ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Internal Audit Report

on

Third Party (Outsourced Service Providers) Governance and Risk Management

IA/2025/05

Office of Internal Oversight

ACRONYMS

BCP	Business Continuity Planning
CISO	Chief Information Security Officer
EAAC	Evaluation and Audit Advisory Committee
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
HLCM-PN	United Nations High Level Committee on Management - Procurement Network
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IIA	Institute of Internal Auditors
IMC	Information Management Committee
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LEB	Legal Affairs and External Relations Bureau
LSMS	Language Services Management System
MOU	Memorandum of Understanding
MSDA	Master Service Delivery Agreement
OIO	Office of Internal Oversight
PRO	Procurement Section
SLA	Service Level Agreement
SME	Subject Matter Expert
SSAQ	Supplier Security Assessment Questionnaire
TPRM	Third Party Risk Management
UNDP	United Nations Development Programme
UNICC	United Nations International Computing Centre
UN-OIOS	United Nations Office of Internal Oversight Services

CONTENTS

EXECUTIVE SUMMARY

1. As part of its annual work plan for 2025 (C-WP/15634), the Office of Internal Oversight (OIO) carried out an internal audit of Third Party (Outsourced Service Providers) Governance, Risk Management and Compliance with internal controls. The audit was conducted in conformance with the Global Internal Auditing Standards of the Institute of Internal Auditors.

2. In this audit, OIO considered that outsourcing is the transfer of entire business processes or functions to third parties for a period of time (rather than the procurement of services from suppliers). Outsourcing to third parties has become a common modality in the private and public sectors. It offers various benefits but also presents various risks, which are categorized as third-party risks. Key phases of the third-party outsourcing lifecycle include selecting, contracting, onboarding, monitoring, and offboarding[1].

3. ICAO has started outsourcing some of its services as part of its efficiency savings approach to utilise the economies of scale and service quality of third parties, which would be quite expensive to perform in-house. OIO observed that ICAO's current cloud strategy is based on the outsourcing of numerous business processes by engaging third-party service providers, primarily United Nations system organizations, but also commercial service providers. The United Nations Development Programme (UNDP) and the United Nations International Computing Centre (UNICC) are among ICAO's primary outsourced service providers in terms of monetary value and strategic and operational relevance. It is expected that this will continue to be the case in view of the new shared ERP system (Quantum). Services are also outsourced or paid to other United Nations system organizations based on long-standing arrangements within these organizations. In addition, "fourth parties", which are normally commercial providers contracted by third-party organizations, provide a significant share of outsourced services. While ICAO can outsource some of its business processes and transfer the related burden and costs to third-party providers, it remains ultimately responsible for the value-for-money aspects and risk management of the outsourced functions, including ongoing monitoring and oversight of the quality and costs.

4. The objective of the audit was to assess whether ICAO has an effective governance, risk management and control framework for the management of third-party risks for outsourced services, based on transactions from January 2023 to April 2025, as well as some earlier or later transactions related to outsourcing decisions.

5. The audit testing was limited to sample cases and cannot provide a reasonable assurance over all outsourced services and associated risks. ICAO does not have an inventory of the outsourced services, but OIO made an attempt to consolidate the list of those services based on its previous audits and feedback from management. Moreover, the audit testing was also limited to existing practices due to the absence of a third-party lifecycle framework and dedicated risk management, which would provide for the key compliance requirements throughout the outsourcing lifecycle. OIO cannot identify a full scope of potential cost-saving opportunities, not only in terms of service fees and expected benefits for outsourced services, but also in terms of internal resources involved in business process oversight and contract management.

6. The main findings of third-party Governance, Risk, and Compliance are summarized as follows:

    - On Governance, OIO observed that some elements of good governance were present, but not standardized and institutionalized. OIO found some good examples where the business cases were developed in support of unit or organizational strategies, reviewed and approved prior to outsourcing, e.g., for some outsourcing services submitted for the Transformational Objective (TO) Programme Board and the Information Management Committee (IMC), which should be institutionalized as a good governance practice. At the same time, ICAO has no formal policy framework to govern its outsourcing decisions. There are some elements of ICT outsourcing in the ICT Strategy and Action Plan 2022-2025. The Procurement Code provides oversight and guidance on the process of tendering and contracting of outsourced service providers; however, the Code does not intend to cover governance and oversight of outsourcing arrangements prior to commencing the procurement process and after the procurement process has ended and the contract has been signed. Also, there is no standard definition and comprehensive inventory for third-party service providers.

[1] https://www.theiia.org/en/standards/2024-standards/topical-requirements/third-party/

- On Risk Management, OIO found that there is no systematic risk management for the end-to-end outsourcing process within the existing ERM framework, including risk identification, mitigation, escalation, and monitoring. The inadequate third-party risk management, which is decentralized to individual functions at ICAO, has decreased the organization's ability to identify, assess, and manage potential risks posed by third parties. In the case of Transformational Objective, the risks associated with each TO project were identified and recorded in the TO risk registers, with the high risks escalated to the Corporate Risk Register. OIO recognizes this as a good practice.

- On Compliance, OIO observed that controls may exist under other policies and initiatives, e.g., procurement and Information Security policies; however, the absence of a third-party framework, cost-benefit monitoring, and dedicated risk identification and management has resulted in limiting the adequacy and cost-effectiveness of internal controls around the outsourcing lifecycle. In particular, controls lack standardization in the form of a robust business case with cost-benefit analysis, a contract template with key provisions for assurance and performance indicators, a mechanism for ongoing monitoring of the outsourced service's continued value for money and exiting from outsourced services if the costs start to exceed the benefits. Among good practices identified by OIO, an information security assessment is conducted at the time of initial contracting and upon the contract renewal with third parties to ensure the service provider meets the Minimum Vendor Information Security Requirements, but it is not conducted periodically to proactively identify and mitigate against any new risks arising due to changes in the third-party provider's infrastructure or other reasons, such as the involvement of other subcontractors.

Audit opinion and overall audit rating

7. Based on the results of the audit, OIO has given an overall audit rating of *'Some Improvement Needed'*.
8. OIO found the following areas to be *"Satisfactory"*: Cybersecurity risk assessments are systematically conducted by the ICAO Information Security Office at the time of initial contracting and renewal with third-party vendors; performance monitoring and periodic validation by HR of outsourced health insurance service.
9. OIO found the following areas needing *"Major Improvement"*: Inadequate governance, inadequate management of the inventory of third parties, lack of dedicated risk management, and related cost-effective controls and cost creep.
10. As ICAO has recently started outsourcing some of its services to third parties, management should identify lessons learned from recent outsourcing cases and enhance its third-party governance and risk management framework in order to make risk-informed outsourcing decisions and manage third-party relationships more effectively in the future. In view of this, OIO has issued four forward-looking recommendations in this report, of which three are of high priority. These are accepted by Management; however, the Management Action Plan will be finalized after the report is issued. OIO will follow up on these recommendations and management actions during its monthly follow-up exercise.

Acknowledgement

11. OIO wishes to thank ICAO's management and personnel for their assistance and cooperation during the audit.

BACKGROUND

Introduction

12. At ICAO, business units are increasingly reliant on third-party service providers to support business operations. These partnerships are crucial for the organization and generally offer various benefits, including service provision by specialized service providers, access to the latest market knowledge and technology, cost savings and lowered administrative burden, greater flexibility, and common practices among the United Nations organizations. At the same time, ICAO's outsourced services entail various third-party and potentially fourth-party risks, including but not limited to strategic, legal, reputational, financial, cybersecurity, operational, and compliance.

13. For the purpose of this audit, outsourcing is described as "*The process of contracting out a business process, which an organization may have previously performed internally or which the organization deems necessary or important, to an independent company, supplier or contractor*[2] *where the process is purchased as a service*". This definition is based on the harmonization guidelines developed through the United Nations High Level Committee on Management - Procurement Network (HLCM-PN) and described in the UN Common Glossary of Procurement Terms.

14. While ICAO can outsource some of its business processes and transfer the related burden and costs to third-party providers, it is still ultimately responsible for value-for-money aspects and risk management of the outsourced functions, including ongoing monitoring and oversight of the quality and costs.

15. ICAO outsources several business processes to UN-system organizations and commercial service providers. Outsourcing may be guided by strategic decision-making, historical practice, a selection process, or a combination of these. While the Procurement Section is responsible for tendering the outsourcing requirement to commercial service providers and the related procurement due diligence, the decision to outsource a function or service rests with the concerned business unit, which is accountable for overall management and monitoring of the third-party relationship. The United Nations Development Programme (UNDP) and the United Nations International Computing Centre (UNICC) are among ICAO's primary third-party service providers. These arrangements are expected to continue with the new, shared ERP system (Quantum).

Audit Objective, Scope and Methodology

16. The objective of the audit was to assess whether ICAO has an effective governance, risk management, and control framework for the management of third-party risks for outsourced services.

17. The audit scope covered the following areas:

    - Effectiveness of the governance, policies, and strategies for systematic outsourcing of services to third parties (definition and inventory of outsourced services, policy framework, business strategies).
    - Effectiveness of risk management for outsourced services (risk management approaches, cost-benefit analyses, assurance over outsourced services, contractual arrangements and Service Level Agreements (SLAs), data and incident management, Business Continuity Planning).
    - Effectiveness of internal controls to obtain outsourced services with the best long-term value for money (selection of third-party providers, performance assessment, monitoring, and reporting of the values and costs of outsourced services).

18. The audit was conducted in conformance with the Global Internal Auditing Standards of the Institute of Internal Auditors (IIA). The audit also benefited from common guidance in the relevant area, for example, the IIA's Practice Guide on Auditing of Third-Party Risk Management and the IIA's Third-Party Topical Requirement, in particular, on the formulation of audit criteria.

19. This audit covered activities and transactions undertaken in the period between 1 January 2023 and 30 April 2025. The audit also covered earlier or later contracts and related transactions, when required for the

[2] Commercial contractor in the context of ICAO.

purposes of this audit, for example, outsourcing decisions made and selections of third-party providers undertaken prior to this period.

20. The audit did not cover individual consultancies, which are covered under the Policy on Consultants, as "outsourcing."

21. The audit methodology included review of policies and procedures, interviews with key stakeholders, document reviews, including contracts and SLAs, and benchmarking with other UN-system organizations to identify best practices and lessons learned.

RESULTS OF THE AUDIT: OBSERVATIONS & RECOMMENDATIONS

Section I: Governance, Policy and Strategy Framework

Overview of ICAO's outsourced services

22. The concept of "outsourced services" is not clearly defined within ICAO. The term is used broadly to refer not only to services fully outsourced to third parties, which is the focus of this audit, but also to consulting engagements, software services, translation services, and other externally provided products and services. This lack of definitional clarity complicates the recording, management, oversight, and reporting of fully outsourced services. An analysis of ICAO Purchase Order transactions for the period January 2023 to April 2025 showed a total of CAD 18,968,053 charged to "Outsourcing". However, OIO has observed that some services that would not fall under the HLCM-PN definition of typical service outsourcing were included in these transactions. For example, procurement of software, purchase of subscription licenses, catering, and even equipment, were charged to the outsourcing accounts.

23. This lack of granularity and clear definition made it difficult to provide financial figures for the total outsourcing volume, as described for this audit. Due to a lack of categorization to distinguish outsourced service providers from the available data, OIO was also not able to assess all third-party outsourced service providers and the associated risks and therefore limited its assessment to three large sample cases, i.e., ERP services provided by UNDP, payroll services provided by UNDP, and ICT services provided by UNICC. Moreover, OIO had previously reviewed other outsourced services like health insurance service (IA/2024/4) and the Languages Services Management System (LSMS) platform (IA/2025/01).

24. The need for a common organization-wide definition of outsourcing was also highlighted in the report of the United Nations Joint Inspection Unit (JIU) entitled "*Review of contemporary practices in the external outsourcing of services to commercial service providers by United Nations system organizations*" (JIU/REP/2019/9). While Management has closed this JIU recommendation as implemented, OIO found that ICAO has not fully adopted a common organization-wide definition of outsourcing and therefore reiterates recommendation 1 of the said JIU report:

    JIU/REP/2019/9 Recommendation 1: *The executive heads of United Nations system organizations should task the relevant offices with developing, through consultations with relevant internal stakeholders, by the end of 2021, a common organization-wide definition of outsourcing and further concretize it by developing approaches and procedural guidelines on the subject matter.*

25. OIO observed that ICAO employs a variety of contractual arrangements for its outsourced services. Some service providers, such as United Nations system organizations, are engaged through a Memorandum of Understanding (MoU), while others are contracted through a service contract or Purchase Order. ICAO's Legal Affairs and External Relations Bureau (LEB) maintains all MOUs and agreements signed with third parties, whereas Purchase Orders are recorded in the ERP system. However, these repositories do not categorize outsourced service providers separately, which results in the absence of a comprehensive inventory and limited visibility into the associated risks. Establishing a centralized inventory that documents the full outsourcing lifecycle for each third-party provider would offer senior management, as well as second-line functions, such as Risk Management (ERM), and the third-line functions, such as internal and external auditors, a holistic view of the scope and risk profile of outsourced services. While OIO made efforts to compile such an inventory – including consideration of their fourth-party relationships – the resulting list (see Table 1 below) may be incomplete due to data limitations and the decentralized nature of outsourcing practices in ICAO.

Table 1 - Inventory of current outsourced services (Note: the data might be incomplete)

Outsourced Service	Description of Service	Business Unit	Third Party Provider
Investigation	Provision of investigation services	ADB	UN-OIOS
MBP	Administration of ICAO Medical Benefit Plan	ADB	Cigna
Training	Provision of training services	ADB	UNSSC
ERP	Provision of ERP (Quantum) services	ADB	UNDP
Infra	Provision of Hosting and network services	ADB	UNICC
Service Desk	Provision of the Service management platform	ADB	UNDP
Emails	Management of Corporate emails,	ADB	UNICC
LSMS	Platform for document management	ADB	UN Secretariat
Security	Provision of security clearance	ADB	UNDSS
Ethics	Provision of independent reviews, preliminary assessments, capacity-building, and back-up support services	Ethics Office	UN Ethics Office
Payroll	Provision of payroll services for Professional and General Service staff	FIN	UNDP
UNAT	United Nations Appeals Tribunal services	LEB	UN

Governance

26. Effective governance establishes clear policies, guiding principles, and a structured implementation strategy with defined actions and oversight mechanisms. These elements are essential for managing outsourced services to ensure accountability, transparency, and strategic alignment. Strong governance also clearly delineates the roles and responsibilities of both internal stakeholders and external service providers, ensuring that the decision-making process supports the organization's mission and goals. Robust governance frameworks enable consistent monitoring, performance evaluation, and proactive risk mitigation, which are key factors for maintaining operational control, achieving value for money, and ensuring compliance with regulatory and contractual requirements.

27. Currently, ICAO lacks a formalized governance mechanism to review the outsourcing business case, its costs, risks and benefits, and the long-term strategy for individual outsourcing. The existing frameworks, such as the Policy on Interactions with External Parties and the Procurement Code, are not intended to provide the strategic oversight required for outsourcing arrangements. To ensure consistency, accountability, and value for money, ICAO should formalize a dedicated governance structure to oversee major outsourcing initiatives. This should begin with the development of a business case or concept for the service to be outsourced, include an initial cost-benefit analysis, and continue with ongoing monitoring of benefits realization in the long run. Such a structure would also play a critical role in identifying and mitigating risks associated with outsourcing, thereby enhancing organizational resilience and performance.

28. The audit revealed a lack of clarity regarding roles and responsibilities in several outsourcing cases at ICAO. Specifically, the responsibilities of key units involved in the end-to-end lifecycle, e.g., primary contract manager and contributing/affected units, second-line monitoring entities (e.g., ERM), and third-party service providers, were not clearly defined. This ambiguity can dilute accountability, hinder effective oversight, leave risks unidentified and unmanaged, and negatively affect the performance and reliability of outsourced services.

29. On a positive note, OIO observed a good example in the management of outsourced health insurance services where a dedicated contract manager was responsible for overseeing the performance of the service provider. The third-party provider submits an annual stewardship report to ICAO, detailing its performance against contractual indicators and standards. Additionally, the business unit has implemented a periodic validation of service and financial accuracy, which strengthens oversight and ensures service quality.

30. Another positive example relates to the Transformational Objective (TO) programme, which has introduced harmonization and oversight in decision-making and implementation, with outsourcing decisions under the TO programme being approved by the Digital Transformation Programme Board. However, as the TO

concluded on 31 December 2025, there is a risk that future outsourcing arrangements may lack sufficient oversight unless a robust outsourcing framework is established.

Policy Framework

31. A comprehensive policy framework establishes formal principles and procedures to guide the development of business cases, the selection and onboarding of service providers, and the ongoing management, monitoring, and eventual offboarding of service providers. Such a framework promotes consistency and transparency in outsourcing decisions and implementation, addressing critical areas including due diligence, service level agreements, data protection, incident management, assurance, and conflict resolution. These policies serve as foundational references for both internal stakeholders and external service providers, helping to enforce standards, reduce ambiguity, and enhance the auditability and accountability of outsourced arrangements.

32. OIO observed that ICAO does not have a dedicated governance and risk management framework for outsourcing. Existing policies do not fully cover outsourcing to third parties, which increases the risk of services being outsourced without adequate oversight, consistency, value for money, or strategic alignment. For example:

    - The ICAO Policy on Interactions with External Parties, approved by the Council in November 2024, provides guidance on engagements with external entities, but it does not apply to procurement transactions governed by the ICAO Procurement Code or Agreements with other UN organizations.
    - The ICAO Procurement Code covers the provision for contract management. However, since outsourcing is not clearly defined within the Code, it falls under the general contract management practices. These do not encompass the full outsourcing lifecycle, particularly the pre- and post-procurement phases such as proof of concept, business case development, and performance monitoring (see Section III). This gap leaves outsourcing decisions vulnerable to ad hoc practices and limits the organization's ability to ensure value for money, manage risks, and maintain accountability.
    - The ICAO Information Security Policy includes provisions for third-party supplier risk management covering vendors, suppliers, partners, contractors, or service providers with access to organizational data, systems, processes, or other privileged information. However, this policy focuses solely on information security controls and does not address the entire outsourcing lifecycle.
    - The ICT Strategy and Action Plan 2022-2025 discuss ICT outsourcing as part of ICAO's Digital Transformation, stating that a comprehensive outsourcing strategy must be developed – though this has not yet been accomplished.

33. Implementing a formal outsourcing framework would allow ICAO to adopt standardized criteria for identifying the needs, evaluating and selecting third-party providers, and ensuring fairness, transparency, value for money, and strategic alignment. Such a policy would require comprehensive due diligence, including background checks, financial assessments, and compliance reviews, before onboarding vendors. It would also establish essential safeguards such as data protection and confidentiality clauses, exit and transition plans, and assurance and compliance requirements. Collectively, these measures would strengthen ICAO's ability to manage outsourced services effectively, mitigate risks, and ensure long-term value for money.

Implementation Strategy

34. A clearly defined implementation strategy, aligned with the overarching framework, enables the organization to proactively identify and prioritize outsourcing opportunities, plan such projects ahead of time, manage interdependencies, and adapt to evolving business needs. From an audit perspective, having such a strategy in place provides assurance that outsourcing is approached as a deliberate, value-driven component of the organization's broader business model, rather than as a reactive or fragmented decision.

35. At ICAO, outsourcing arrangements are initiated and managed according to the internal strategies of each contracting entity. For instance, the ICT Strategy 2022-2025 highlighted that, as part of ICAO Digital Transformation, outsourcing will be the primary method for acquiring and maintaining technology under the new Target Operating Model.

Recommendation 1 (High Priority)	Governance framework
ICAO Management, in collaboration with PRO, ERM, CISO, LEB, and other Subject Matter Experts, should develop a comprehensive outsourcing framework by consolidating existing provisions and strategies related to outsourcing arrangements at ICAO. This framework should, at a minimum, define outsourcing, establish risk tolerance, clarify delegated authority, set governance and oversight, outline key phases of the outsourcing lifecycle, address requirements for risk management, data protection and security, performance monitoring and evaluation, assurance, as well as exit strategy and transition planning.	

Recommendation 2 (Medium Priority)[3]	Inventory of outsourced services
In order to have visibility over all the outsourced services and the associated third-party and fourth-party risks, ICAO Management should complete and maintain the inventory of existing and future outsourced services to be used for risk management and oversight processes.	

Section II: Risk Management

Third Party Risk Management

36. Effective management of risks associated with third-party service providers is critical for safeguarding ICAO's operations, data integrity, reputation, and compliance posture. Embedding Third-Party Risk Management within the outsourcing framework (see recommendation 1) will provide a systematic approach to identifying, assessing, managing, and monitoring risks linked to external service providers. This will ensure that third-party engagements are consistent with ICAO's risk appetite, governance standards, and strategic priorities, thereby enhancing resilience, accountability, and informed decision-making.

37. OIO observed that ICAO's risk registers do not consistently capture third-party risks. As ICAO's reliance on external vendors for critical services grows, the complexity and scope of associated risks also increase. To address this gap, ICAO should formally include the third-party risk category in its risk universe.

38. Currently, third-party risk management at ICAO is handled within individual Bureau risk registers, but there is no systematic process for comprehensive due diligence and risk assessment prior to outsourcing decisions. As ICAO continues to expand its engagement with third parties, including outsourcing and co-sourcing arrangements, it should implement a structured third-party risk management process that covers key risk categories, including[4]:
    - Strategic (impact on ICAO's mission, strategic goals and enablers).
    - Reputational (potential harm to ICAO's relationships and trust).
    - Ethical (integrity failure, conflicts of interest, corruption).
    - Operational (security, service disruptions, achievements of objectives).
    - Financial (third-party insolvency, fraud).
    - Compliance (adherence to regulatory requirements).
    - Cybersecurity and data protection (risk of data compromise).
    - Information technology (support for critical operations).
    - Legal (disputes, contract breaches).
    - Sustainability (environmental, social, governance).
    - Geopolitical (disputes/sanctions, political instability).

[3] This recommendation will assist with addressing two overdue JIU recommendations from JIU/REP/2014/9 and JIU/REP/2019/9. JIU/REP/2014/9 Recommendation 11: "*The executive heads of the United Nations system organizations should augment the capabilities of their existing information technology systems such as Enterprise Resource Planning systems, or consider other specialized contract-management systems, to support the management of post-award contract activities based on a cost/benefit analysis and taking into account the level of need for such functionality*".
JIU/REP/2019/9 Recommendation 2: "*The legislative bodies of the United Nations system organizations should request their executive heads to ensure that, by the end of 2022, annual reports on procurement include a subsection on expenditures on services sourced from commercial service providers.*"

[4] https://www.theiia.org/en/standards/2024-standards/topical-requirements/third-party/

39. The organization's risk tolerance and appetite for third-party risks are not yet clearly defined, except within the procurement processes, which follow established tolerance ceilings. To strengthen the third-party risk management process, ICAO should consider best practices identified during the benchmarking with other UN system organizations:

    - Integrate third-party risk management into the existing ERM framework to ensure alignment with ICAO's overall risk appetite and strategic goals.
    - Foster cross-functional collaboration by involving procurement, Information Security, legal, ICT, and other business units throughout the third-party lifecycle.
    - Adopt a risk-based approach, prioritizing oversight and resources for high-risk vendors and critical services, and regularly review those services by management and oversight functions.

Recommendation 3 (High Priority)	Third-Party Risk Management
To address inconsistent oversight, fragmented risk assessments, and limited visibility into third-party performance, ICAO Management should formally incorporate third-party risk management into the outsourcing framework, based on applicable ERM processes. This should include a requirement for a dedicated risk assessment for each outsourced service, with regular monitoring of the effectiveness of mitigating measures.	

Assurance over outsourced services

40. Obtaining assurance over the internal controls for outsourced services is essential for mitigating operational, financial, legal, and reputational risks, as the accountability for outsourced services remains with the organization. Assurance mechanisms such as independent audits and certifications (e.g., ISO 27001[5], ISAE 3402[6]), internal control assessments, contractual audit clauses, well-defined service level agreements, and risk-based monitoring frameworks help ensure that external service providers are managing risks appropriately. These mechanisms enhance governance, accountability, and operational efficiency by providing confidence in the reliability and integrity of outsourced arrangements.

41. In the absence of formal assurance mechanisms, organizations face heightened risks, including data breaches, service disruptions, reputational damage, and financial losses. OIO observed that ICAO currently lacks systematic processes to obtain assurance over the internal controls of third-party service providers, especially for services outsourced to UN system organizations. These entities apply mutual recognition and single audit principles, but this may not guarantee regular assessment of controls related to an outsourcing entity. This gap has also been highlighted by the UN external audit providers and the Evaluation and Audit Advisory Committee (EAAC), particularly in relation to the ERP Quantum and other outsourced services. These assurance issues are a growing concern and underscore the need for a coordinated approach to managing outsourced services shared by different organizations.

42. A review of MOUs and contracts for sampled cases revealed several issues:

    - The MOU between UNDP and ICAO for the provision of ERP services, along with the associated SLAs, does not cover regular assurance provisions over internal controls. Given that UNDP manages ICAO's sensitive data and personally identifiable information (PII) of its personnel, it is essential for ICAO to obtain formal assurance regarding the adequacy of these controls. As a member of the Quantum Consortium, ICAO should continue to engage with UNDP and other partners to establish an annual assurance mechanism that addresses these concerns.
    - ICAO's interim payroll services agreement with UNDP lacks explicit assurance provisions. This arrangement was based on a mutual understanding that ICAO would subsequently establish a comprehensive corporate MOU with UNDP, supported by detailed SLAs for each service. OIO recommends that future detailed SLAs for payroll include requirements for UNDP to demonstrate the effectiveness of its internal controls, including data protection, accuracy, and compliance.

[5] Information Security Management Systems (ISMS)

[6] International Standard on Assurance Engagements (ISAE) are Assurance Reports on Controls at a Service Organization.

- The Master Service Delivery Agreement (MSDA) for ICAO Digital Transformation between UNICC and ICAO indicates that UNICC has ISO 20000[7], ISO 27001, and ISAE 3402[8] certifications. While it is encouraging to see that UNICC has introduced compliance with ISAE 3402 since 2013, there is no indication in the MSDA that these assurance reports are provided systematically to ICAO. Therefore, it is essential that ICAO receives regular assurance reports to confirm that UNICC continues to comply with ISAE 3402 standards.
- The Languages Services Management System audit (IA/2025/01) also identified a lack of adequate third-party assurance mechanisms for United Nations Software-as-a-Service (SaaS) applications, raising concerns about data security, service reliability, and compliance.
- The review of health insurance service showed that the service provider's internal controls are reviewed by its external auditors as part of the audit of its annual financial results, but ICAO did not receive copies of these audit reports due to external restrictions. This lack of direct assurance was partially mitigated by strengthening ICAO's own internal controls and validation processes.

43. Benchmarking with other UN system organizations revealed a good practice where one UN agency required a confirmation letter from the service provider's oversight entity that most of the outsourced functions were covered by its audit in recent years. OIO recommends that ICAO require annual assurance statements from its third-party service providers. See recommendation 1, which includes assurance provisions.

Section III: Internal controls

44. Although ICAO has established internal controls within existing frameworks such as the Procurement Code, ERM, and the Accountability Framework, due to inadequate governance and risk management processes (see Section I and Section II), these controls are not sufficiently standardized or risk-focused for managing third-party service providers. This may lead to fragmented and inconsistently applied controls across outsourced relationships.

45. To strengthen the management of third-party relationships, ICAO should design and implement robust, standardized internal controls that span the entire third-party lifecycle, from sourcing and due diligence to contracting, monitoring, issue resolution, and termination. Such controls are critical to ensure consistency, accountability, and effective risk mitigation.

Business Case and Sourcing

46. Outsourcing decisions should be justified through a formal business case reviewed by a governing entity or second-line oversight function before they are approved. During the initial identification phase, management should begin conducting preliminary research and due diligence to narrow down potential candidates. Before engaging a third party, it is critical to understand the business context and associated risks.

47. ICAO's contracts issued by Procurement in excess of $200,000 ($50,000 in case of sole-source) are submitted to the Contracts Board, which reviews the procurement process and reasonableness of price and makes a recommendation to the Secretary General. While this is recognized as good internal control for the procurement process, it is suggested that outsourcing business cases should be reviewed by a governance body prior to the procurement process, given the significant risks associated with outsourcing services to third parties.

48. The review of documents revealed the absence of a standardized process for outsourcing projects, resulting in incomplete and inconsistent information for decision-making. It is essential to develop a standard business case template that includes cost-benefit analysis, risk assessment, and evaluation of alternatives, as well as in-house components and future management. Business cases must demonstrate long-term value and address potential risks, including implementation challenges and the impact of vendor failure. Practices at

[7] IT Service Management (ITSM)
[8] ISAE 3402, titled Assurance Reports on Controls at a Service Organization, is an international assurance standard that describes Service Organization Control (SOC) engagements, which provide assurance to an organization's customer that the service organization has adequate internal controls.

ICAO for outsourcing vary depending on the type of service and whether the service provider is a UN organization or a commercial entity. For sampled outsourcing cases to UN organizations, OIO found that:

- In the case of ERP, a business case had been developed outlining business needs, alternative solutions, implementation path, timeline, contingency plan, change management, and risk management. This business case was approved by the Digital Transformation Programme Board.
- For payroll services, an implementation options analysis was conducted to identify the best approach for integrating payroll within the ERP solution. However, a full business case was not developed for outsourcing, as the payroll module was initially included as an in-house module in the ERP-PPM project, which was subsequently descoped to exclude payroll management.
- Business cases related to UNICC followed different governance due to the introduction of the TO board in 2023. Business cases related to Business Plan Output SS15 projects were reviewed by the Information Management Committee (IMC) and approved by the Secretary General, whereas after the introduction of the TO, proposals and business cases related to Business Plan Output TO3 and TO4 were reviewed and approved by the Digital Transformation Programme Board.

Due Diligence

49. Once ICAO has shortlisted potential third-party providers, it is essential to conduct comprehensive due diligence. This should include risk assessment, background checks, compliance verification, and evaluation of the vendor's information security posture. These steps are critical to ensure that vendors meet ICAO's standards and requirements.

50. OIO observed that due diligence activities are currently fragmented across various frameworks, such as the Procurement Code, Information Security Policy, Vendor Sanctions Policy, Anti-Fraud Anti-Corruption Policy, and the Policy on Interactions with External Parties. There is a need for dedicated provisions that outline all due diligence requirements specifically for outsourcing arrangements.

51. A positive practice was noted in the area of cybersecurity, where the ICAO Information Security Office conducts risk assessments using the Supplier Security Assessment Questionnaire (SSAQ) for outsourcing to third parties. This ensures that the vendor's information security management programme complies with internationally recognized standards and meets ICAO's Minimum Vendor Information Security Requirements. OIO confirmed that SSAQs were completed for all sampled cases for this audit. These assessments are currently performed at the initial contracting stage and upon contract renewal, providing a point-in-time snapshot of the vendor's security strategy and controls. OIO advises that, as good assurance practice, the SSAQ be updated periodically to maintain continuous oversight of the vendor's evolving cybersecurity posture, in line with the Administrative Instructions on Information Security.

Contracting

52. Contracts are essential for managing third-party risks. They should clearly communicate ICAO's risk appetite, internal control expectations, and service standards, and include safeguards such as SLAs with Key Performance Indicators (KPIs), data protection clauses, audit rights, termination provisions, and clearly defined roles and responsibilities.

53. All agreements and contracts for outsourced services should be reviewed by a governance committee, with inputs from relevant stakeholders, including PRO, LEB, CISO, ERM, and other SMEs where applicable, to ensure comprehensive risk coverage. Inadequate contract review, especially without SME involvement, is a common risk.

54. A leading practice is to use the organization's own standard contract templates, which can be customized as needed. In the case of UN entities, OIO observed that ICAO, in general, does not use its own templates of MOU and SLA, and the signed MOUs did not always include provisions such as assurance and audit rights. However, in the case of a commercial service provider, OIO observed that ICAO's own contract template was used, which was comprehensive and included important provisions such as audit rights, confidentiality clause, subcontracting, and termination provisions. OIO recognizes this as good practice and suggests that ICAO's standard contract template be used, to the extent possible, for future outsourcing arrangements. In cases

where a third-party provider's contract template is used, ICAO should ensure that all pertinent provisions are included in the contract and SLA.

55. OIO found varying practices related to provisions on business continuity and incident reporting in the contracts with third parties, which pose a risk of service disruption to outsourced services in the event of a cyber or other incidents.

Monitoring and Issue Resolution

56. ICAO contract managers should regularly monitor the performance of outsourced service providers to ensure compliance with contractual obligations, SLA parameters, and long-term value for money. This includes reviewing vendor performance and obtaining and assessing assurance reports, such as ISAE 3402, where applicable.

57. To strengthen oversight, OIO advises that in the Terms of Reference for the procurement of outsourced services, the requesting office clearly outline the requirements for relevant certifications and periodic reporting on specific KPIs. Automated tools and dashboards can support continuous monitoring of critical outsourced service providers. In the case of UNICC, although the service provider holds certifications such as ISO 27001, ISO 20000, ISO 22301[9], and ISAE 3402, these reports are not systematically shared with or reviewed by ICAO.

58. Additionally, risks associated with fourth-party providers, i.e., vendors used by ICAO's third parties, are more difficult to manage, as they fall outside ICAO's direct control. These need to be part of ICAO's due diligence and risk management.

59. In one sampled case, ICAO receives annual stewardship reports from its service provider, detailing performance against agreed KPIs and service standards. The contract includes specific performance metrics, and the contract manager has also implemented a mechanism to periodically validate the accuracy of some data and monitor the value-for-money of this contract.

60. In other cases, outsourcing has not yet stabilized to perform ongoing reviews of value-for-money of services, including the realization of expected benefits and control of overall costs, including servicing fees and any in-house costs. Continuous monitoring of the quality and costs will allow ICAO to demonstrate the continued value for money of its outsourced services.

61. OIO noted a good practice in other UN entities where service providers' costs and performance were continuously monitored to ensure the outsourced service continued to provide value for money to the organization.

62. Third-party relationship owners must actively monitor and address service issues, failures, or breaches. While ICAO's contracts include a general provision about incident reporting and issue resolution, most contracts lack detailed provisions and KPIs, supported by clear documentation and escalation protocols. The need to implement strong access control provisions to limit third-party access to sensitive systems and data is paramount. Data exchanged with vendors must be protected both in transit and at rest. Vendors should be required to promptly report any incidents involving ICAO data.

63. Benchmarking with other UN system organizations showed that centralized ongoing monitoring of third-party contracts helps ensure consistency and value-for-money.

Termination

64. Contract termination provisions are essential to protect ICAO from vendor lock-in and mitigate risks associated with early termination. While the contracts with sampled third-party service providers included a termination clause, they lacked clearly defined exit plans, outlining procedures for service transition and secure return or destruction of sensitive data upon termination.

[9] Business Continuity Management System (BCMS)

Recommendation 4 (High Priority)	Internal Controls
ICAO Management should coordinate with the contract managers to ensure that all future contracts for outsourcing arrangements include risk-driven internal controls to govern the full lifecycle of third-party service providers, as established in the new outsourcing framework (see recommendation 1).	

ANNEX 1: MANAGEMENT ACTION PLAN

Ref	Recommendation	Closure Criteria	Priority Rating	Accepted (Y/N)	Agreed Actions	Office/ Section Responsible	Target Date
1.	ICAO Management, in collaboration with PRO, ERM, CISO, LEB, and other SMEs, should develop a comprehensive outsourcing framework by consolidating existing provisions and strategies related to outsourcing arrangements at ICAO. This framework should, at a minimum, define outsourcing, establish risk tolerance, clarify delegated authority, set governance and oversight, outline key phases of the outsourcing lifecycle, address requirements for risk management, data protection and security, performance monitoring and evaluation, assurance, as well as exit strategy and transition planning.	An outsourcing framework, either as a standalone governance document or embedded within the ICAO Procurement Code.	High	Yes	Management will provide a detailed action plan during the 1st quarter of 2026.	To be decided	No later than 31 December 2026
2.	In order to have visibility over all the outsourced services and the associated third-party and fourth-party risks, ICAO Management should complete and maintain the inventory of existing and future outsourced services to be used for risk management and oversight processes.	A comprehensive database with a dedicated dashboard of all outsourced services and their primary service providers and related documentation.	Medium	Yes	Management will provide a detailed action plan during the 1st quarter of 2026.	To be decided	No later than 31 December 2026
3.	To address inconsistent oversight, fragmented risk assessments, and limited visibility into third-party performance, ICAO Management should formally incorporate third-party risk management into the outsourcing framework, based on applicable ERM processes. This should include a requirement for a dedicated risk assessment for each outsourced service, with regular monitoring of the effectiveness of mitigating measures.	Embedding of third-party risk management within the outsourcing framework.	High	Yes	The ERM function will participate in the development of the outsourcing framework (as part of the actions for Recommendation # 1) by reviewing and strengthening the risk assessment approach for outsourcing decisions and subsequent monitoring activities.	OSG	No later than 31 March 2027

Ref	Recommendation	Closure Criteria	Priority Rating	Accepted (Y/N)	Agreed Actions	Office/ Section Responsible	Target Date
4.	ICAO Management should coordinate with the contract managers to ensure that all future contracts for outsourcing arrangements include risk-driven internal controls to govern the full lifecycle of third-party service providers, as established in the new outsourcing framework (see recommendation 1).	A documented mechanism to confirm internal controls, as established in the framework, for outsourcing contracts. The outsourcing framework includes provisions for key compliance requirements and controls, including: - at sourcing – business cases with cost-benefits and risk assessment. - at tendering – due diligence, data and cybersecurity assessments and risk updates. - at contracting – comprehensive provisions on roles and responsibilities, set of expected controls, KPIs and performance monitoring, audit and assurance clauses, data protection, incident and issue resolutions, and termination provisions. - at contract management and monitoring – regular reports against the KPIs, areas for improvement and risk updates, including review of continued value for money.	High	Yes	Management will provide a detailed action plan during the 1st quarter of 2026.	To be decided	No later than 30 June 2027

ANNEX 2: DEFINITION OF AUDIT TERMS

Audit Ratings

In providing an overall assessment of the results of the audit, OIO uses the following standardized audit rating definitions:

Audit Assessment	Definition
Effective	Controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Some Improvement Needed	A few specific control weaknesses or areas for improvement were noted; generally however, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Major Improvement Needed	Several key control weaknesses were noted and/or several areas of strategic/high importance were identified where significant improvements can be made to increase efficiency and effectiveness.
Unsatisfactory	Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and objectives should be met.

Internal control is defined as a process effected by senior management and staff, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance objectives. Whilst internal control provides reasonable (but not absolute) assurance of achieving organizational objectives, limitations may result from:

- suitability of objectives established as a precondition to internal control;
- reality that human judgment in decision making can be faulty and subject to bias;
- breakdowns can occur because of human failures such as simple errors;
- ability of management to override internal control;
- ability of management, other staff, and/or third parties to circumvent controls through collusion;
- external events beyond the organization's control.

Priority of Audit Recommendations

The audit recommendations in this report are categorized according to priority as a guide to management in addressing the issues raised. The following categories are used:

High: recommendations, which address significant and/or pervasive deficiencies or control weaknesses, or areas where significant improvements can be made.

Medium: recommendations, which address important deficiencies or control weaknesses, or areas where some improvements can be made.

Low: suggestions, which represent best practice, or general opportunities for improvement.