Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2020/003

Audit of processes for the development and acquisition of software applications at the United Nations Secretariat

The regulatory framework needs to be strengthened to improve efficient and effective development and acquisition of software applications across the Secretariat

12 February 2020
Assignment No. AT2019/517/02

Audit of processes for the development and acquisition of software applications at the United Nations Secretariat

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of processes for the development and acquisition of software applications at the United Nations Secretariat. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes in ensuring that the processes for software development and acquisition at the United Nations Secretariat are efficient and effective. The audit covered the period from January 2012 to September 2019 and included: (a) regulatory framework and governance mechanisms; (b) acquisition planning and procurement of software applications; and (c) software development lifecycle and production support.

The audit showed that the regulatory framework needs to be strengthened to improve efficient and effective development and acquisition of software applications across the Secretariat. To address issues identified in the audit, the Office of Information and Communications Technology (OICT) needed to:

- Strengthen the regulatory framework for software development and acquisition by: ensuring that Information and Communications Technology (ICT) committees are constituted and meet periodically, as appropriate; finalizing the delegation of authority for ICT; providing direction on information security compliance and ensuring entities certify their compliance with ICT security policies and standards; clarifying the methodology for costing and sharing of application acquisition and support costs; establishing an effective mechanism to globally track the total cost of ownership of ICT applications; and implementing the decision of the General Assembly establishing Vienna as an Enterprise Application Centre.

- Establish appropriate mechanisms in consultation with the Office of Legal Affairs to protect the Organization’s intellectual property for internally developed software; and require all entities within the Secretariat to identify internally developed software that need such protection so that appropriate protection could be secured.

- Provide guidance on the types of system development life cycle methodologies appropriate for projects based on their size and complexity; and provide a standardized collaboration tool for the software development life cycle.

- Identify the mandatory data fields in the UniteApps portfolio and ensure that mandatory data is captured; require all offices to clean up their portfolio of systems in UniteApps and update it with the required information; and identify the critical applications, update the UniteApps database accordingly, and require the preparation of disaster recovery plans for those applications.

The United Nations Office at Vienna (UNOV)/United Nations Office on Drugs and Crime (UNODC) needed to:

- Finalize its ICT reorganization and disseminate revised job descriptions to the affected staff members; strengthen controls to ensure that the project costs charged are accurate and justified; establish service level agreements and associated metrics for all active applications; define future operating objectives for the surplus accrued from the ‘goPortfolio’ application; and stop the practice of using credit cards for purchasing software.

OICT and UNOV/UNODC accepted the recommendations and have initiated action to implement them.

CONTENTS

Audit of processes for the development and acquisition of software applications at the United Nations Secretariat

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of processes for the development and acquisition of software applications at the United Nations Secretariat.

2. In terms of the Secretary-General's bulletin ST/SGB/2016/11 on the organization of the Office of Information and Communications Technology (OICT), as the central authority for matters pertaining to information and communications technology (ICT) software development and acquisition, OICT 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.

3. The United Nations Secretariat's ICT strategy (Secretary-General's report A/69/517, which was endorsed by General Assembly resolution 69/262) defines the ICT roadmap for the global Secretariat beginning in October 2014. It provides a common vision for ICT service delivery through modernization, transformation, and innovation and establishes a framework for improved governance, strong leadership and optimal use of ICT resources to support effective decision-making. The Enterprise Application Centres (EACs) in New York, Bangkok and Vienna, as well as four Regional Technology Centres, are key service delivery pillars of OICT activities.

4. OICT oversees the Secretariat's ICT operations to ensure compliance with policies, standards and the ICT strategy by: (a) coordinating Secretariat-wide ICT resource planning and budget formulation, workforce planning and performance reporting; (b) coordinating global ICT acquisition and contract management; (c) developing guidance for management and reporting of ICT software assets in coordination with the Department of Operational Support (DOS) and the Department of Management Strategy, Policy and Compliance (DMSPC); and (d) developing ICT investment plans.

5. The Procurement Division of DOS has the responsibility, amongst others, to: (a) conduct efficient, effective and timely procurement of goods and services for all entities of the Secretariat; (b) provide procurement support services including technical advice on local procurement and acquisition issues; (c) ensure implementation of the United Nations Financial Regulations and Rules (FRR) and policies during the full software acquisition cycle from requisition, tendering, contract award process, contract negotiation and contract administration with due regard to good industry practices; and (d) conduct compliance and peer reviews in the Secretariat.

6. The Communications and Information Technology Sections in field missions and Offices away from Headquarters are responsible for defining the specifications of their ICT requirements.

7. According to the major commodity statistics for ICT goods and services published by the Procurement Division, the total value of procurement of ICT goods and services in 2017 and 2018 was $424.3 million and $369 million, respectively.

8. The functions of the Office of the Director-General of the United Nations Office at Vienna (UNOV) are combined with those of the Executive Director of the United Nations Office on Drugs and Crime (UNODC). Both offices are integrated and supported with resources from the regular budget as well as extrabudgetary funds. UNOV/UNODC's 2019 budget for software development and acquisition was $6.8 million, which represented 48.8 per cent of their total ICT budget.

9. Comments provided by DMSPC, OICT and UNOV/UNODC are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

10. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes in ensuring that the processes for software development and acquisition at the United Nations Secretariat are efficient and effective.

11. This audit was included in the 2019 risk-based work plan of OIOS due to the risk that potential weaknesses in processes for acquisition and development of software applications could affect the achievement of the Secretariat's business objectives. According to the Procurement Division's statistics on major commodities purchased by the Secretariat, the expenditure on ICT goods and services was ranked second and fourth in 2017 and 2018, respectively.

12. OIOS conducted this audit from May to September 2019 at Headquarters and Vienna. The audit covered the period from January 2012 to September 2019. The audit covered risk areas in global software development and acquisition activities which included: (a) regulatory framework and governance mechanisms; (b) acquisition planning and procurement of software applications; and (c) software development lifecycle and production support.

13. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) sampling; (d) surveys, interviews and walk-throughs; (e) analytical reviews; and (f) tests of controls.

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

III. AUDIT RESULTS

A. Regulatory framework and governance mechanisms

<u>The regulatory framework for software development and acquisition needs to be strengthened</u>

15. The ICT strategy for the years 2015-2019 (A/69/517) approved by the General Assembly in its resolution 69/262 outlines three elements for ensuring a cohesive and coordinated approach towards software development and acquisition at the Secretariat: (i) global sourcing and asset management; (ii) development of EACs; and (iii) harmonization and standardization of ICT structures. Further, OICT had issued an applications management strategy, some ICT policies and technical procedures on applications development, a project management framework, and a policy document on the procurement of software using low value acquisition.

16. Professional ICT standards recommend that an organization should create a strategic plan that defines, in cooperation with relevant stakeholders, how ICT goals will contribute to the organization's strategic objectives and how ICT will support ICT-enabled investment programmes, services and assets. The ICT strategy should be complemented by an ICT governance framework that defines the distribution of the decision-making rights and responsibilities among various units in the organization.

17. The Secretariat had defined the overall ICT strategic direction and the main goals driving its ICT programme and initiatives. It had also established the related regulatory framework (policies and standard

operating procedures). The present audit indicated the need to strengthen the existing regulatory framework on the lines explained below:

(i) Administrative instruction ST/AI/2005/10 on ICT initiatives including software development and acquisition defines the role of an ICT committee amongst others to bear the primary responsibility for substantive review of the high-level business cases for ICT initiatives, ensuring that each initiative is substantively aligned with the entity's goals and objectives. However, there was no ICT committee at UNOV/UNODC in Vienna, and the ICT Board in New York had not met in recent years. These bodies need to be constituted and convened at periodic intervals to assure that they play their expected role in ICT governance, including acquisition and development of software.

(ii) As a result of the reform that went into effect on 1 January 2019, there were significant changes to delegation of authority in the Secretariat. An automated portal was implemented to support the new delegation of authority structure. However, clarity was required regarding the responsibility for global monitoring in several ICT-related areas including compliance with the ICT strategy and the policies and procedures pertaining to software development and acquisition. At the time of the audit, the proposed delegation of authority for ICT was still in draft form. There is need for clarity on the responsibilities of OICT vis-à-vis: (i) the delegation of authority to heads of entities and offices and responsibilities for monitoring and enforcing ICT policies and procedures on a global basis, considering that many activities have been decentralized; and (ii) the responsibilities of the Business Transformation and Accountability Division within DMSPC.

(iii) Before and after the ICT strategy of 2015, there were and still are ICT units in each Secretariat entity that have the capacity to develop applications. The EACs put in place a working group called the Software Development Coordination Group to coordinate software development activities across the Secretariat and to ensure that new projects comply with the ICT standards and do not duplicate similar solutions. However, there were still instances of duplication of effort and proliferation of applications across the Organization. One of the objectives of the establishment of EACs was to institute regional centres for application development and support across the Organization and thereby reduce the proliferation of applications. OIOS acknowledges that the establishment of EACs has significantly contained the proliferation of applications. But there is a need to strengthen oversight, prevent duplication of effort, and further promote standardization. For example, guidance issued by OICT on EACs states that applications and websites operating outside the purview of (or without approval of) EACs will be subject to decommissioning. However, the audit showed that several applications were still operating without EAC approval.

(iv) OICT had issued guidelines on embedding information security requirements for software acquisition and development. OIOS noted that according to the "ICT security compliance self-assessment dashboard" which was managed by OICT, the compliance status of applications/websites with ICT security policies was not known as this was not reported to OICT as required. Non-compliance with ICT security policies exposes the Organization's ICT infrastructure to significant risks.

(v) The absence of a costing methodology and cost-sharing mechanism resulted in a non-standardized approach to determining costs and charge back. Further, there was lack of consistency in payment of ongoing support for globally-shared applications (such as UniteDocs and iNeed). Only some offices at Headquarters and field missions were paying their share for development and maintenance of these applications. Some offices indicated that they did not have visibility over what OICT was charging them for. Additionally, the total cost of ownership and total cost of applications acquired over time was not known to facilitate charge back and asset management.

(vi) In a previous audit (Report 2018/072) on acquisition and management of ICT assets in OICT, OIOS had recommended that OICT should deploy a central software license library for identifying non-licensed software and ensure that intangible assets are identified and capitalized. This recommendation was still under implementation. The present audit showed that, globally, software licenses of commercial off-the-shelf systems (such as Sharepoint and Oracle) were still either tracked manually or not at all. Also, OIOS' review of software purchased from 2013 to 2019 showed that only 72 software items had been capitalized since Umoja go-live in 2013, and that most entities were not capitalizing software. OICT did not have visibility over the costs of internally developed applications due to inconsistent reporting of application development projects and costs globally. Since OIOS' previous recommendation to resolve these issues was still under implementation, no further recommendation is made in this area.

(vii) Three EACs were identified in the ICT strategy – New York, Vienna and Bangkok. However, Vienna's designation as an EAC was yet to be implemented due to funding complexities. Currently, OICT has no oversight of the Information Technology Service (ITS) in UNOV/UNODC, including its application development activities for Member States which constituted a significant source of income. The inclusion of Vienna as an EAC should facilitate harmonization and the envisaged standardization, economies of scale and reduction in duplication of effort.

18. Strengthening of the regulatory framework is essential to address the issues explained above and promote more effective and efficient use of ICT resources across the Secretariat.

(1) OICT, in collaboration with DMSPC, should strengthen the regulatory framework for software development and acquisition by: (a) ensuring that ICT committees are constituted and meet periodically, as appropriate; (b) finalizing the delegation of authority for ICT; (c) providing direction on information security compliance and ensuring that entities certify their compliance with ICT security policies and standards; (d) clarifying the methodology for costing and sharing of application acquisition and support costs; (e) establishing an effective mechanism to globally track the total cost of ownership of ICT applications; and (f) implementing the decision of the General Assembly establishing Vienna as an Enterprise Application Centre.

OICT accepted recommendation 1 and provided evidence to show that parts (d) and (e) have been implemented. Recommendation 1 remains open pending receipt of evidence that: (i) ICT committees have been constituted and meet periodically; (ii) delegation of authority for ICT has been finalized; (iii) direction on information security compliance has been provided and entities have certified their compliance with ICT security policies and standards; and (iv) Vienna has been established as an EAC.

<u>Intellectual property rights of United Nations-owned software need to be adequately protected</u>

19. It is best practice to define policies for software intellectual property rights to maximize the economic value of an application asset and protect it from theft or unauthorized use.

20. The Secretariat develops software that is critical to its programmes, or those of Member States (i.e., UNODC programmes) for a fee. Currently, there is no comprehensive policy for protecting the Organization's software intellectual property from financial, reputational and security risks. [redacted]

21. OIOS reviewed a sample of internally developed software on a global basis and noted that several systems were unique in nature (such as the "go" suite of applications in UNOV/UNODC, the Field Remote

Infrastructure Management System in the United Nations Global Service Centre, the Grants Management tool in the Office for the Coordination of Humanitarian Affairs, and the National Accounts Statistical System in the Department of Economic and Social Affairs). Also, staff working on coding for unique software were not required to sign non-disclosure agreements or intellectual property agreements. The Office of Legal Affairs (OLA) stated that staff working on coding or software would not be required to sign any non-disclosure agreements or other agreements as Staff Rule 1.9 provided that all intellectual property developed by staff members in their official capacity is owned by the United Nations. However, in OIOS' opinion, clarification is needed on whether the Staff Rule can be enforced when the staff member no longer works for the United Nations.

22. The Integrated Security Clearance and Tracking system (TRIP), which had been developed in 2006 by a Member State government and protected by copyright, was licensed to the United Nations for 12 years and then subsequently donated to the Organization in 2018. The Member State government also transferred the copyright to the United Nations at the time of the donation.

23. Protection of intellectual property of applications developed by, or donated to the Organization is essential to deter their use without permission, prevent unauthorized changes to the software, and safeguard their ownership.

(2) OICT, in collaboration with DMSPC, should: (a) establish appropriate mechanisms in consultation with the Office of Legal Affairs to protect the Organization's intellectual property for internally developed software; and (b) require all entities within the Secretariat to identify internally developed software that need such protection so that appropriate protection could be secured.

OICT accepted recommendation 2. Recommendation 2 remains open pending receipt of evidence that: (i) appropriate mechanisms to protect the Organization's intellectual property for internally developed software are established in consultation with OLA; and (ii) all entities within the Secretariat are required to identify internally developed software that need protection so that appropriate protection could be secured.

ICT governance and resource management needed to be strengthened at UNOV/UNODC

24. OIOS identified a number of areas at UNOV/UNODC that pointed to the need for strengthening ICT governance and management of resources, as explained below:

(i) The recent ICT reorganization in UNOV/UNODC seemed to be unclear to staff. The proposed organization chart and terms of reference were yet to be formalized. In the meantime, there was lack of clarity regarding roles and responsibilities entrusted to staff. This led to segregation of duties conflicts. For example, developers had access to production systems (the 'goCase' application).

(ii) UNOV/UNODC resources did not change with the increase in its clientele (there were 27 and 43 clients in 2017 and 2019, respectively). For instance, there was only one analyst tasked with quality assurance which posed the risk that the systems developed may not meet user expectations. Further, ongoing support for internal software provided to process/programme owners such as the Unite suite of applications (e.g., UnitePark, UniteTours, UniteGift) and other software supported by ITS was not adequately funded, which may impact the availability and security of the software.

(iii) Cost plans were prepared by ITS and presented to the Finance Resource Management Service (FRMS) for review and approval. FRMS reconciled income with cost plans. However, it was difficult to reconcile project costs due to lack of clarity as to their basis (for example, the use of funds earmarked for one project to implement others). Further, posts earmarked for specific projects that were included in the cost plans which served as the basis for charging Member States were sometimes not filled.

(iv) For the software products delivered to Member States, there were 16 'live' applications of which only 5 had active service level agreements (SLAs) with Member States. The remaining 11 applications without SLAs were supported using funds from the active SLAs. This indicates the possibility that clients with active SLAs may be getting overcharged to support the costs of maintaining applications that do not have an active SLA.

(v) Costs were charged to software support accounts for which the staff were not assigned. OIOS' sample review of staff assigned to the various software applications, interviews with a sample of developers and managers for those applications, and walk-throughs of their day to day activities indicated discrepancies in the cost centres charged and the amount of work performed by the staff for the applications to which their cost was charged. Also, cost calculation algorithms were inconsistently applied when preparing SLAs with different Member States for the same products, resulting in significantly different costs for different Member States. The cost calculations should be performed more consistently (e.g., for 'goAML', one Member State was charged three times more than another).

(vi) There was a funding surplus of approximately $6.7 million for the 'goPortfolio' software even though the chargeback methodology did not envisage profit-making. UNOV/UNODC stated the composition of the surplus mainly consisted of income recognized for future delivery of 'goPortfolio' and not any profit earned.

(vii) ITS used credit cards to purchase software. This practice was contrary to procurement procedures which do not permit such purchases because of legal implications.

(3) UNOV/UNODC should: (a) finalize its ICT reorganization and disseminate revised job descriptions to the affected staff members; (b) strengthen controls to ensure that the project costs charged are accurate and justified; (c) establish service level agreements and associated metrics for all active applications; (d) define future operating objectives for the surplus accrued from the 'goPortfolio' application; and (e) stop the practice of using credit cards for purchasing software.

UNOV/UNODC accepted recommendation 3 and stated that part (e) was implemented with immediate effect. Recommendation 3 remains open pending receipt of evidence that: (i) the UNOV/UNODC ICT reorganization has been finalized and revised job descriptions have been disseminated to the affected staff members; (ii) controls have been strengthened to ensure that project costs charged are accurate and justified; (iii) SLAs and associated metrics for all active applications have been established; and (iv) the future operation objectives for the surplus accrued from the 'goPortfolio' application has been defined.

B. Acquisition planning and procurement of software applications

Controls over global software acquisition need to be strengthened

25. The ICT strategy outlined how the increasing costs and efficiency gains in global purchasing and management of ICT goods and services acquired through systems contracts should be controlled by strengthening visibility and control of ICT expenditures through: (i) the establishment of standard processes; (ii) a centralized contract management capacity; (iii) a repository of contracts and a management tool for software licenses and hardware purchases; and (iv) global sourcing that will be implemented using

Umoja to support process integrity and visibility in accordance with the requirements of the International Public Sector Accounting Standards (IPSAS).

26. There was no consistent approach to software acquisition planning to facilitate planning forecasts, areas for major investment, and economies of scale. Further, the total cost of ownership and total cost of software acquired over time was not known. For instance, as part of the budgetary process, offices and departments were required to send OICT the details of their ICT acquisition plans and projects but, in practice, this was not done in most cases.

27. OIOS reviewed software purchases during the audit period and noted the following:

(i) The Procurement Manual states that unless a requisitioner provides valid reasons as to why a bid process should not be used, the established bid procedures should be followed. OIOS noted that requisitioners were at times able to bypass the solicitation process by citing exemptions to the use of formal methods of solicitation in the FRR. OIOS' review of software purchases for 2017 and 2018 showed two purchases (in the amounts of Euro 55,556 and Euro 84,762) where FRR 105.15 (a) (i) (i.e., exceptions when there is no competitive marketplace for the product) was cited as the reason for exemption from bidding. There were additional instances of these exceptions being utilized for standard software which did not fall under this category.

(ii) OIOS noted that one entity consistently purchased Microsoft products with high dollar amounts without utilizing the established systems contract with the vendor. This entity purchased Microsoft Office and Windows software for a total of $669,551 during 2017 and 2018 outside the systems contract. Also, there was no oversight of software purchased at the field level. Table 1 shows examples of the same software purchased outside the systems contract, thereby missing the opportunity to ensure optimization of resources and support.

Table 1
Instances of same applications purchased repeatedly without using systems contract

Software	No. of instances between May 2018 and May 2019
Business Process Modeling	141
Project Management	48
Adobe Acrobat	61
Adobe Creative Cloud	84
Microsoft Office	29
Database	53
Reporting	45
ArcGIS	66
Communications	171
VMware Virtual Center	50
Cisco License Manager	125

(iii) OIOS' review of the approved shopping carts for software purchased from May 2018 to May 2019 indicated that out of 1,938 approved shopping carts, approximately 786 contained purchases of software that was not on the OICT standard list. This could lead to acquisition of non-standard applications which is contrary to the goals of the ICT strategy.

28. In a previous audit (Report 2018/072) on acquisition and management of ICT assets in OICT, OIOS had made similar observations and recommended that the Procurement Division should collaborate with

OICT to strengthen controls over the purchase of software globally. Procurement Division indicated that this recommendation would be implemented by 31 December 2019.

C. Software development lifecycle and production support

Need for policies and standards for collaboration tools and source code management

29. The use of collaboration tools in the software development process is a best practice that is beneficial and encouraged. These tools provide many benefits such as allowing design and development teams to organize projects, centralize tasks, streamline the software definition phase, build out prototypes and workflows, track requests, and assign work.

30. OIOS review of the software development life cycle (SDLC) process in a sample of 10 systems globally as well as four software at UNOV/UNODC indicated that there was no policy and standardized tool to facilitate consistency in source code management and SDLC in general across the Secretariat. Further, the use of collaboration tools was inconsistent across the Secretariat and there was no global standard regarding the use of these tools. Consequently, offices/entities used various tools (i.e., JIRA, Microsoft Azure, and Trello). Further, even within ICT units in the same office/entity, there was no consistency since different collaboration tools were used. OIOS also noted the following:

(i) Teams utilizing collaboration tools also relied upon them for important SDLC controls such as source code management, software version control, release management, and system documentation repository. However, though some of the tools had control features built in, others were not appropriate for standard SDLC controls nor intended for such use.

(ii) Some teams mitigated the limitations of these tools by integrating them with other software (e.g., Bitbucket version control software), and some implemented compensating manual processes. However, there was no monitoring to ensure that all teams utilizing the tools maintained proper SDLC controls.

(iii) The United Nations Retention Schedule for ICT Records (INM.01.PROC) specifies time frames for retention of records and the methods of disposal. Included in this policy are items such as approved business cases and system design documents. Teams using collaboration tools indicated that the tool was also used as a repository of the documentation. However, in 5 cases out of 12 systems reviewed by OIOS, project managers were unable to retrieve all system documentation that was required to be maintained. In most cases, important documentation such as approved business cases and system design documents could not be located.

(iv) There was no consistency as to when a team would use different types of system development methodologies (i.e., Agile, Waterfall, Scrum) with a given collaboration tool, which should be determined based on the size and complexity of the project.

31. A standardized policy for SDLC and collaboration tools for software development and source code management are required to ensure effective management and oversight of internally developed software and adequate control over source codes.

(4) OICT should: (a) provide guidance on the types of system development life cycle methodologies appropriate for projects based on their size and complexity; and (b) provide a standardized collaboration tool for the software development life cycle.

OICT accepted recommendation 4. Recommendation 4 remains open pending receipt of evidence that: (i) guidance is provided on the types of SDLC methodologies appropriate for projects based on their size and complexity; and (ii) a standardized collaboration tool for SDLC is provided.

Software development and acquisition data was not adequately captured in UniteApps portfolio

32. The OICT Application Management Strategy for the United Nations Secretariat, dated 27 March 2015, applies to all software development undertaken in ICT globally (field and non-field entities of the Secretariat). This document specifies the establishment of the United Nations Global Application Portfolio (UniteApps) as part of the strategy to improve ICT activities globally and enable OICT to have a global view of all software in the Secretariat. All offices are required to enter detailed information regarding their systems into the portfolio.

33. The UniteApps portfolio showed that the number of 'internally developed' and 'off-the-shelf' applications were 2,069 and 199, respectively. There were 97 critical applications. OIOS noted the following with regard to the data fields:

(i) Some 1,135 items (not counting those flagged as 'to be retired') were identified as custom developed but had zero or blanks in the 'development costs' field. This limited OICT's view of internally developed software costs on a global basis and its ability to monitor and identify software that should be capitalized.

(ii) OICT had documented implementation guidelines for disaster recovery (DR) and required that all entities should review and designate their critical software and develop, document, implement and periodically update the DR plans for critical software. OIOS noted that out of the 1,582 internally developed software listed in the database, the DR data field was left blank for 1,456 items. Further, except for enterprise software maintained by OICT, most offices had not reviewed and defined critical software or developed DR plans. Also, the majority of the systems including enterprise systems maintained by OICT had not been subject to DR tests in the recent past. OICT stated that it did not perform disaster recovery testing for non-senior emergency policy team ("non-SEPT") critical applications.

(iii) Out of 199 records identified as 'commercial off-the-shelf', 156 had zero or blanks in the 'initial license cost' field, 158 had zero or blanks in the 'maintenance cost for licenses' field, and 32 had blanks in 'number of licenses' data field. This constrained OICT's ability to assess software licensing and usage which could have financial and reputational implications for the Organization.

34. The missing information in UniteApps defeats the purpose of the database which is to improve global visibility and monitoring of software in the Secretariat.

(5) OICT should: (a) identify the mandatory data fields in the UniteApps portfolio and ensure that mandatory data is captured; (b) require all offices to clean up their portfolio of systems in UniteApps and update it with the required information; and (c) identify the critical applications, update the UniteApps database accordingly, and require the preparation of disaster recovery plans for those applications.

OICT accepted recommendation 5 and stated that: (a) 'mandatory" data fields will be designated; (b) OICT will remind authorized focal points to update their entity application information; and (c) to avoid confusion between applications that a particular entity may consider as critical, OICT will add a flag to UniteApps. Recommendation 5 remains open pending receipt of evidence that (i) mandatory data fields in the UniteApps portfolio have been identified and captured where possible; (ii) all offices have cleaned up their portfolio of systems in UniteApps and updated it with the required information; and (iii) critical applications have been updated in the UniteApps database and disaster recovery plans have been prepared for applications where required.

IV. ACKNOWLEDGEMENT

35. OIOS wishes to express its appreciation to the management and staff of DMSPC, OICT and UNOV/UNODC 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 processes for the development and acquisition of software applications at the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	OICT, in collaboration with DMSPC, should strengthen the regulatory framework for software development and acquisition by: (a) ensuring that ICT committees are constituted and meet periodically, as appropriate; (b) finalizing the delegation of authority for ICT; (c) providing direction on information security compliance and ensuring that entities certify their compliance with ICT security policies and standards; (d) clarifying the methodology for costing and sharing of application acquisition and support costs; (e) establishing an effective mechanism to globally track the total cost of ownership of ICT applications; and (f) implementing the decision of the General Assembly establishing Vienna as an Enterprise Application Centre.	Important	O	Receipt of evidence that: (i) ICT committees have been constituted and meet periodically; (ii) delegation of authority for ICT has been finalized; (iii) direction on information security compliance has been provided and entities have certified their compliance with ICT security policies and standards.it has been fully implemented; and (iv) Vienna has been established as an EAC.	31 December 2021
2	OICT, in collaboration with DMSPC, should: (a) establish appropriate mechanisms in consultation with the Office of Legal Affairs to protect the Organization's intellectual property for internally developed software; and (b) require all entities within the Secretariat to identify internally developed software that need such protection so that appropriate protection could be secured.	Important	O	Receipt of evidence that: (i) appropriate mechanisms to protect the Organization's intellectual property for internally developed software are established in consultation with OLA; and (ii) all entities within the Secretariat are required to identify internally developed software that need protection so that appropriate protection could be secured.	31 December 2020
3	UNOV/UNODC should: (a) finalize its ICT reorganization and disseminate revised job	Important	O	Receipt of evidence that (i) UNOV/UNODC ICT reorganization has been finalized and revised job	31 December 2020

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

[3] C = closed, O = open

[4] Date provided by OICT and UNOV/UNODC in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of processes for the development and acquisition of software applications at the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
	descriptions to the affected staff members; (b) strengthen controls to ensure that the project costs charged are accurate and justified; (c) establish service level agreements and associated metrics for all active applications; (d) define future operating objectives for the surplus accrued from the 'goPortfolio' application; and (e) stop the practice of using credit cards for purchasing software.			descriptions have been disseminated to the affected staff members; (ii) controls have been strengthened to ensure project costs charged are accurate and justified; (iii) service level agreements and associated metrics for all active applications have been established; and (iv) the future operation objectives for the surplus accrued from the 'goPortfolio' application has been defined.	
4	OICT should: (a) provide guidance on the types of system development life cycle methodologies appropriate for projects based on their size and complexity; and (b) provide a standardized collaboration tool for the software development life cycle.	Important	O	Receipt of evidence that: (i) guidance is provided on the types of SDLC methodologies appropriate for projects based on their size and complexity; and (ii) a standardized collaboration tool for SDLC is provided.	31 December 2020
5	OICT should: (a) identify the mandatory data fields in the UniteApps portfolio and ensure that mandatory data is captured; (b) require all offices to clean up their portfolio of systems in UniteApps and update it with the required information; and (c) identify the critical applications, update the UniteApps database accordingly, and require the preparation of disaster recovery plans for those applications.	Important	O	Receipt of evidence that: (i) mandatory data fields in the UniteApps portfolio have been identified and captured where possible; (ii) all offices have cleaned up their portfolio of systems in UniteApps and updated it with the required information; and (iii) critical applications have been updated in the UniteApps database, and disaster recovery plans have been prepared for applications where required.	31 December 2020

APPENDIX I

Management Response

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar, Deputy Director
A: Internal Audit Division
Office of Internal Oversight Services

DATE: 17 January 2020

THROUGH: Olga de la Piedra, Director O de la Piedra
S/C DE: Office of the Under-Secretary-General
Department of Management Strategy, Policy and Compliance

FROM: Mario Baez, Chief, Accountability Service
DE: Business Transformation and Accountability Division
Department of Management Strategy, Policy and Compliance

SUBJECT: **Draft report on an audit of processes for the development and acquisition of**
OBJET: **software applications at the United Nations Secretariat (Assignment No. AT2019/517/02)**

1. We refer to your memorandum dated 30 December 2019 regarding the above-mentioned draft report. Please find below and in Appendix I the consolidated comments from the Office of Information and Communications Technology (OICT) and the United Nations Office at Vienna/United Nations Office on Drugs and Crime (UNOV/UNODC).

United Nations Office at Vienna/United Nations Office on Drugs and Crime (UNOV/UNODC)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3. The assertion, made in the second sentence of the above paragraph, that a 100 percent goCase funded staff member "never worked on goCase" is factually incorrect. UNOV/UNODC has documentation on the staff funding and work outputs that show the statement to be factually incorrect. In 2019 only two staff were 100 percent charged to the goCase cost centre, and both of those staff provided work for goCase. UNOV/UNODC requests that this statement be deleted from the text. A supporting document showing that only two staff were 100 percent funded by cost center 13489 for goCase has been provided to OIOS.

4. Thank you for giving us the opportunity to provide comments on the draft report.

APPENDIX I

Management Response

Audit of processes for the development and acquisition of software applications at the United Nations Secretariat

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OICT, in collaboration with DMSPC, should strengthen the regulatory framework for software development and acquisition by: (a) ensuring that ICT committees are constituted and meet periodically, as appropriate; (b) finalizing the delegation of authority for ICT; (c) providing direction on information security compliance and ensuring that entities certify their compliance with ICT security policies and standards; (d) clarifying the methodology for costing and sharing of application acquisition and support costs; (e) establishing an effective mechanism to globally track the total cost of ownership of ICT applications; and (f) implementing the decision of the General Assembly establishing Vienna as an Enterprise Application Centre.	Important	Yes	Director, Policy Strategy Governance Division, OICT (for parts (a), (b), (c)) Office of the Chief Information Technology Officer (CITO), OICT (for part (f))	Parts (a), (b) and (c): 31 December 2020 Parts (d) and (e) were implemented as of December 2019 Part (f):31 December 2021	Parts (d) and (e) of the recommendation have already been implemented as of December 2019. The supporting evidence of implementation has been provided to OIOS.
2	OICT, in collaboration with DMSPC, should: (a) establish appropriate mechanisms in consultation with the Office of Legal Affairs to protect the	Important	Yes	Director, Policy Strategy Governance Division, OICT	31 December 2020	OICT accepts this recommendation.

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Management Response

Audit of processes for the development and acquisition of software applications at the United Nations Secretariat

	Organization's intellectual property for internally developed software; and (b) require all entities within the Secretariat to identify internally developed software that need such protection so that appropriate protection could be secured.					
3	UNOV/UNODC should: (a) finalize its ICT reorganization and disseminate revised job descriptions to the affected staff members; (b) strengthen controls to ensure that the project costs charged are accurate and justified; (c) establish service level agreements and associated metrics for all active applications; (d) define future operating objectives for the surplus accrued from the 'goPortfolio' application; and (e) stop the practice of using credit cards for purchasing software.	Important	Yes	Chief, Information Technology Service, UNOV/UNODC	31 December 2020	UNOV/UNODC accepts the recommendation. Parts (a) to (d) of the recommendation are expected to be fully implemented by the end of 2020. Part (e) was implemented with immediate effect.
4	OICT should: (a) provide guidance on the types of system development life cycle methodologies appropriate for projects based on their size and complexity; and (b) provide a standardized collaboration tool for the software development life cycle.	Important	Yes	Chief, Enterprise Service Solutions, OICT	31 December 2020	OICT accepts this recommendation
5	OICT should: (a) identify the mandatory data fields in the UniteApps portfolio and ensure that mandatory data is captured; (b) require all offices to clean up their	Important	Yes	Chief, Enterprise Service Solutions, OICT	31 December 2020	OICT accepts this recommendation and will implement it as follows:

	portfolio of systems in UniteApps and update it with the required information; and (c) identify the critical applications, update the UniteApps database accordingly, and require the preparation of disaster recovery plans for those applications.					(a) "mandatory" data fields will be designated as such. (b) OICT will remind authorized IT focal points to update their entity application information. However, the responsibility to provide timely and accurate data in this regard remains with the respective entities. (c) To avoid the confusion between the Senior Emergency Policy Team (SEPT) applications and other applications that a particular entity may consider as critical, OICT will add a flag to UniteApps. It should be noted that OICT prepares the plans for enterprise applications that are managed by OICT.