICT infrastructure and resources.

3. The Secretary-General's bulletin ST/SGB/2016/11 on the Organization of the Office of Information and Communications Technology (OICT) states that OICT, as the central authority for matters pertaining to ICT, provides leadership for the establishment and implementation of Organization-wide ICT standards and activities in support of programmes and mandates, modernization of information systems, and improvement in the ICT services available to the Organization.

4. In April 2018, the Chief Information and Communications Technology Officer (CITO) approved a cloud strategy which proposes a hybrid, multi-cloud approach and a "cloud first" but not "cloud always" model with emphasis on standardizing platforms for application development and procuring off-the-shelf cloud-based solutions to accelerate the pace with which cloud computing technologies are adopted and used by the Secretariat's entities.

5. OICT and the United Nations Global Service Centre (UNGSC) coordinate the provision of cloud services under the umbrella of a Cloud Centre of Excellence for the Secretariat and serve as cloud brokers. Since the promulgation of the strategy, the Secretariat has established contracts and connectivity with two major public cloud service providers (CSPs). Both offered a range of infrastructure, platforms, tools and software services and products on demand, with a subscription/pay-as-you-go pricing model. Also, there were some pre-existing contracts with other CSPs within the Secretariat (e.g., SAP, Salesforce, Oracle). The cloud service delivery models in use are currently "Software as a Service" (SaaS), "Infrastructure as a Service" (IaaS), and "Platform as a Service" (PaaS). However, with the implementation of the Secretary-General's data strategy, other delivery models such as "Data as a Service" are also being considered.

6. Complete data on the expenditure incurred by the Secretariat for cloud services was not readily available. Based on data obtained from Umoja, the best estimate of the expenditure incurred on cloud services since 2017 was approximately $90 million.

7. Comments provided by OICT are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

8. 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 in the Secretariat.

9. This audit was included in the 2020 risk-based work plan of OIOS due to high risks associated with management of cloud services.

10. OIOS conducted this audit from July 2020 to May 2021. The audit covered the period from January 2017 to May 2021. Based on an activity-level risk assessment, the audit covered risks areas in the management of cloud services which included: (a) governance, risk management and compliance; (b) budget, costing and cost recovery; (c) delivery strategy and architecture; (d) ICT operations and support; (e) cloud change, configuration and asset management; (f) data management; and (g) data security, resilience and availability.

11. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data; and (d) tests of internal controls.

12. 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

The cloud strategy needs to be realigned with business requirements

13. The cloud strategy envisaged that the Secretariat leverages a critical opportunity to achieve innovation, agility and optimize value without compromising security and performance. However, due to lack of change management mechanisms for setting and communicating the change and securing the stakeholders' buy-in, many business users expressed concern that the cloud strategy did not adequately align with their business goals and objectives because they were not involved in requirements analysis, identification of suitable cloud models and mapping requirements. At the time of audit, other than M365 cloud subscriptions, only 14 Secretariat entities/offices had adopted cloud services for their business activities. The need for cloud services has become even more necessary due to the COVID-19 pandemic, the Secretary-General's data strategy, and the shift towards remote working.

(1) OICT should: (a) update the cloud strategy based on a systematic assessment of the Secretariat's business requirements; and (b) implement change management mechanisms to facilitate the adoption of cloud services and stakeholder engagement across the Secretariat.

OICT accepted recommendation and stated that due to the complexity of the United Nations Secretariat, it will take a minimum of 18 months to assess pertinent business requirements, translate these into a systematic assessment and update the strategic guidance on cloud. OICT also stated that change management is part of the overall organizational change management process. Recommendation 1 remains open pending receipt of evidence that: (a) the cloud strategy has been updated based on a systematic assessment of the Secretariat's business requirements; and (b) change management mechanisms have been implemented.

Governance structures, process ownership and enforcement need to be strengthened

14. OICT has responsibility for setting the direction and establishing policies and procedures for ICT across the Secretariat. OICT had defined risk management controls in the ICT Technical Procedure on Cloud Computing. However, guidelines and procedures were required on security operations, resource planning, costing and service support. Without an integrated governance framework for guiding, monitoring and enforcement across the Secretariat, economies of scale, scalability, high availability and

enhanced security described in the cloud strategy may not be achieved. Inadequate governance structures and processes caused the following:

(a) A gap analysis of the current state and the desired state was not conducted to direct and describe the synergy that could be derived from the adoption of cloud services. Requirements were not adequately defined which led to gaps in services provided by CSPs. For instance, 14 services out of 117 described as required were not available. Some of the services were deemed critical for data availability and security.

(b) The risk profile and architecture of cloud services differed from the traditional ICT setup. However, the same ICT security policies applicable to on-premises services were also applied to cloud services. Additional policies and procedures are required to reflect the risk profile of the cloud environment.

(c) Enforcement mechanisms were not adequate to ensure security, effectiveness and efficiencies of migration decisions. Several instances of non-compliance and suboptimal deployments were noted.

[redacted]

(e) Roles and responsibilities between cloud subscribers, internal service providers, and CSPs were not clearly defined for decisions regarding cloud migration, monitoring, data management, data security and support. For instance, many self-managed subscribers were unclear about their responsibilities for disaster recovery. As such, they did not consider it as part of their cloud deployments.

(f) The governance structure was convoluted with various teams responsible for varying elements of the process. For example, 12 teams with overlapping roles and responsibilities were described for similar or related services.

[redacted]

(h) Existing CSP contracts were issued without competitive bidding on the grounds that there was no competition. There was no evidence of cost-benefit and options appraisal to demonstrate that the sole-source selection of CSPs represented best value for money. For example, in the selection of a recent CSP with a not-to-exceed amount of $17.5 million over a five-year period, the statement of award document provided to the Headquarters Committee on Contracts described the basis of award as purchase of equipment/services already standardized. Further, the vendor did not accept the United Nations standard contract template.

(i) A benefits realization plan is used to determine whether the expected benefits of the products deployed have been realized. OICT defined the expected benefits of adopting cloud services which included, amongst others, cost savings ($3.4 million from 2017 to 2020), cybersecurity, scalability and availability. However, OICT did not define any metrics for ensuring that the benefits of the migration to the cloud are achieved.

(2) OICT should: (a) strengthen cloud governance by establishing effective oversight; (b) establish the requirement for conducting procurement due diligence in the selection of future cloud service providers; (c) conduct an assessment of the impact of the missing cloud services and institute compensating controls as appropriate; (d) ensure that the roles and responsibilities of all service providers and self-managed subscribers are clearly defined; (e) enhance existing policies and procedures to reflect the cloud environment risk profile; and (f) define metrics and mechanisms for measuring, tracking and reporting of benefits realization.

OICT accepted recommendation 2. Recommendation 2 remains open pending receipt of evidence that: (a) effective oversight has been established; (b) due diligence procedures in selection of future CSPs has been established; (c) an assessment of missing cloud services has been conducted, and compensating controls instituted; (d) roles of self-managed subscribers have been defined; (e) existing policies and procedures have been enhanced; and (f) metrics and mechanisms have been defined for measuring, tracking and reporting of benefits realization.

B. Budget, costing and cost recovery

Need to improve budgeting, costing and cost recovery for cloud services

15. Best practices require that the key elements of a project are monitored at each stage, and that total cost of ownership is tracked against budget.

16. Umoja data indicated that the Secretariat had paid approximately $90 million to CSPs. However, there was no visibility over costs (i.e., posts, consultancies, contracts, maintenance and cloud support costs) including the quantitative and qualitative value and benefits of adopting cloud services. Further, there was no central mechanism whereby the costs of cloud services are tracked and monitored for the entire Secretariat. OICT explained that there was no project cost, and deployments were funded within existing resources.

17. Cloud services are funded on a cost recovery model based on licenses or a consumption/pay-as-you-go model with monthly/quarterly cost recovery from consumers. The cost applicable to entities using the Azure services are defined in a cloud service level agreement (C-SLA), and for M365 services, subscribers are pre-assessed in advance, based on rate cards approved by the Controller. OIOS noted the following:

(a) There was no standardization and consistency of the charges to consumers of cloud services within the Secretariat. The basis for deriving the charges for cost recovery was not transparent.

(b) Cloud subscribers expressed dissatisfaction that there were no economies derived from the brokerage model of service obtained via OICT/UNGSC, and that it was cheaper to go to CSPs directly. For example, one CSP gave the Secretariat a 15 per cent discount but there was no visibility on whether the discount had been transferred to subscribers.

(c) A cloud consumption assessment was done for M365-related services and a projection submitted to the vendor in October-November for the next year. However, in situations where an entity has over-projected, there is no ability to revise downwards until the next revision period, whereas the entity can revise the assessment in cases of under-projection. With regard to services for IaaS- and PaaS-based cloud services, OICT had deployed tools to track consumption rates, but not at the granularity required to inform decision making. Also, no templates were provided to self-managed subscribers to guide them in determining future cloud consumption capacity across all CSPs.

(3) OICT should: (a) ensure clarity, consistency and transparency of cloud services costs, budget, cost recovery and reporting mechanisms; and (b) develop guidance and templates to facilitate cloud consumption assessments for planning and budgeting purposes.

OICT accepted recommendation 3. Recommendation 3 remains open pending receipt of evidence that: (a) procedures have been established to ensure clarity, consistency and transparency of cloud services costs, budget, cost recovery and reporting mechanisms; and (b) guidance and templates have been developed to facilitate cloud consumption assessments for planning and budgeting purposes.

C. Delivery strategy and architecture

Need to strengthen cloud migration strategy, skill set and architecture

18. The cloud strategy defined a vision of an end state that will: (a) synchronize and/or replicate data between public and private clouds; (b) migrate services on a continuous basis between public and private clouds; (c) optimize balance between high control, easy adoption, and economies of scale; (d) balance use of internal assets and external services; and (e) reduce 75 per cent of the data centre footprint by 2021.

19. A systematic and documented cloud migration strategy is essential for moving from an on-premises architecture to the cloud and should include a well-defined cloud architecture that validates the most efficient and secure way to prioritize and migrate. In the ICT Technical Procedure on Cloud Computing, OICT defined some success criteria for deployment into the cloud, including the role of the Enterprise Architecture Task Force (EATF) in reviewing compliance and confirming that the architecture of the proposed system meets functional and quality requirements. A Unite Cloud Reference Architecture and Unite Cloud Administrator Guide were also prepared to capture any approved changes.

20. OIOS conducted a gap analysis of the proposed end state vis-à-vis the actual end state and identified that some parts of the implemented cloud architecture did not align with the end state vision. The results of the analysis indicated that an effective and secure cloud migration strategy was yet to be implemented. OIOS noted the following:

(a) The Cloud business case described the mixture of public and private cloud deployments that will allow the Secretariat to transition applications, resources and data deployment between public and private infrastructure based on needs or organizational policies. However, the current architecture did not show any integration between the public and private cloud to facilitate this vision. Many subscribers expressed concern at the inability to use a hybrid model. For example, one entity explained that it would like to keep its applications in the cloud and its databases on-premises but was unable to do so due to lack of integration between the public and private cloud.

(b) One of the critical success factors of the migration to the cloud is the availability of knowledgeable and skilled resources. No assessment had been conducted to identify skills gaps. Consequently, some self-managed subscribers were unable to effectively document an architecture for effective, efficient and secure deployment in a cloud native way. OICT stated that it does not have the resources to support the skills gap. If this gap is not addressed, there is a risk of migrating assets and resources in an inefficient and insecure manner.

(c) The role of EATF needs to be strengthened in regard to oversight of the deployment of cloud services and its ability to provide some advisory/support function to assist subscribers until maturity. However, EATF had only one full-time member out of a membership of five, which limited its visibility and ability to review migration documents in a timely manner.

(d) Many members of the cloud user community stated that there was no centralized forum (Community of Practices) within the Secretariat to facilitate knowledge management, track best practices and lessons learned across cloud deployments within the Secretariat.

(e) The ability to deploy services and resources (servers and infrastructure) into the cloud effectively and efficiently depends on availability of automated tools across the migration process, as well as the automation of workflows. OIOS noted that the tools were insufficient, and many processes required manual authorization and verification which was time and resource intensive.

(4) OICT should: (a) reassess the current architecture and provide the required integration between the public and private cloud, scalability and flexibility described in the cloud strategy; (b) implement mechanisms to address the resource gap related to knowledge, skills and tools; (c) strengthen the role of the Enterprise Architecture Task Force; and (d) establish a Community of Practice to facilitate knowledge management, tracking of best practices and lessons learned.

OICT accepted recommendation 4. Recommendation 4 remains open pending receipt of evidence that: (a) the current architecture has been reassessed to provide integration, scalability and flexibility; (b) mechanisms have been implemented to address resource gaps related to knowledge, skills and tools; (c) role of EATF has been strengthened; and (d) a Community of Practice has been established.

D. ICT operations and support

Need to strengthen cloud production support mechanism

21. As the Secretariat migrates from the traditional on-premises infrastructure to rely more on CSPs for infrastructure, platforms, applications and data, C-SLAs are fundamental to describe the minimum level of service, levels of reliability, availability, responsiveness and roles and responsibilities amongst service subscribers and service providers. C-SLAs should also define the metrics for measuring performance, and penalties if service levels are not met. The ICT Technical Procedure on Cloud Computing specifies 38 core components that should, at a minimum, describe the CSP capabilities and their related service objectives in each of the 38 core requirements.

22. OIOS' assessment of the effectiveness of production support indicated that processes and criteria for measuring performance of cloud production support were not well defined, and production support structure and processes had not been realigned to accommodate the complexities of cloud service provision and its integration with existing ICT production support mechanisms. The following were noted:

(a) The production support mechanism was multi-layered, involving both internal and external support teams. However, there was no integration amongst the teams to facilitate timely response to service requests, and monitoring of incidents and problem resolution.

(b) Internal C-SLAs between OICT/UNGSC and self-managed subscribers were not consistently aligned to the 38 core elements. Also, 7 out of 11 self-managed subscribers did not have C-SLAs in place. The four self-managed subscribers with C-SLAs did not have 29 out of the 38 core elements defined. These included intellectual property, data retention, data incidents, data location requirements, and support response. Also, quarterly compliance monitoring reports were not consistently produced.

(c) The internal mechanisms for supporting cloud-related service requests needs to be realigned. There were 24 different support groups in iNeed for cloud services, without any description of their roles and responsibilities. The current process was not optimal and created confusion among the cloud service subscribers regarding which support group to address service requests to, leading to delays.

(d) Some service requests were raised directly to the external CSP, while some were raised through the Unite Service Desk for similar issues. However, due to lack of integration between internal and external support mechanisms, there was limited visibility over issues raised directly, their nature and criticality, which may lead to unapproved changes and service inefficiencies. Between 1 July 2019 and 31 March 2021, the external CSP received 712 service requests whereas Unite Service Desk received 1,510 service requests for the period 1 October 2019 to 31 March 2021. There was no central analysis of both data streams.

(e) OIOS' analysis of the Unite Service Desk service requests and cases raised with the external CSP during the period 2019-2021 indicated that there were no standardized criteria for prioritizing internal service requests in C-SLAs vis-à-vis prioritization levels in iNeed (see Table 1). Without standardized criteria, performance against the C-SLA cannot be achieved.

Table1: Priority levels of internal service requests

C-SLA	iNeed
Urgent	1-Critical
High	2-High
Normal	3-Medium
Low	4-Low
Question	5-Question

(f) There was no consistent approach to documenting C-SLAs across the varying types of service providers (internal and external). C-SLAs between the Secretariat and the major external CSP were based on a generic list of C-SLAs published by the vendor on its website. The Secretariat did not assess the generic list for applicability and adequacy. OIOS reviewed the generic C-SLAs of CSPs and noted that they referred only to general conditions of service availability, without defining the acceptable service levels, performance metrics and enforcement mechanisms. The absence of clearly defined C-SLAs with external CSPs caused delayed resolution of cloud support issues. Further, there were no baselines for determining and monitoring potential contract breaches.

(g) An ageing analysis of open and pending internal requests indicated that there was no mechanism for reviewing and resolution of delayed cloud service requests. The average number of business days taken to resolve internal service requests for Azure and M365 were 13 and 28, respectively.

(5) OICT should: (a) establish mechanisms to integrate internal and external service support to facilitate timely response and monitoring of service; (b) establish cloud service-level agreements with external service providers for defining service requirements and monitoring; and (c) standardize the criteria for prioritizing internal service requests in the Cloud service-level agreements vis-à-vis prioritization levels in iNeed.

OICT accepted recommendation 5. Recommendation 5 remains open pending receipt of evidence that: (a) mechanisms have been established to integrate internal and external service support; (b) C-SLAs have been established with external service providers; and (c) the criteria for prioritizing internal service requests have been standardized.

E. Cloud change, configuration and asset management

Cloud change, configuration and asset management processes need to be strengthened

23. The adoption of cloud computing necessitates implementing effective change and configuration management procedures and tools to assure better oversight and monitoring of all changes across the entire cloud infrastructure and to ensure that the related assets and resources (configuration items) are tracked, logged and managed.

24. Existing change and configuration management policies, procedures and guidelines had not been updated to reflect the different change management requirements unique to the cloud computing environment. OIOS noted the following:

(a) Inter-dependencies between various configuration items were not adequately captured, and there was limited visibility of the processes and relation between parts, subsystems, and systems of cloud computing across the Secretariat. This information is required for ensuring a secure cloud environment, including timely visibility of security vulnerabilities.

(b) The procedures for granting emergency configurations and changes were not defined for the cloud scenario. Further, there were no pre-approved changes for cloud related scenarios which caused delays and by-passing of internal change management procedures to CSPs to make system changes. OICT agreed that there is a need for change and configuration management mechanisms to be revised to ensure a holistic and more dynamic approach that is aligned to the requirements of the Secretariat's cloud strategy.

(c) There was no integrated change management tool within the Secretariat to facilitate end-to-end change management. Multiple tools existed across the Secretariat with no interface and common criteria for tracking and monitoring. Therefore, the ability to globally track and review changes, including those performed by CSPs, was limited. For instance, the CSP did not notify the Secretariat of the breakout rooms enhancement in Teams, and applicable test scenarios were not conducted to assess the possible impact on the Secretariat's infrastructure. In another case, the CSP established a portal through which all requests for change, configurations or tickets could be raised directly without OICT/UNGSC having access to the portal.

(d) Minimum-security policies and 31 guardrails (Unite Cloud Azure Guardrails v1.0 (PROD)) were implemented for self-managed subscribers to enable control over changes and configurations to code, network pipelines and data locations. However, the implementation of guardrails was not subject to any change and configuration management procedures. Further, exceptions were allowed without a formalized process for review and approval. Without a systematic approach for assessing exemptions, inappropriate exemptions may be granted which may put the cloud infrastructure at risk (for example, a recent request for policy exception to install resources in a non-approved data location).

25. Cloud asset management provides visibility and control of all the assets and infrastructure in the cloud environment and facilitates their optimization and security. The Secretariat did not have visibility over cloud-based assets because there was no inventory. A cloud inventory is required to manage the discovery of assets that are non-compliant with policies and procedures.

(6) OICT should formalize and update procedures for the request, review and approval of change and configurations management, guardrails and related exceptions.

OICT accepted recommendation 6 and stated that there is a change management process implemented for managed subscriptions, but the process for modifications related with guardrails and exceptions needs to be refined. Recommendation 6 remains open pending receipt of evidence that procedures for the request, review and approval of change and configurations management, guardrails and related exceptions have been standardized and updated.

F. Data management

Need to define data residency and retention requirements for cloud services

26. In April 2020, the Secretary-General promulgated a data strategy which identified the need to build capabilities in data management and analytics. It is envisaged that the cloud infrastructure will be an enabler in facilitating data analytics and the use of data as a strategic resource/asset. Further, with the transition to remote working necessitated by the COVID-19 pandemic, effective data governance and management procedures are required for cloud deployments within the Secretariat to ensure the success of the cloud and data strategies. OIOS noted the following:

(a) The cloud project business case envisaged reliance on the public cloud for non-sensitive operations and on the private cloud for critical, particularly sensitive operations. However, there was no definition of sensitive vis-à-vis non-sensitive operations, and there were no clear policies and procedures on what should be migrated into the cloud and what should not be. Further, the lack of effective data classification mechanisms made it difficult to identify resources that are sensitive as opposed to non-sensitive. Consequently, data is currently migrated into the cloud without regard to sensitivity. For example, SharePoint Online has been approved as the proposed cloud solution for document management for storage and management of unclassified and confidential content only, and not for strictly confidential content.

(b) There were no policies regarding data retention and archiving within the cloud environment. Data retention requirements were not defined for most deployments and by default, they were held indefinitely by CSPs. OICT explained that it was in the process of revising the ICT Technical Procedure on Data Retention. The absence of retention and archiving policies and procedures for documents stored in the cloud environment exposed data to loss or retention for longer than necessary. Further, data disposal requirements were not specified to ensure secure and logged disposal.

(c) Defining data residency is a best practice for controlling the processing, transfer and storage of classified data within approved geolocations. There were limited data residency procedures and guidelines to direct cloud service subscribers on approved locations to store data within the cloud environment. OIOS' review of the contract terms of an external CSP showed that the Secretariat's data residency requirements were not specified in the contract. OICT explained that Azure cloud data locations were at the discretion of cloud subscribers. To mitigate this risk, OICT implemented data residency guardrails to limit the storage of Secretariat data to only pre-approved locations. However, the guardrails were configured after deployment of data by many cloud subscribers and would require additional effort to enforce retroactively. OIOS' review of eight major self-managed deployments showed that four deployments had data residing in East US2, which was not an approved location in the guardrail.

(7) OICT should: (a) provide clarity to cloud service subscribers on the definition of sensitive and non-sensitive operations; (b) finalize the updated ICT Technical Procedure on Data Retention; (c) assess the feasibility and develop a plan to relocate data stored in

unapproved locations; and (d) define data residency requirements, policies and procedures.

OICT accepted recommendation 7 but stated with regard to item (d) that there are no general residency requirements for the United Nations Secretariat as a whole. OIOS is of the view that, to prevent inappropriate storage of the Secretariat's sensitive information in unapproved and/or high-risk locations, OICT needs to define data residency requirements in consultation with the Office of Legal Affairs. Recommendation 7 remains open pending receipt of evidence that: (a) the definition of sensitive and non-sensitive operations has been clarified; (b) ICT Technical Procedure on Data Retention has been finalized; (c) a feasibility assessment and plan has been developed to relocate data stored in unapproved locations; and (d) data residency requirements, policies and procedures have been defined.

G. Data security, resilience and availability

Need to strengthen controls for secure deployment and use of cloud computing

[redacted]

[1] 'DevSecOps' stands for development, security, and operations; it involves utilizing security best practices from the beginning of development, shifting the focus on security away from auditing at the end and towards development in the beginning using a shift-left strategy.

[redacted]

[redacted]

[redacted]

(8) OICT should: (a) define the procedures for assessment, oversight and compliance with information security policies and the use of secure coding practices; and (b) review the results of the Azure console security configurations and implement the recommendations of the independent assessment.

OICT accepted recommendation 8. Recommendation 8 remains open pending receipt of evidence that: (a) the procedures for assessment, oversight and compliance with information security policies and the use of secure coding practices have been defined; and (b) the results of the Azure console security configurations have been reviewed and the recommendations of the independent assessment have been implemented.

Need to strengthen cloud services access management

[redacted]

[redacted]

(9) OICT should strengthen access control mechanisms by: (a) reviewing the current architecture for the use of multi-factor authentication across systems and applications; and (b) developing guidance and defining the roles and responsibilities for use of eDiscovery.

OICT accepted recommendation 9. Recommendation 9 remains open pending receipt of evidence that: (a) the current architecture for the use of multi-factor authentication has been strengthened; and (b) guidance has been developed and roles and responsibilities defined for the use of eDiscovery.

Data backup and disaster recovery requirements need to be defined

29. Documentation of data backup requirements and implementation of disaster recovery arrangements ensure availability and restoration of services or system within the tolerable outage time for key business processes. Existing deployments did not always consider back up and disaster recovery before deployment into the cloud. OIOS noted the following:

(a) Although OICT/UNGSC stated that the Secretariat had a standard disaster recovery policy, no evidence was provided as to how this has been embedded into the cloud architecture and communicated to CSPs. There was a perception among self-managed subscribers that cloud services do not require disaster recovery as such, and many did not consider recovery time and resilience requirements.

(b) A number of self-managed subscribers had not opted for backup of their data or defined their disaster recovery mechanisms, thereby exposing systems and data to availability risks. Out of nine self-managed subscribers reviewed, eight had not defined backup and disaster recovery requirements.

(10) OICT should ensure that all cloud subscribers define their data backup and disaster recovery requirements.

OICT accepted recommendation 10 and stated that currently this is part of the EATF review process. Recommendation 10 remains open pending receipt of evidence that procedures have been established to ensure that all cloud subscribers define their data backup and disaster recovery requirements.

Need to strengthen data incident management procedures

30. Incident management procedures should be established to monitor data incidents, determine the magnitude of the threat presented by them, and promptly respond to incidents in a way that limits damage and reduces recovery time and costs. Further, all Secretariat personnel should be aware of such procedures.

[redacted]

32. Without clear policies and procedures, the Secretariat was unable to manage data incidents effectively and take appropriate mitigating actions in a timely manner.

(11) OICT should establish Secretariat-wide policies and procedures for end-users to detect, report and promptly respond to data privacy and security incidents.

OICT accepted recommendation 11. Recommendation 11 remains open pending receipt of evidence that Secretariat-wide policies and procedures have been established for end-users to detect, report and promptly respond to data privacy and security incidents.

IV. ACKNOWLEDGEMENT

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

(*Signed*) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of cloud services in the United Nations Secretariat

Rec. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	OICT should: (a) update the cloud strategy based on a systematic assessment of the Secretariat's business requirements; and (b) implement change management mechanisms to facilitate the adoption of cloud services and stakeholder engagement across the Secretariat.	Important	O	Receipt of evidence that: (a) the cloud strategy has been updated based on a systematic assessment of the Secretariat's business requirements; and (b) change management mechanisms have been implemented.	1 March 2023
2	OICT should: (a) strengthen cloud governance by establishing effective oversight; (b) establish the requirement for conducting procurement due diligence in the selection of future cloud service providers; (c) conduct an assessment of the impact of the missing cloud services and institute compensating controls as appropriate; (d) ensure that the roles and responsibilities of all service providers and self-managed subscribers are clearly defined; (e) enhance existing policies and procedures to reflect the cloud environment risk profile; and (f) define metrics and mechanisms for measuring, tracking and reporting of benefits realization.	Important	O	Receipt of evidence that: (a) effective oversight has been established; (b) due diligence procedures in selection of future CSPs has been established; (c) an assessment of missing cloud services has been conducted, and compensating controls instituted; (d) roles of self-managed subscribers have been defined; (e) existing policies and procedures have been enhanced; and (f) metrics and mechanisms have been defined for measuring, tracking and reporting of benefits realization.	1 March 2023
3	OICT should: (a) ensure clarity, consistency and transparency of cloud services costs, budget, cost recovery and reporting mechanisms; and (b) develop guidance and templates to facilitate cloud consumption assessments for planning and budgeting purposes	Important	O	Receipt of evidence that: (a) procedures have been established to ensure clarity, consistency and transparency of cloud services costs, budget, cost recovery and reporting mechanisms; and (b) guidance and templates have been developed to facilitate cloud consumption assessments for planning and budgeting purposes.	1 March 2022
4	OICT should: (a) reassess the current architecture and provide the required integration between the public and	Important	O	Receipt of evidence that: (a) the current architecture has been reassessed to provide	1 March 2023

[2] 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.

[3] 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.

[4] Please note the value C denotes closed recommendations whereas O refers to open recommendations.

[5] Date provided by [entity] in response to recommendations. [Insert "Implemented" where recommendation is closed; (implementation date) given by the client.]

STATUS OF AUDIT RECOMMENDATIONS

Audit of cloud services in the United Nations Secretariat

	private cloud, scalability and flexibility described in the cloud strategy; (b) implement mechanisms to address the resource gap related to knowledge, skills and tools; (c) strengthen the role of the Enterprise Architecture Task Force; and (d) establish a Community of Practice to facilitate knowledge management, tracking of best practices and lessons learned.			integration, scalability and flexibility; (b) mechanisms have been implemented to address resource gaps related to knowledge, skills and tools; (c) role of EATF has been strengthened; and (d) a Community of Practice has been established.	
5	OICT should: (a) establish mechanisms to integrate internal and external service support to facilitate timely response and monitoring of service; (b) establish Cloud service-level agreements with external service providers for defining service requirements and monitoring; and (c) standardize the criteria for prioritizing internal service requests in the cloud service-level agreements vis-à-vis prioritization levels in iNeed.	Important	O	Receipt of evidence that: (a) mechanisms have been established to integrate internal and external service support; (b) C-SLAs have been established with external service providers; and (c) the criteria for prioritizing internal service requests have been standardized.	1 March 2022
6	OICT should formalize and update procedures for the request, review and approval of change and configurations management, guardrails and related exceptions.	Important	O	Receipt of evidence that procedures for the request, review and approval of change and configurations management, guardrails and related exceptions have been standardized and updated.	1 March 2022
7	OICT should: (a) provide clarity to cloud service subscribers on the definition of sensitive and non-sensitive operations; (b) finalize the updated ICT Technical Procedure on Data Retention; (c) assess the feasibility and develop a plan to relocate data stored in unapproved locations; and (d) define data residency requirements, policies and procedures.	Important	O	Receipt of evidence that: (a) the definition of sensitive and non-sensitive operations has been clarified; (b) ICT Technical Procedure on Data Retention has been finalized; (c) a feasibility assessment and plan has been developed to relocate data stored in unapproved locations; and (d) data residency requirements, policies and procedures have been defined.	30 June 2022
8	OICT should: (a) define the procedures for assessment, oversight and compliance with information security policies and the use of secure coding practices; and (b) review the results of the Azure console security configurations and implement the recommendations of the independent assessment.	Important	O	Receipt of evidence that: (a) the procedures for assessment, oversight and compliance with information security policies and the use of secure coding practices have been defined; and (b) the results of the Azure console security configurations have been reviewed and the recommendations of the independent assessment have been implemented.	1 March 2022

STATUS OF AUDIT RECOMMENDATIONS

Audit of cloud services in the United Nations Secretariat

9	OICT should strengthen access control mechanisms by: (a) reviewing the current architecture for the use of multi-factor authentication across systems and applications; and (b) developing guidance and defining the roles and responsibilities for use of eDiscovery.	Important	O	Receipt of evidence that: (a) the current architecture for the use of multi-factor authentication has been strengthened; and (b) guidance has been developed and roles and responsibilities defined for the use of eDiscovery.	1 July 2022
10	OICT should ensure that all cloud subscribers define their data backup and disaster recovery requirements.	Important	O	Receipt of evidence that procedures have been established to ensure that all cloud subscribers define their data backup and disaster recovery requirements.	1 March 2022
11	OICT should establish Secretariat-wide policies and procedures for end-users to detect, report and promptly respond to data privacy and security incidents.	Important	O	Receipt of evidence that Secretariat-wide policies and procedures have been established for end-users to detect, report and promptly respond to data privacy and security incidents.	30 June 2022

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of cloud services in the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted ? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OICT should: (a) update the cloud strategy based on a systematic assessment of the Secretariat's business requirements; and (b) implement change management mechanisms to facilitate the adoption of cloud services and stakeholder engagement across the Secretariat.	Important	Yes	Chief, Technology Operations - OSD/OICT	1 March 2023	a) Due to the complexity of the UN Secretariat, it will take a minimum of 18 months to assess all the pertinent business requirements and to translate these into a systematic assessment and subsequently update the cloud strategy strategic guidance. b) As per above, this change management is an undertaking in a broader and wider organizational change management process.
2	OICT should: (a) strengthen cloud governance by establishing effective oversight; (b) establish the requirement for conducting procurement due diligence in the selection of future Cloud Service Providers; (c) conduct an assessment of the impact of the missing cloud services and institute compensating controls as appropriate; (d) ensure that the roles and responsibilities of all service providers and self-managed subscribers are clearly defined; (e) enhance existing policies and procedures to reflect the cloud environment risk profile; and (f) define metrics and mechanisms for measuring, tracking and reporting of benefits realization.	Important	Yes	1) Chief, Technology Operations - OSD/OICT 2) Chief, Service and Information Security Management Section - UNGSC	1 March 2023	

[1] 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.

[2] 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.

Management Response

Audit of cloud services in the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted ? (Yes/No)	Title of responsible individual	Implementation date	Client comments
3	OICT should: (a) ensure clarity, consistency and transparency of cloud services costs, budget, cost recovery and reporting mechanisms; and (b) develop guidance and templates to facilitate cloud consumption assessments for planning and budgeting purposes.	Important	Yes	Chief, Service and Information Security Management Section - UNGSC	1 March 2022	
4	OICT should: (a) reassess the current architecture and provide the required integration between the public and private cloud, scalability and flexibility described in the cloud strategy; (b) implement mechanisms to address the resource gap related to knowledge, skills and tools; (c) strengthen the role of the Enterprise Architecture Task Force; and (d) establish Community of Practice to facilitate knowledge management, tracking of best practices and lessons learned.	Important	Yes	1) Chief, Cyber Security Service - OICT 2) Chief, Technology Operations - OSD/OICT	1 March 2023	
5	OICT should: (a) establish mechanisms to integrate internal and external service support to facilitate timely response and monitoring of service; (b) establish Cloud service-level agreements with external service providers for defining service requirements and monitoring; and (c) standardize the criteria for prioritizing internal service requests in the Cloud service-level agreements vis-à-vis prioritization levels in iNeed.	Important	Yes	Chief, Service and Information Security Management Section - UNGSC	1 March 2022	
6	OICT should formalize and update procedures for the request, review and	Important	Yes	1) Chief, Service and Information	1 March 2022	UNGSC: There is a change management process implemented for managed subscriptions but the

Management Response

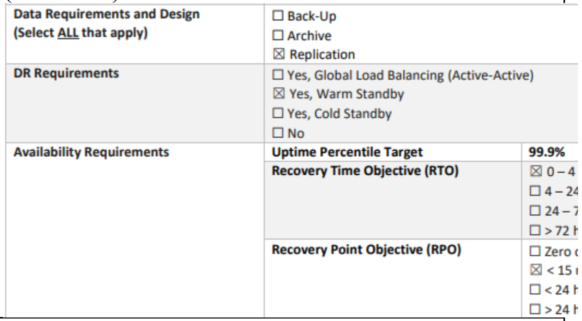
Audit of cloud services in the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	approval of change and configurations management, guardrails and related exceptions.			Security Management Section - UNGSC 2) Chief Infrastructure and Operations Section - UNGSC		process for modifications related with guardrails and exceptions needs to be refined.
7	OICT should: (a) provide clarity to cloud service subscribers on the definition of sensitive and non-sensitive operations; (b) finalize the updated ICT Technical Procedure on Data Retention; (c) assess the feasibility and develop a plan to relocate data stored in unapproved locations; and (d) define data residency requirements, policies and procedures.	Important	Yes (except d)	Director, PSGD/OICT	30 June 2022	d) PSGD – not accepted There are no general residency requirements for the UN Secretariat as a whole.
8	OICT should: (a) define the procedures for assessment, oversight and compliance with information security policies and the use of secure coding practices; and (b) review the results of the Azure console security configurations and implement the recommendations of the independent assessment.	Important	Yes	1) Chief, Technology Operations - OSD/OICT 2) Chief Infrastructure and Operations Section - UNGSC 3) Chief, Cyber Security Service - OICT	1 March 2022	

APPENDIX I

Management Response

Audit of cloud services in the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
9	OICT should strengthen access control mechanisms by: (a) reviewing the current architecture for the use of multi-factor authentication across systems and applications; and (b) developing guidance and defining the roles and responsibilities for use of eDiscovery.	Important	Yes	1) Chief, Cyber Security Service 2) Chief, Technology Operations - OSD/OICT	1 July 2022	
10	OICT should ensure that all cloud subscribers define their data backup and disaster recovery requirements.	Important	Yes	Chief Infrastructure and Operations Section - UNGSC	1 March 2022	UNGSC: This is currently part of the Enterprise Architecture Task Force (EATF) review process and documentation as per screenshot below (Section 7):  **Data Requirements and Design (Select ALL that apply)**: ☐ Back-Up ☐ Archive ☒ Replication **DR Requirements**: ☐ Yes, Global Load Balancing (Active-Active) ☒ Yes, Warm Standby ☐ Yes, Cold Standby ☐ No **Availability Requirements** **Uptime Percentile Target**: **99.9%** **Recovery Time Objective (RTO)**: ☒ 0 – 4 ☐ 4 – 24 ☐ 24 – 7 ☐ > 72 h **Recovery Point Objective (RPO)**: ☐ Zero ☒ < 15 ☐ < 24 h ☐ > 24 h
11	OICT should establish Secretariat-wide policies and procedures for end-users to detect, report and promptly respond to data privacy and security incidents.	Important	Yes	Director, PSGD/OICT	30 June 2022	