The Institute of Internal Auditors

IFACI Certification

INTERNATIONAL CIVIL AVIATION ORGANIZATION
OFFICE OF INTERNAL OVERSIGHT - INTERNAL AUDIT – EXTERNAL QUALITY ASSESSMENT

Report – December 2024

Contents

The IIA independent assessment team would like to thank the OIO and ICAO stakeholders for their valuable contributions to this Quality Assessment.

"Il semble que la perfection soit atteinte non quand il n'y a plus rien à ajouter, mais quand il n'y a plus rien à retrancher."

"Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away."

- Antoine de Saint-Exupéry (1900-1944*), l'Avion (*Terre des hommes*)

EXECUTIVE SUMMARY

SECTION 1

ICAO – OIO – Internal Audit
External Quality Assessment - 12/2024

Executive Summary

Standards Sections	⚓ Attribute Standards				⚙ Performance Standards							👍 IIA Code of Ethics
Standard Categories	1000 Purpose, Authority, and Responsibility	1100 Independence and Objectivity	1200 Proficiency and Due Professional Care	1300 Quality Assurance Improvement Program	2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance	IIA Code of Ethics
Conclusions	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms	Generally conforms
Overall opinion	**Generally conforms**											

Notable OIO accomplishments

- In our opinion, the OIO audit activity **generally conforms** with the International Professional Practice Framework (2017) and the Code of Ethics of the Institute of Internal Auditors.

- OIO's audit function, despite its small size, delivers assurance across a wide range of topics, demonstrating the experience, qualifications and technical competence of the team.

- OIO has struck a good balance between partnering with the business and aligning with ICAO strategic objectives while remaining objective and independent, both organisationally and in mindset.

- OIO's communications, both formal and informal, are seen as "excellent". Audit reports synthesize complex matters effectively and are well received, even when the message is critical. Regular contact with stakeholders ensures currency, relevance and understanding. OIO recommendations are weighty and valued by management.

- OIO's data analytics capacity has developed well and is a definite strength.

Recommendations for OIO

Adoption of a framework for IT Governance assurance (3.1)
- OIO should adopt a recognized IT governance framework to guide its IT audit work

Role in ERP (3.2)
- OIO should undertake a more pro-active challenge of the ERP project

Resources (3.3)
- Given the inherent risks associated with its small scale, OIO should explore alternative resource models

Data analytics: a strength (3.4)
- OIO should continue to develop its strong data analytics capability, particularly in the context of Quantum. OIO could share its skills with the business.

Plans to adopt an audit tool (3.5)
- Plans to adopt an audit automation tool should be coordinated and optimized carefully with ERM and other relevant functions.

Further opportunities for continuous improvement (3.6)

Opinion of the IIA Evaluation Committee

The IIA Evaluation Committee confirms that ICAO's Office of Internal Oversight (OIO) generally conforms with the IIA Standards (2017) and Code of Ethics.

We commend OIO's strong governance alignment, stakeholder engagement, and audit excellence while encouraging further enhancements in IT governance, ERP oversight, and resource scalability.

IIA Standards	GC	PC	NC	NA	Reference to recommendations / insights
1000 - Purpose, Authority, and Responsibility & 1000.A1	GC				
1010 - Recognition of the IPPF in the Internal Audit Charter	GC				
1100 - Independence and Objectivity	GC				
1110 - Organizational Independence	GC				
1110.A1 - Free from interference	GC				
1111 - Direct Interaction with the Board	GC				
1112 - Chief Audit Executive Roles Beyond Internal Auditing	GC				
1120 - Individual Objectivity	GC				
1130 - Impairment to Independence or Objectivity	GC				
1200 - Proficiency and Due Professional Care	GC				
1210 - Proficiency	GC				
1210.A1 Obtain competent advice and assistance	GC				
1210.A2 Fraud	GC				
1210.A3 Systems	GC				
1220 - Due Professional Care	GC				
1220.A2 Systems	GC				
1230 - Continuing Professional Development	GC				
1300 - Quality Assurance and Improvement Program	GC				
1310 - Requirements of QA & Improvement Program	GC				
1311 - Internal Assessments	GC				
1312 - External Assessments	GC				
1320 - Reporting on Quality Assurance & Improvement Program	GC				
1321 - Use of "Conforms with the IPPF"	GC				
1322 - Disclosure of Nonconformance	GC				
2000 - Managing the Internal Audit Activity	GC				
2010 - Planning	GC				
2010 - Systems	GC				
2020 - Communication and Approval	GC				
2030 - Resource Management	GC				
2040 - Policies and Procedures	GC				
2050 - Coordination	GC				
2060 - Reporting to Senior Management and the Board	GC				
2070 - External Service Provider	GC				
2100 - Nature of Work	GC				
2110 - Governance	GC				
2110.A1 Ethics	GC				
2110.A2 Systems		PC			
2120 - Risk Management	GC				
2120.A1 Systems		PC			
2120.A2 Fraud	GC				
2130 – Control	GC				
2130.A1 Systems		PC			

IIA Standards	GC	PC	NC	NA	Reference to recommendations / insights
2200 - Engagement Planning	GC				
2201 - Planning Considerations	GC				
.A2 - Engagement Objectives	GC				
2220 - Engagement Scope	GC				
2220.A1 Systems	GC				
2230 - Engagement Resource Allocation	GC				
2240 - Engagement Work Program	GC				
2300 - Performing the Engagement	GC				
2310 - Identifying Information	GC				
2320 - Analysis and Evaluation	GC				
2330 - Documenting Information	GC				
2340 - Engagement Supervision	GC				
2400 - Communicating Results	GC				
2410 - Criteria for Communicating	GC				
2420 – Quality of Communications	GC				
2421 – Errors and Omissions	GC				
2430 – Use of "Conducted in Conformance with the IPPF"	GC				
2431 – Engagement Disclosure of Nonconformance	GC				
2440 – Disseminating Results	GC				
2450 - Overall Opinions	GC				
2500 – Monitoring Progress	GC				
2600 – Resolution of Senior Management's Acceptance of Risks	GC				
Code of Ethics	GC				

Legend	
GC	Generally conforms
PC	Partially conforms
NC	Does not conform
NA	Not applicable/not assessed
GTC	Gap to conformance
OCI	Opportunity for continuous improvement

3
SECTION

RECOMMENDATIONS

ICAO – OIO – Internal Audit
External Quality Assessment - 12/2024

The Institute of
Internal Auditors

The Institute of Internal Auditors

Observation

IT risks are particularly critical at this point in ICAO's development, not least given the significant and ambitious objectives of the Transformational Objective (TO), including its focus on "Digitization" and "Information Security" as key facilitators of transformation. Thus, ICAO has a growing appetite for assurance over IT and information security risks. This is highlighted in our stakeholder interviews (see section 4).

In addition to considering systems risks in non-IT audits, OIO's approach to providing assurance over systems risks has largely focused on its selection of approximately one dedicated IT audit per year. Recent IT projects included:

• IT Asset Management (2023/2024)
• Review of Information Security Roadmap implementation (2022)
• Performance Audit of Data Management (2021/2022)

In addition, OIO has been working closely with the CISO in the context of ICAO's adoption of ISO 27000 and is currently considering how it will continue to play a role in providing assurance over ICAO's adoption of the ISO 27000 information security standard (see also 3.3).

All this work contributes significantly to assurance over IT risks; however, OIO is now at a juncture where it could significantly enhance its IT assurance capacity. As a guiding foundation for that capacity, we would expect OIO to have adopted a widely accepted standard to frame its work in IT governance, such as COBIT, ITIL or other. Further, we believe there are significant opportunities to deliver assurance in the Quantum project (see 3.2) and to consider IT audit resourcing needs (3.3).

Recommendation

We recommend that OIO adopt a widely recognised IT governance framework such as COBIT or ITIL, to bring a holistic structure to their ongoing IT risk analysis and assurance. Where possible, that analysis should leverage and align with any existing governance work that ICT may have implemented, including the ERP (see also 3.2) and ISO 27000 initiatives (see also 3.3).

Further, OIO should collaborate with ICAO's ICT and other assurance providers to map assurance across the standard IT governance framework, thereby ensuring completeness of IT risk assessment and assurance coverage as part of a multi-year rotational plan.

OIO Action Plan

OIO agrees with the recommendation and plans to adopt best practice IT Governance Frameworks during 2025-2026 as part of its annual and ongoing risk assessment to inform our IT audit plan.

OIO will continue collaborating with ICT to ensure completeness of the IT risk assessment and audit coverage for its multi-year rotational plan.

Related Standards

Gaps to conformance 2110.A2, 2120.A1, 2130.A1

Observation

The ERP (Enterprise Resource Planning) project is ICAO's initiative to move to a cloud-based Oracle solution in an established multi-UN body consortium led by UNDP, known as Quantum. Started in 2024, it is a flagship project under the Transformational Objective (TO). It is complex, placed at the heart of the organisation, and will therefore have a fundamental effect on risk and internal control. Key stakeholders are looking to OIO to provide assurance over the ERP project and related processes.

OIO's involvement in the project to date has included:

- Advising management in terms of their plans and business decisions on an *ad hoc* basis;
- Reviewing, at a high-level, progress of the project, within the "Mid-Term Assessment of the Implementation of the TO" (July 2024); and
- Providing the ERP team with initial criteria for a risk-focused roll-out readiness assessment (on OIO's initiative).

In 2025, OIO plans to do the following work in relation to ERP:
- A roll-out readiness assessment (per the criteria above);
- A review of the effectiveness of the implementation of one module (likely the Human Resources module, since financial modules are to be covered by external audit); and
- An end-to-end risk and internal control process assessment for selected processes.

We note that OIO is largely focused on the non-financial aspects of the ERP implementation, as the External Auditors are understood to be concentrated on the financial aspects of the project.

OIO resources have direct experience working with Quantum at UNDP and UN Women and are therefore well placed to foresee risks and propose practical solutions that require detailed experience and are pertinent to ICAO's implementation.

Related Standards

Opportunities for continuous improvement 1210.A3, 2000, 2030, 2050, 2130.A1

Recommendation

We encourage OIO's further pro-active involvement in and constructive challenge of the ERP project. In the short term, this should take the form of providing assurance over the effectiveness of project management, roll-out plans and, as foreseen, risks and internal controls in all the processes affected by the implementation, including financial processes. All this work should aim to also foster the development of a strong Second Line[1].

It is prudent to avoid duplication of work to the extent that the External Auditors may be involved with financial processes. However, experience suggests that internal audit may have the capacity and perspective to provide assurance that covers a wider range of criteria beyond external audit requirements. Therefore, internal audit functions often take the lead on providing (Third Line) assurance over ERP processes.

Generally, OIO should engage with the external audit team to explore how external audit may be able to rely on the work of internal audit, where possible, in accordance with International Standard on Auditing 610 and other relevant guidance / constraints.

In the medium term, we would encourage OIO to formulate a strategy to continue to develop data-rich audit techniques, including continuous auditing, in the context of the new ERP environment (see 3.4). OIO is well positioned to leverage its evident strength in data analytics to provide cost-effective assurance with fewer resources than might otherwise be required. OIO may also play a facilitative role in the organisation's adoption of analytic tools such as PowerBI, and thereby support the Second Line, if only temporarily.

OIO, while providing such value-added assurance and facilitation to ICAO, should carefully weigh such value with the need to maintain the objectivity and independence of the Third Line[1].

1. *The IIA's Three Lines Model*, The Institute of Internal Auditors, July 2020. See also *Leveraging COSO across the Three Lines of Defense*, COSO, July 2015.

OIO Action Plan

OIO agrees with the recommendation and has planned three audit/advisory engagements specific to the REP implementation in 2025.

In line to increase coordination and related reliance on OIO work, OIO will continue coordination with the external auditor, including regular information exchange on the oversight topics, work plans and observations/conclusions to ensure effective oversight coverage.

OIO will update its continuous data analytics audit approach, by exploring the use of artificial intelligence and new ERP data for its oversight needs. OIO will assess the need and liaise with the second-line functions to share its good practices without compromising its independence.

Observation

OIO's internal audit team comprises three professional staff under the leadership of the Chief OIO and the assistance of an administrative staff member (see 6.4 Organization Chart). Despite its small size, the team covers an impressive range of competencies through their extensive professional experience, training and professional qualifications. OIO's expertise and skills are widely appreciated by auditees and governance bodies, as corroborated during our stakeholder interviews.

The small size of the team nonetheless gives rise to several inherent risks, including:

- Dependence on individuals and therefore continuity risk;
- Lack of leverage – with no junior staff, all audit work is performed by senior professionals, which is sub-optimal from cost-effectiveness and job satisfaction perspectives;
- Despite best efforts and the capabilities of the team, there are gaps in deep technical expertise in increasingly important operational areas and in IT (e.g. cyber security);
- Lack of spare capacity to provide additional assurance or advisory work, as recently requested by oversight bodies and auditees.

We also observed that management has increasing expectations for OIO to provide assurance in the absence of strong Second Line oversight and monitoring.

Related Standards

Opportunities for continuous improvement: 1200, 1210, 2020, 2030, 2050, 2110 2230, 2250.1

Recommendation

OIO should consider alternative resourcing and assurance models to enhance capacity and skills, and thereby to mitigate the risks associated with the small size of the internal audit team. OIO could also facilitate mapping Second Line assurance responsibilities. The following are examples of possible solutions discussed with OIO and stakeholders during our review:

- **Long-term agreement with IT audit service provider.** As noted in 3.1, ICAO's digitization program will increase the need for assurance over a range of technologies. It is a common practice, especially for small audit groups, to engage a specialist IT audit firm with the scale to provide resources as required, as part of a long-term agreement (LTA). OIO plans to engage such a firm for its periodic review of ICAO's ISO 27000 regime; that arrangement could be extended to cover other occasional specialized IT audit needs. (See also 3.1 and 3.2)
- **Third party assurance in the context of the Quantum consortium.** OIO should work with ICAO management and other Quantum consortium members to pursue a collective approach to assurance over the design and operating effectiveness of internal controls related to Quantum. This may take the form of reliance on other user organizations' assurance. It may also be possible to institute a third-party Service Organisation Control type 1 (SOC1) audit service auditors' report covering collective internal controls.
- **Guest auditors**. To foster mutual exchanges of technical knowledge and audit skills and awareness, guest auditors could be deployed on specific engagements. Guests could be brought in from other ICAO functions or other UN bodies and may provide generic capacity or specialized technical expertise. It may be possible to operate such a scheme with little or no direct cost implications. Objectivity and independence and maintenance of quality would have to be carefully considered.
- **Documentation, peer review.** OIO team members should continue to document audits thoroughly such that a third party could readily follow the working papers (we noted this as a strength in our review of files). This aspect could be furthered by the adoption of standard processes and documentation within the planned audit automation tool. Peer review of files would also aid continuity.
- **Investigations**. If OIO is involved in the insourcing of investigation services, it will likely involve augmenting the team with specialist investigators and/or engaging a specialist firm of investigators on an LTA, overseen by OIO.

OIO Action Plan

OIO agrees with the recommendation and will consider mechanisms such as alternative resourcing and assurance types to enhance its capacity and skills, and to mitigate the risks associated with the small size of its internal audit team.

OIO plans to perform a mapping of second line assurance responsibilities.

Observation

OIO has developed its data analytics capacity well in recent years. Our file review afforded us a view of exemplary data work using PowerBI and other tools, such as on the Payroll, IT Asset Management and Procurement audits. Such data analysis results, in much greater coverage of transactions than might otherwise be possible, provide unique insights, and thereby amplify the potential assurance derived from audit engagements.

With the implementation of the new ERP, the potential for data analysis techniques will dramatically increase due to standardization, the consolidation of legacy systems, and anticipated improvements in data quality and ease of access. In addition, "continuous auditing", in which data is continually extracted and analyzed, and results reported to auditors, will be more readily achievable.

Related Standards

Opportunities for continuous improvement: 1220.A2, 2420

Recommendation

In addition to OIO's role in the ERP noted in 3.2, OIO should also undertake an explicit stream of work to foresee and develop the potential for data analytics and continuous auditing in the new system.

The primary objective for this work should be for OIO to obtain audit assurance in its Third Line[1] role. However, OIO is also well positioned to encourage the adoption of such valuable techniques by the First and Second Lines[1]. Through demonstrations, possible training and awareness building, but refraining from direct design or operation of controls, OIO could deliver considerable value while maintaining its independence and objectivity.

OIO should explore presentation-style, or even online interactive report formats, particularly for data analytics and continuous audit output, building on the user-friendliness of its current PowerBI dashboards.

1. *The IIA's Three Lines Model*, The Institute of Internal Auditors, July 2020. See also *Leveraging COSO across the Three Lines of Defense*, COSO, July 2015.

OIO Action Plan

OIO agrees with the recommendation and plans to update its data analytics and continuous auditing approach based on real-time data from the new ERP system.

OIO will consider conducting training, awareness and coordination with the First and Second Lines while advocating for the importance of dashboards and exception-based reports.

Observation

OIO plans to adopt an audit tool, principally to automate audit working papers and thereby streamline and further standardize audit processes and workflows. While IFACI remain neutral as to the efficacy of audit automation tools, many audit functions benefit from the efficiencies of a well-implemented system.

The tool is also intended to include management recommendation processing and workflow, and potentially functionality supporting Enterprise Risk Management. We are also aware that the ERM initiative has ambitions to implement an in-house developed or packaged tool to automate ERM processes.

Related Standards

Opportunities for continuous improvement: 2000, 2010.1, 2120, 2300, 2330, 2500.1

Recommendation

OIO should consider involving the incoming manager responsible for ERM and with relevant senior management to ensure that an optimal and efficient solution for ERM functionality can be coordinated with the planned audit tool.

Consideration should be given to the following:

- The need to incorporate and maintain strategic, program and other organizational objectives in the tool automatically;
- Automated integration with Quantum and reporting systems (such as PowerBI), as appropriate;
- Facility to leverage ERM risk analysis into aligned audit risk analysis and planning;
- The necessity for OIO to maintain its Third Line[1] independence and objectivity with regards to ERM standards, processes (Second Line[1]) and substantive content (First Line[1]).

In an eventual adoption of an audit tool, OIO should undertake a thorough review of relevant information security risks, particularly related to a cloud-based solution. Those risks may be augmented and made more complex if the solution contains self-service auditee / management functionality such as management recommendations or other ERM/GRC functionality.

1. *The IIA's Three Lines Model*, The Institute of Internal Auditors, July 2020. See also *Leveraging COSO across the Three Lines of Defense*, COSO, July 2015.

OIO Action Plan

OIO notes the recommendation and will provide advice to ensure an optimal and efficient solution for ERM functionality, without compromising its oversight needs in selecting the audit application.

OIO will review information security risks with support from CISO before implementing the audit tool.

Observations

We observed the following further opportunities for continuous improvement (OCI#nnnn where nnnn is the relevant Standard):

- **OCI#1220** While the selection of audits and scope is risk-driven, allocation of staff at the planning stage does not necessarily reflect differences in risk, complexity and other factors. Instead, it is a rough, standard allocation of person-days (50 days for 2024).

- **OCI#1311** OIO's self-assessment, part of its Quality Assurance and Improvement Program (QAIP), performed April 2024 was performed by a team member.

- **OCI#2010** OIO have implemented an impactful PowerBI planning tool and performance monitoring dashboard.

- **OCI#2440** The SG is currently required to "endorse" management action plans prior to the finalisation of audit reports. This can often cause some delay in report issuance due to OSG workload.

- **OCI#2450** The report ratings are not formalised in the Audit Manual.

- **OCI#2450.1** Conclusions at the level of the business unit or organization.

Recommendations

- **OCI#1220** Consider the benefits of tailoring budgets by audit, such that resources are allocated and tracked on a risk driven and cost-effective basis.

- **OCI#1311** OIO's self-assessment within its quality assessment program (QAP) could be more objective and therefore insightful if performed by a peer external to the audit function, but nonetheless familiar with the Standards.

- **OCI#2010** Consider sharing the OIO PowerBI dashboard more widely with stakeholders.

- **OCI#2440** Consider changing the necessity for the SG to endorse all management action plans to streamline the process. One possibility might be to require the SG's involvement where there is disagreement, its overall rating is low, or the subject of the audit is particularly sensitive or wide-reaching.

- **OCI#2450-1** OIO should consider including report rating and associated guidance in the Audit Manual currently under revision.

- **OCI#2450** OIO should consider the implications of and guidance for Standard 11.3 of the 2024 *Global Internal Standards*, specifically the assurance needs and requests of the Council, EAAC and Senior Management, balanced with OIO's capacity to deliver such conclusions.

OIO Action Plan

OIO agrees with the above opportunities for enhancement. The following will be actioned:

- OIO will determine its budget and time to be spent for individual oversight engagement, by allocating resources based on risks and audit scope.

- OIO will reach out to UNRIAS community members to perform an internal self-assessment once within a five-year cycle.

- OIO will assess which of its Power BI dashboards can be more widely shared with its stakeholders. This determination will be made after OIO's tools are updated and linked to the new ERP.

- The Chief OIO will discuss with the SG their involvement in the audit report issuance process, including the cases where management disagrees with audit recommendations or if the engagement is particularly sensitive or wide-reaching.

- OIO will include its report rating and associated guidance in the Audit Manual which is currently under revision to incorporate GIAS requirements. Currently, the report rating and associated guidance are referred to in the Annex to the Audit Manual.

- OIO is in the process of incorporating the requirements of GIAS, including the consideration of assurance needs and requests of the Council, EAAC and Senior Management. The needs assessment will be linked with OIO's assurance mapping exercise.

OBSERVATIONS BY STANDARD

ICAO – OIO – Internal Audit
External Quality Assessment - 12/2024

The Institute of
Internal Auditors

The Institute of Internal Auditors

1000 Purpose Authority and Responsibility	1100 Independence and Objectivity	1200 Proficiency and Due Professional Care	1300 Quality Assurance and Improvement Program

IPPF Mandatory Requirements

- **1000**. The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

- The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization, including the nature of the chief audit executive's functional reporting relationship with the board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.

- **1000.A1** – The nature of assurance services provided to the organization must be defined in the internal audit charter.

- If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

- **1000.C1** – The nature of consulting services must be defined in the internal audit charter.

Demonstrated Accomplishments
Areas for further Conformance Action

- The Charter clearly sets out the purpose, authority and responsibility of the audit activity.
- The Charter is approved by the Council, establishing:
  - OIO's position in ICAO
  - The functional and administrative reporting lines of the CAE
  - The CAE's relationship with the Council
  - OIO's authority to access records, personnel
  - A definition of the scope of audit activities

- The Charter defines the nature of assurance services under Section 3, "Mandate".

- Audit reports are generally published, as defined in Section 9.3 of the Charter.
- Section 7.3 of the Charter restricts advisory engagements to those which could not subsequently affect the objectivity of audit.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
- Conforms

1000
Purpose Authority and Responsibility

1100
Independence and Objectivity

1200
Proficiency and Due Professional Care

1300
Quality Assurance and Improvement Program

IPPF Mandatory Requirements

▶ **1010**. The mandatory nature of the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing must be recognized in the internal audit charter.

▶ The chief audit executive should discuss the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework with senior management and the board.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ The Charter recognizes these in paragraph 1.2.

▶ The Annual Report, discussed with the Council, EAAC and senior management, and published, clearly refers to the Mission and these mandatory elements.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

The Institute of Internal Auditors

1100 – INDEPENDENCE AND OBJECTIVITY - 1110 - ORGANIZATIONAL INDEPENDENCE
1111 - DIRECT INTERACTION WITH THE BOARD - 1112 – CHIEF AUDIT EXECUTIVE ROLES BEYOND INTERNAL AUDITING 1/2

1000
Purpose Authority and Responsibility

1100
Independence and Objectivity

1200
Proficiency and Due Professional Care

1300
Quality Assurance and Improvement Program

IPPF Mandatory Requirements	Demonstrated Accomplishments Areas for further Conformance Action	Recommendations on Gaps to Conformance and Opportunities for Continuous Improvement

IPPF Mandatory Requirements

▶ **1100**. The internal audit activity must be independent, and internal auditors must be objective in performing their work.

  ↳ To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board.

▶ **1110**. The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfil its responsibilities.

▶ The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

  ↳ Organizational independence is effectively achieved when the chief audit executive reports functionally to the board.

▶ **1110.A1**. The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

  ↳ The chief audit executive must disclose such interference to the board and discuss the implications.

Demonstrated Accomplishments

▶ Factors contributing to OIO's independence include:
  ↳ Reporting lines (see below)
  ↳ The establishment of the Communication Plan
    • Regularly scheduled meetings with stakeholders, including the Council, EAAC and senior management
    • Distribution and publication of audit reports
  ↳ OIO participation in senior management meetings and committees
  ↳ Unrestricted access to all records and personnel
  ↳ Conformance with the IIA Standards
  ↳ No direct responsibility for operations
  ↳ Annual OIO and individual declarations
▶ The CAE reports functionally to the Council, and administratively to SG. She receives advice from the EAAC.
▶ The independence of OIO and the CAE is confirmed in the Annual Report to Council.

▶ The Charter declares that the CAE operates free from interference. The CAE confirms that no such interference has occurred.

Recommendations on

Conclusion
▶ Conforms

The Institute of Internal Auditors

1100 – INDEPENDENCE AND OBJECTIVITY - 1110 - ORGANIZATIONAL INDEPENDENCE
1111 - DIRECT INTERACTION WITH THE BOARD - 1112 – CHIEF AUDIT EXECUTIVE ROLES BEYOND INTERNAL AUDITING 2/2

1000
Purpose Authority
and Responsibility

1100
Independence and
Objectivity

1200
Proficiency and Due
Professional Care

1300
Quality Assurance
and Improvement
Program

IPPF Mandatory Requirements	**Demonstrated Accomplishments** Areas for further Conformance Action	**Recommendations on** Gaps to Conformance and Opportunities for Continuous Improvement

IPPF Mandatory Requirements

▶ **1111**. The chief audit executive must communicate and interact directly with the board.

▶ **1112**. Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.

Demonstrated Accomplishments

▶ As defined in the OIO Charter, the CAE reports directly and has unrestricted access to the Council President and the Council, with whom the CAE meets regularly.

▶ The CAE has unrestricted access to the EAAC, who may advise the CAE.

▶ OIO's triennial and annual budgets are presented to the SG and EAAC but approved by the Council (budget extensions can be approved by the SG).

▶ The Council approves the engagement and dismissal of the CAE.

▶ The CAE is also responsible for ICAO's evaluation capacity. IFACI has not identified conflicts of interest between this role and the internal audit function. Evaluation staff can assist audit team members, particularly with specialised technical aviation topics.

Recommendations on

Conclusion

▶ Conforms

1000 Purpose Authority and Responsibility

1100 Independence and Objectivity

1200 Proficiency and Due Professional Care

1300 Quality Assurance and Improvement Program

IPPF Mandatory Requirements

- **1120**. Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

- **1130**. If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

- **1130.A1.** Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

- **1130.A2**. Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

- **1130.A3**. The internal audit activity may provide assurance services where it had previously performed consulting services, provided the nature of the consulting did not impair objectivity and provided individual objectivity is managed when assigning resources to the engagement.

Demonstrated Accomplishments
Areas for further Conformance Action

- OIO's independence is declared in the Annual Report and on each audit. Individual auditors sign ICAO and IIA codes of ethics declarations.

- No instance of impairment noted.

- As noted in Section 7 of the Audit Manual, auditors are required to confirm for each audit that they have no conflict of interest.

- The CAE has no such obligation in the organization.

- OIO is periodically requested to provide ad hoc advisory work. When considering such work, OIO carefully considers how, if at all, it could affect its ongoing third line of defence role.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

- Conforms

Recommendations & Suggestions

- **OCI#1130.A3 (see 3.2, 3.4, 3.5)** In the interests of the organization, particularly to further the maturation of ICAO's risk management and internal control environment, OIO may consider temporarily increasing its activity in 2nd lines of defence. Undertaking such roles could bring considerable value to ICAO and audit functions are often called upon to provide such capacity. However, OIO must carefully consider how such advisory work might affect its ability to provide objective assurance of such areas in the future.

IPPF Mandatory Requirements	**Demonstrated Accomplishments** *Areas for further Conformance Action*	**Recommendations on** *Gaps to Conformance and Opportunities* *for Continuous Improvement*

IPPF Mandatory Requirements

▸ **1200**. Engagements must be performed with proficiency and due professional care.

▸ **1210**. Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

▸ **1210**.**A1** The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Demonstrated Accomplishments

▸ The OIO audit team holds a broad range of qualifications and professional designations, including: 2 X CIA (internal audit), 2 X CA/CPA/ACCA (general accounting), 2 X CFE (fraud), 2 X CRMA(risk management), 2 X CISA (IT audit).

▸ The small size of the audit group creates dependency on individuals and therefore threatens continuity.

▸ IFACI file reviews and other IFACI EQA activity corroborates audit proficiency, skills and knowledge of practitioners.

▸ OIO calls on external consultants to complement the small in-house team, as required. Examples of recent engagements where consultants have been used include: the ERM audit (2023) and the Mid-term Assessment of the TO (2024). However, as noted in 2030, each such arrangement requires SG approval.

Recommendations on

Conclusion

▸ Conforms

Recommendations & Suggestions

▸ **OCI#1200 (see 3.3)** Mitigate dependence on individuals, particularly in IT, through work shadowing, redundancy in skills across team, thorough documentation, continued information exchange across the team, and leveraging external resources.

▸ See **OCI#2030** and **OCI#2230 (see 3.3)** regarding discretionary budget for consultants.

1210 – Proficiency

1000 Purpose Authority and Responsibility	**1100** Independence and Objectivity	**1200** Proficiency and Due Professional Care	**1300** Quality Assurance and Improvement Program

IPPF Mandatory Requirements

▸ **1210.A2** Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

▸ **1210.A3** Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ While OIO does not have dedicated fraud or investigations capacity, Fraud is specifically considered at the audit project level, as corroborated by IFACI file reviews.

▸ The new audit Chief and one other are CFE

▸ Fraud investigation work is outsourced to UN OIOS (which can also provide expert advice)

▸ Audit planning systematically includes "red flags"

▸ "Integrity assessments" have been carried out

▸ Fraud related issues raised in the EAAC are visible to OIO

▸ Procurement, Payroll and Mobile Device audits took a focused look at fraud risks

▸ Although two OIO team members are CISA qualified, OIO is dependent on one auditor for detailed IT controls and data analysis capacity. While that team member covers a wide range of technical skills, we would expect OIO to use appropriate external resources regularly to ensure that adequate assurance is obtained over detailed technical matters. This is particularly relevant with regards to the Quantum (Oracle ERP implementation) and the ISO 27000 (information security) initiatives.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
▸ Conforms.

Recommendations & Suggestions
▸ **OCI#1210.A3 (see 3.2, 3.3)** Consider the possibility of supplementing OIO's IT audit resource with additional external specialists, either through procuring standing agreements with suitable firms, or through resource-sharing with other UN institutions.

▸ See also **OCI#2230 (see 3.2).**

1220 - Due Professional Care

1000 Purpose Authority and Responsibility	**1100** Independence and Objectivity	**1200** Proficiency and Due Professional Care	**1300** Quality Assurance and Improvement Program

IPPF Mandatory Requirements

- **1220**. Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.
- **1220.A1** Internal auditors must exercise due professional care by considering the:
  - Extent of work needed to achieve the engagement's objectives.
  - Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
  - Adequacy and effectiveness of governance, risk management, and control processes. Probability of significant errors, fraud, or noncompliance.
  - Cost of assurance in relation to potential benefits.
- **1220.A2** In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.
- **1220.A3** Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

Demonstrated Accomplishments
Areas for further Conformance Action

- The Audit Manual provides clear guidance and is structured following the Standards. Sections 10 and 11 describe OIO's approach to its risk-based audit approach, and how the extent and nature of audit procedures are determined.
- Aspects of internal control and specific risks of fraud are considered in each audit, as corroborated by IFACI's review of files.
- While the selection of audits and scope is risk-driven, allocation of staff at the planning stage does not necessarily reflect differences in risk, complexity and other factors. Instead, it is a rough, standard allocation of person-days.

- Data analysis is specifically considered for each audit and embedded in the planning. Data analysis is a strength, as observed in the payroll and procurement audits.
- A detailed review of files shows evidence of advanced data analytics work, especially payroll and procurement files.
- Risk analysis is undertaken at the overall planning stage and in detail at the audit level. Both processes are collaborative and well documented.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
- Conforms

Recommendations & Suggestions
- **OCI#1220 (see 3.6)** Consider the benefits of tailoring budgeting by audit, so that resources are allocated and tracked on a risk-driven and cost-effective basis.

- **OCI#1220.A2 (see 3.4)** Data analytics are a strength. OIO could expand this in the context of Quantum and share skills with First and Second Lines.

1230 - Continuing Professional Development

1000 Purpose Authority and Responsibility	1100 Independence and Objectivity	1200 Proficiency and Due Professional Care	1300 Quality Assurance and Improvement Program

IPPF Mandatory Requirements	**Demonstrated Accomplishments** Areas for further Conformance Action	**Recommendations on** Gaps to Conformance and Opportunities for Continuous Improvement
▶ **1230**. Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.	▶ A training policy in place. ▶ Training is organised according to upcoming needs derived from the annual audit plan. The process is simple but appropriate given the size of the team. ▶ OIO has established Long-Term Agreements with McGill University Continuing Education and the Canadian Audit and Accountability Foundation to provide individual and team training as needs arise. Recent group courses have included communications and root cause analysis. ▶ Team members also participate in other in-person and online training (e.g. LinkedIn Learning), as indicated in the annual needs analysis. ▶ Those courses, and other general mandatory ICAO training, are covered by the Performance and Competency Evaluation (PACE) system. ▶ Staff members maintain a log of their Continuing Professional Education (CPE) hours which are recorded centrally within OIO.	**Conclusion** ▶ Conforms

1310 - REQUIREMENTS OF THE QAIP - 1311 - INTERNAL ASSESSMENTS
1312 - EXTERNAL ASSESSMENTS - 1320 - REPORTING ON THE QAIP
1321 - 1322 - DISCLOSURE OF CONFORMANCE AND NON-CONFORMANCE

The Institute of
Internal Auditors

1000
Purpose Authority
and Responsibility

1100
Independence and
Objectivity

1200
Proficiency and Due
Professional Care

1300
Quality Assurance
and Improvement
Program

IPPF Mandatory Requirements

- **1300**. The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

- **1310**. The quality assurance and improvement program must include both internal and external assessments.

- **1311**. Internal assessments must include:
  - Ongoing monitoring of the performance of the internal audit activity.
  - Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

- **1312**. External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The chief audit executive must discuss with the board:
  - The form and frequency of external assessment.
  - The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

- **1320**. The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

Demonstrated Accomplishments
Areas for further Conformance Action

- A comprehensive Quality Assurance and Improvement Program is in place, structured closely with the Standards and OIO's other policies, and with regular reporting to governing bodies.

- The Power BI KPI dashboard is an effective means of monitoring performance.

- Continual interaction with and monitoring by EAAC reinforces quality and action.

- Client satisfaction surveys are generally favourable (Annual Report) and consistently cite the quality of output as a strength. Corroborated by IFACI stakeholder interviews.

- An internal annual self-assessment was last performed in April 2024.

- OIO undertook external assessments in 11/2019 and 12/2024.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

- Conforms

Recommendations & Suggestions

- **OCI#1311 (see 3.6)** The self-assessment could be more objective and therefore insightful if performed by a peer external to the audit function, but nonetheless familiar with the Standards.

The Institute of Internal Auditors

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▸ **2000**. The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

▸ The internal audit activity is effectively managed when:

➥ It achieves the purpose and responsibility included in the internal audit charter.

➥ It conforms with the Standards.

➥ Its individual members conform with the Code of Ethics and the Standards.

➥ It considers trends and emerging issues that could impact the organization.

▸ The internal audit activity adds value to the organization and its stakeholders when

➥ it considers strategies, objectives, and risks;

➥ strives to offer ways to enhance governance, risk management, and control processes;

➥ and objectively provides relevant assurance.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ The Internal Audit Strategy, 2022-2025 (currently being updated for 2026-2028 triennium) outlines:

➥ Mid-range goals in line with the Charter, reflected in triennial and annual audit plans

➥ Reporting lines

➥ Key objectives for OIO

➥ Actions and guiding principles

▸ The revised strategy will also align OIO strategy with ICAO's overall strategic objectives.

▸ OIO is committed to its conformity with new IIA standards

➥ Strategy, Audit Manual and SOPs are currently being updated to reflect Standards

➥ Internal and external quality assessments

▸ Auditors attest to their conformance with the Standards, IIA and OIO codes of ethics on individual audits and annually.

▸ While respecting the necessity to maintain the objectivity and independence of its 3rd Line role, OIO could adopt a more pro-active role in the ERP project. This is especially relevant given that OIO team members have hands-on experience with Quantum from their work at UNDP and UN Women.

▸ Similarly, OIO could contribute considerably to the adoption of ERM at ICAO.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms

Recommendations & Suggestions

▸ **OCI#2000 (see 3.2)** While respecting its 3rd line role, OIO should consider how it could leverage its expertise and hands-on experience of its team members to provide foresight and solutions for risks in the ERP implementation project. Similarly, OIO should consider how it might make substantial contributions to the ERM initiative.

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

- ▶ **2010**. The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

  - ➥ To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes.

- ▶ The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

- ▶ **2010.A1** The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually.

- ▶ The input of senior management and the board must be considered in this process.

- ▶ **2010.A2** The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

Demonstrated Accomplishments
Areas for further Conformance Action

- ▶ There is a 3-year planning process in line with the ICAO triennial processes, but it is updated annually.

- ▶ The 3-year and annual audit plans are approved by Council and the EAAC.

- ▶ KPIs: 6 audits (at least one is IT), see 2010, and 3 evaluations per year. 5 audits were expected to be completed in 2024 with another 4 in the final stages.

- ▶ In addition, "Advisory reviews" are performed on an *ad hoc* basis for emerging issues. 2 were performed in 2024: accountability framework, Business Plan results framework; and ERP pre-rollout independent evaluation will be completed in 2025.

- ▶ The Power BI planning tool and OIO dashboard have been implemented

  - ➥ 71 topics identified in the audit universe (organizational functions, units, processes, bureaux, projects and others), adjusted periodically to reflect developments

- ▶ Topics are risk-rated per OIO Risk Assessment Methodology (updated October 2024)

  - ➥ Incorporates numerous relevant factors, including senior management input and ERM processes where available.

- ▶ Sharing the OIO Power BI dashboard with stakeholders could enhance transparency and understanding.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

- ▶ Conforms

Recommendations & Suggestions

- ▶ **OCI#2010 (see 3.6)** Consider sharing the OIO Power BI dashboard with stakeholders. See also **OCI#2500**.

- ▶ **OCI#2010.1 (see 3.5)** As ERM matures in the organisation, OIO's planning process could take management's risk management into account more. This interaction could not only enhance the quality of OIO's risk estimation, but also provide management with a critical, independent view of their risk management processes.

| **2000** Managing the Internal Audit Activity | **2100** Nature of Work | **2200** Engagement Planning | **2300** Performing the Engagement | **2400** Communicating Results | **2500** Monitoring Progress | **2600** Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2010**. The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

  ➥ To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes.

▶ The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

▶ **2010.A1** The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually.

▶ The input of senior management and the board must be considered in this process.

▶ **2010.A2** The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ The risk-based audit planning process identifies one IT audit topic per year which is aligned with audit priorities (IT asset management in 2023 – selected for IFACI file review). This is corroborated in discussions with CISO and CIO.

▶ Reviews for the given topic are informed by control objectives and other guidance from standards such as COBIT, ITIL, ISO 27000 and other technical IT audit guidance.

▶ Relevant IT risks are also systematically considered in the context of all other audits, as evidenced in our detailed file reviews.

▶ Use of the Power BI-based planning tool is well developed and enhances risk assessment and engagement.

▶ The planning process is collaborative (with intelligence/interaction from various management groups - ERM, ERP, TO, and annual workplan OIO retreats)

▶ As noted in 2110.A2, OIO does not currently map IT assurance to a recognised IT governance framework, such as COBIT.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
▶ Conforms

Recommendations & Suggestions
▶ See **GTC#2110.A2 (see 3.1)**

| **2000** Managing the Internal Audit Activity | **2100** Nature of Work | **2200** Engagement Planning | **2300** Performing the Engagement | **2400** Communicating Results | **2500** Monitoring Progress | **2600** Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2020**. The chief audit executive must communicate the internal audit activity's plans and resource requirements,

   ➡ including significant interim changes, to senior management and the board for review and approval.

▶ The chief audit executive must also communicate the impact of resource limitations.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ Section 11 of the Annual Report contains a discussion of resources.

▶ Recent interaction with the Council and EAAC has highlighted OIO's limited capacity to provide further advisory services.

▶ Possible resource implications of the in-sourcing of investigations currently outsourced to OIOS are currently being discussed with SG, EAAC.

▶ The small team size is an inherent limitation to capacity and increases risk of dependency on individuals.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

Recommendations & Suggestions

▶ **OCI#2020 (see 3.3)** Small team size inherently increases risk of dependency on individuals.

2000 Managing the Internal Audit Activity

2100 Nature of Work

2200 Engagement Planning

2300 Performing the Engagement

2400 Communicating Results

2500 Monitoring Progress

2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ **2030**. The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

➥ Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan.

➥ Sufficient refers to the quantity of resources needed to accomplish the plan.

➥ Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ The OIO Chief discusses resourcing with the Council and the EAAC regularly and reports formally via the Annual Report (see section 11 of the 2023 report).

▶ The team, despite its small absolute size, possesses a wide range of qualifications and experience that cover much of the audit universe (OIO has mapped team competencies to the audit plan). Inevitably, there are areas that require external specialist resources, under OIO's supervision. A specialist was hired to collaborate on the 2023 ERM audit, for example. Looking forward, it is foreseen that specialists will be required to assist in other areas such as:

➥ IT audit (ISO 27000 initiative, Quantum)

➥ Detailed technical operations

➥ Local health insurance arrangements

➥ Possible investigations work (if OIO assumes this role)

▶ The budget only covers staff costs, necessitating *ad hoc* approval of the SG for any additional investments, including for training, co-sourcing and other regularly occurring and exceptional items. Although the process rarely results in a refusal of resources, it can cause delays and therefore slows OIO's adaptability.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

Recommendations & Suggestions

▶ **OCI#2030 (see 3.2, 3.3)** For regularly occurring non-staff expenditures, such as training, co-sourcing and small discretionary items, OIO should explore establishing an overall pre-approved budget to manage autonomously.

2040 - Policies and Procedures

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ **2040**. The chief audit executive must establish policies and procedures to guide the internal audit activity.

➡ The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ The Charter for OIO (2020) was approved by the Council.

▶ OIO has an Audit Manual in place (2021) which is currently being revised to better reflect the 2024 IIA Standards. The Manual addresses these key points:

➡ Positioning of IA function

➡ Independence

➡ Audit process

➡ Quality control and assurance

➡ Communication and coordination

▶ In addition, Standard Operating Procedures and other policies provide guidance on specific topics (as noted elsewhere in our detailed observations), including the Communication Plan, Report Clearance and others).

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms.

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ **2050**. The chief audit executive should

➥ share information,

➥ coordinate activities,

➥ and consider relying upon the work of other internal and external assurance and consulting service providers

- to ensure proper coverage and minimize duplication of efforts.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ Per the OIO Communication Plan, OIO shares information formally and informally through regular meetings with stakeholders (external audit, Council, the SG, senior management committees).

▶ The collaborate planning approach ensures that stakeholder needs are taken into account on a macro level and within the context of individual audits.

▶ OIO carefully considers the planned work of external audit, the JIU, EAAC and other assurance activity to avoid duplication and audit fatigue.

▶ As noted in 2500, OIO administers all management recommendations from OIO, JIU, external audit, and EAAC centrally.

▶ External audit does not place reliance on OIO's work, although there may be potential to do so and thereby further reduce duplication.

▶ Management is currently revisiting the investigation services provided by the UN Office of Internal Oversight Services. One solution involves OIO taking over that function. However, OIO does not currently have the capacity to deliver that service.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms.

Recommendations & Suggestions

▶ **OCI#2050 (see 3.2)** OIO should engage with the external audit team to explore how external audit may be able to rely on the work of internal audit, where possible, in accordance with *International Standard on Auditing 610* and other relevant guidance / constraints. This may be particularly relevant in the context of the Quantum ERP implementation and ongoing controls assurance.

▶ See **OCI#2230 (3.3)**.

▶ **OCI#2250.1 (see 3.3)** In the context of possible in-sourcing of investigation services, OIO should consider a model whereby investigations may be overseen by OIO, but the bulk of the work is outsourced to professional services firms with the scale, expertise and reach to cost-effectively deliver such projects.

2000 Managing the Internal Audit Activity

2100 Nature of Work

2200 Engagement Planning

2300 Performing the Engagement

2400 Communicating Results

2500 Monitoring Progress

2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

- **2060**. The chief audit executive must report periodically to senior management and the board on

  - the internal audit activity's purpose, authority, responsibility, and performance relative to its plan

  - and on its conformance with the Code of Ethics and the Standards.

- Reporting must also include

  - significant risk and control issues, including fraud risks,

  - governance issues,

  - and other matters that require the attention of senior management and/or the board.

- The frequency and content of reporting are determined collaboratively by the chief audit executive, senior management, and the board.

  - The frequency and content of reporting depends on

    - the importance of the information to be communicated

    - and the urgency of the related actions to be taken by senior management and/or the board.

Demonstrated Accomplishments
Areas for further Conformance Action

- Annual reports are well written, substantial in commentary, well received by stakeholders (corroborated by stakeholder interviews), and delivered formally to the Council:

  - refer to IIA Standards
  - Overview of OIO activity for the year, summary of each audit and evaluation project
  - Commentary on key risks to the organisation
  - Information on resources and performance
  - Cooperation with oversight bodies

- Regular meetings are held with SG, President, bureau heads, various management committees (ERM, Quantum, ICT, ERM reference, IMC, PMO etc.), as defined by OIO's Communication Plan. The management recommendation status is reported regularly (see 2500).

- OIO's work program is reviewed by EAAC and approved by the Council.

- In 2024, 3 audits were completed with reports issued, and a further 4 audits were in the final stages of delivery. OIO has a target performance indicator of 6 audits per year. In addition, OIO completed one advisory paper (Implementation of the Accountability Framework).

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

- Conforms

The Institute of Internal Auditors

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ **2110**. The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

➥ Making strategic and operational decisions.

➥ Overseeing risk management and control.

➥ Promoting appropriate ethics and values within the organization.

➥ Ensuring effective organizational performance management and accountability.

➥ Communicating risk and control information to appropriate areas of the organization.

➥ Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ See 2120, 2130 below.

▶ The ethics framework was audited in 2022

▶ OIO was represented on the Interoffice Advisory Group.

▶ OIO performed an informal review of the proposed Accountability Framework at the request of the SG.

▶ Ethical considerations were part of the Statement of Internal Control, Management Assurance Declaration and other audits.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

The Institute of Internal Auditors

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2110.A1** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

▶ **2120.A2** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ The ethics framework was audited in 2022

▶ ICAO is currently considering in-sourcing investigation work currently outsourced to UN OIOS. It is possible that OIO will be asked to be involved in investigations in that scenario.

▶ There are ethics and fraud considerations in current Procurement, Payroll, Statement of Internal Control audits.

▶ An AFAC (Anti-fraud, Anti-corruption) audit is planned for 2025.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms.

Recommendations & Suggestions

▶ **OCI#2110 (see 3.3)** If investigations are in-sourced, and OIO is involved, additional specialist resources will be required, either in-house or a combination of in-house and outsourcing to a specialist firm.

The Institute of Internal Auditors

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

- **2110.A2** The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

Demonstrated Accomplishments
Areas for further Conformance Action

- IT governance was last audited holistically in 2018. Much has changed since then. The ISO 27000 program will change/enhance IT governance radically.
- OIO is closely involved with the ISO 27000 project and will undertake periodic review of the ongoing compliance for certification.
- OIO conducts one major IT audit per year based on a risk assessment in consultation with senior management (2024 project was asset management).

- OIO sits on the Information Management Committee and thereby keeps abreast of IT developments and risk.
- While the risk-based topic selection process is valid, it is also good practice to consider a recognised IT governance framework, such as COBIT, to demonstrate and ensure coverage of key areas of IT risk.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

- Partially conforms

Recommendations & Suggestions

- **GTC#2110.A2 (see 3.1)** We would encourage OIO's adoption of a recognised IT governance framework, currently planned for the coming year. This initiative should be coordinated with the ISO 27000 certification project and leverage the Information Management Service's governance initiatives.
- The OIO IT governance component should be incorporated into OIO's broader risk-assurance mapping exercise.
- IT audit planning decisions should be made, in part, with reference to the adopted framework, with a view to gaining assurance coverage across the range of domains on a multi-year rotational basis.

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ **2120**. The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

▶ Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- ➡ Organizational objectives support and align with the organization's mission.

- ➡ Significant risks are identified and assessed.

- ➡ Appropriate risk responses are selected that align risks with the organization's risk appetite.

- ➡ Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

▶ The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

▶ Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ See 2130 below.

▶ As noted, OIO's 2023 review of ERM concluded that ICAO was at the early stages of maturity on the Reference Maturity Model of the High-level Committee on Management and only "partially met" ERM benchmarks set out by the JIU. While further progress has been made, it is widely recognised that ERM is not as embedded or as mature as senior management expects (as corroborated by stakeholder interviews).

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Partially conforms

Recommendations & Suggestions

▶ **OC#2120 (see 3.5)** OIO should consider what role it can play in fostering the maturity of ERM and internal controls within the organisation, bearing in mind the need to maintain its independent, "third line" perspective.

▶ **See 2110.A2 (see 3.1)**

The Institute of Internal Auditors

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2120**.A1 The internal audit activity must evaluate risk exposures relating to the organisation's governance, operations, and information systems regarding the:

➡ Achievement of the organisation's strategic objectives,

➡ Reliability and integrity of financial and operational information.

➡ Effectiveness and efficiency of operations and programs.

➡ Safeguarding of assets; and

➡ Compliance with laws, regulations, policies procedures and contracts.

▶ **2120.C1** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

▶ **2120.C2** Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organisation's risk management processes.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ See 2130 below.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Partially conforms

Recommendation

▶ **See 2110.A2 (see 3.1)**

2000 Managing the Internal Audit Activity

2100 Nature of Work

2200 Engagement Planning

2300 Performing the Engagement

2400 Communicating Results

2500 Monitoring Progress

2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▸ **2130**. The internal audit activity must assist the organisation in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

▸ **2130.A1** The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organisation's governance, operations, and information systems regarding the:

➥ Achievement of the organisation's strategic objectives,

➥ Reliability and integrity of financial and operational information;

➥ Effectiveness and efficiency of operations;

➥ Safeguarding of assets; and

➥ Compliance with laws, regulations, and contracts.

▸ **2130.C1** Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organisation's control processes.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Each audit contains an assessment of internal controls as part of the risk assessment, as corroborated by IFACI file reviews.

▸ The Annual Report notes key organizational risks and commentary on control effectiveness.

▸ OIO undertook an overall review of ICAO's Enterprise Risk Management program in 2023 and the Statement of Internal Control in 2024 and continues to follow up resultant management recommendations.

▸ OIO plans to develop a holistic "assurance map", reflecting the organisation's risk universe, and different sources of assurance (e.g. OIO, External Audit, self-assessment) during 2025.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms

Conclusion

▸ Partially conforms

Recommendations & Suggestions

▸ **GC#2130.A1 (see 3.1)** Partially conforms (see 2110.A2)

▸ **OCI#2130.A1 (see 3.2)** We would encourage the development of the assurance map, to include risks associated with Quantum and other TO projects, and that OIO include input from a range of risk, internal control and assurance stakeholders in that process.

2000 Managing the Internal Audit Activity	**2100** Nature of Work	**2200** Engagement Planning	**2300** Performing the Engagement	**2400** Communicating Results	**2500** Monitoring Progress	**2600** Resolution of Risks Acceptance

IPPF Mandatory Requirements

- **2200.** Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

  - ➥ *The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.*

- **2201.** In planning the engagement, internal auditors must consider:

  - ➥ The *strategies* and objectives of the activity being reviewed and the means by which the activity controls its performance.

  - ➥ The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.

  - ➥ The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.

  - ➥ The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

Demonstrated Accomplishments
Areas for further Conformance Action

As evidenced by our file reviews,

- Audit plans set out objective, scope, timing and resource considerations.

- Audits consider and document inherent risks, expected internal controls and assessments of the design and operating effectiveness of controls.

- Audits routinely identify significant opportunities for improvements to control processes.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

- Conforms

2210 – Engagement Objectives

2000 Managing the Internal Audit Activity	**2100** Nature of Work	**2200** Engagement Planning	**2300** Performing the Engagement	**2400** Communicating Results	**2500** Monitoring Progress	**2600** Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ **2210.** Objectives must be established for each engagement.

➥ **2210.A1** Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review.

➥ Engagement objectives must reflect the results of this assessment.

▶ **2210.A2** Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

▶ **2210.A3** Adequate criteria are needed to evaluate governance, risk management, and controls.

▶ Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished.

➥ If adequate, internal auditors must use such criteria in their evaluation.

➥ If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ Audit planning and communications clearly establish audit objectives.

▶ During the engagement planning phase, matrices are prepared to document inherent risks, expected internal controls and weaknesses, and expected residual risk. That analysis drives decisions in the nature and extent of audit evidence sought in the engagement. The analysis is updated to compare actual with expected results upon completion of the audit.

▶ Audit files show evidence of continual interaction with auditee management during the planning phase, which facilitates understanding and incorporating management expectations into audits.

▶ At the general level, OIO's regular meetings with the Council, EAAC, senior management and management committees ensures that broader management objectives and expectations are reflected in the audit plan and within engagements.

▶ Planning in audit files demonstrate consideration of fraud risk.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

2000 Managing the Internal Audit Activity	**2100** Nature of Work	**2200** Engagement Planning	**2300** Performing the Engagement	**2400** Communicating Results	**2500** Monitoring Progress	**2600** Resolution of Risks Acceptance

IPPF Mandatory Requirements

▶ The established scope must be sufficient to achieve the objectives of the engagement.

▶ **2220.A1** The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

▶ **2220.C1** In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

▶ **2220.C2** During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ Audit files reviewed consistently demonstrated sufficient scope in support of the objectives and conclusions of the audits.

▶ Engagement planning processes, observed during audit file review, include appropriate consideration of processes, IT systems, staff, internal controls, and inherent and residual risk analysis.

▶ OIO does not perform consulting engagements but is, nonetheless, called upon to do so.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

| **2000**
Managing the Internal Audit Activity | **2100**
Nature of Work | **2200**
Engagement Planning | **2300**
Performing the Engagement | **2400**
Communicating Results | **2500**
Monitoring Progress | **2600**
Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2230.** Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

▶ **2240.** Internal auditors must develop and document work programs that achieve the engagement objectives.

▶ **2240.A1** Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement.

▶ The work program must be approved prior to its implementation, and any adjustments approved promptly.

▶ **2240.C1** Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ Appropriate resourcing is considered during the overall annual audit planning processes, and for individual audits. The small team and its breadth of experience and qualifications make these processes straightforward.

▶ Work programs are developed that align with engagement objectives. Files reviewed by IFACI showed evidence of CAE involvement and approval of work programs.

▶ Given the small team size, OIO uses external specialised resources where the nature of the audit indicates (e.g. the ERM audit was executed with an external consultant). Budgetary and procurement procedure constraints can inhibit timely provision of appropriate resources.

▶ Use of external resources has also introduced challenges of quality and supervision, as evidenced by the ERM file, particularly because an individual, rather than a firm, was engaged.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

Recommendations & Suggestions

▶ **OCI#2230 (see 3.3)** OIO should explore options to improve supervision and delivery of external consultants. One option may be to hire firms with multiple consultants capable of delivering the assignment, thereby reducing the reliance on individuals.

2300 – Performing the engagement

2000
Managing the Internal Audit Activity

2100
Nature of Work

2200
Engagement Planning

2300
Performing the Engagement

2400
Communicating Results

2500
Monitoring Progress

2600
Resolution of Risks Acceptance

IPPF Mandatory Requirements

▸ **2300.** Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

▸ **2310.** Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Audit working papers describing tests are structured in a consistent and coherent manner, clearly stating the audit objective, risk tested, audit procedure, work done, conclusion and draft recommendation.

▸ The information is consistent and relevant with the objectives for the engagement workpapers. Workpapers document the link between risks, controls, the testing approach, summary of interview, results, evidence and conclusions.

▸ Relevant information supports engagement observations and recommendations.

▸ Cross referencing and evidence of workflow/supervision would be facilitated through the use of an audit tool.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms.

Recommendations & Suggestions

▸ **OCI#2300 (see 3.5)** If, as is planned, OIO chooses to adopt an audit documentation tool, careful consideration should be given to how such a tool may facilitate more effective cross referencing, workflow/supervision, and evidence thereof in the files.

2320 - Analysis and Evaluation

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▸ **2320.** Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Sufficient and appropriate evidence is obtained so that a prudent, informed person would reach the same conclusions as the auditor who conducted the engagement.

▸ Audit reports clearly present an executive summary, the results of the audit carried out, objectives and scope, and findings and recommendations.

▸ Audit files reviewed by IFACI demonstrate audit trails (although cross referencing is weaker than in a dedicated tool) and follow a logical structure supporting conclusions.

▸ The Internal Auditor acknowledges satisfactory performance in the communications and provides an opinion on the control environment. It is also indicated that collaborations were obtained during the audit.

▸ Root causes are routinely analyzed to arrive at meaningful and effective recommendations.

▸ A good balance of collaboration/professional skepticism yields fair audit results that generally foster constructive management engagement.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms

2330 - Documenting Information

| **2000** Managing the Internal Audit Activity | **2100** Nature of Work | **2200** Engagement Planning | **2300** Performing the Engagement | **2400** Communicating Results | **2500** Monitoring Progress | **2600** Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2330.** Internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

▶ **2330.A1** The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

▶ **2330.A2** The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organisation's guidelines and any pertinent regulatory or other requirements.

▶ **2330.C1** The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organisation's guidelines and any pertinent regulatory or other requirements.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ Evidence on files reviewed by IFACI is sufficient, reliable and extensive enough to support the audit results, conclusions and recommendations.

▶ Access to audit engagement records is limited to audit staff via ICAO information security.

▶ There are plans to adopt an audit tool which is likely to be cloud-based, introducing new risks in audit data access.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

Recommendations & Suggestions

▶ **OCI#2330 (see 3.5)** In an eventual adoption of an audit tool, OIO should undertake a thorough review of relevant information security risks, particularly related to a cloud-based solution. Those risks may be augmented and made more complex if the solution contains self-service auditee / management functionality such as recommendation management or GRC functionality.

The Institute of **Internal Auditors**

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▸ **2340.** Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

▸ The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement.

▸ The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review.

▸ Appropriate evidence of supervision is documented and retained.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ The CAE reviews all audit reports, key communications (planning, notification letter, draft reports, final report).

▸ There was evidence of supervision in audit files reviewed by IFACI.

▸ The small team size inherently facilitates close supervision by the CAE. The CAE is often involved in audit execution and first level review.

▸ The CAE is involved in oversight and approval of recommendations in the Symbiant system and related reporting mechanisms (see 2500)

▸ Audits include a person-day budget and analysis while stopping short of a potentially burdensome time reporting system.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms

The Institute of Internal Auditors

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▸ **2410.** Communications must include the engagement's objectives, scope, and results.

▸ **2410.A1** Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans.

▸ Where appropriate, the internal auditors' opinion should be provided.

▸ An opinion must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

▸ **2410.A2** Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Audit reports, the Annual Report and other communications to stakeholders include objectives, scope and results clearly, either in detail or summary form.

▸ Audit reports contain overall conclusions and conclusions by objective, recommendations and action plans agreed by management.

▸ Audit reports contain a conclusion by objective, but also an overall rating (see 2450).

▸ The collaborative working style of OIO ensures that multiple stakeholder expectations are taken into consideration in the planning and reporting phases.

▸ The rating scheme and report content facilitates auditors' acknowledgement of satisfactory performance.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms

2420 – Quality of Communications

2000 Managing the Internal Audit Activity

2100 Nature of Work

2200 Engagement Planning

2300 Performing the Engagement

2400 Communicating Results

2500 Monitoring Progress

2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▸ **2420.** Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

➥ Accurate communications are free from errors and distortions and are faithful to the underlying facts.

➥ Objective communications are fair, impartial, and unbiased and are the result of a fair- minded and balanced assessment of all relevant facts and circumstances.

➥ Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.

➥ Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness.

➥ Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed.

➥ Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions.

➥ Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Audit reports are well structured, succinctly presented in "traditional" narrative format, in line with house style.

▸ Effectively written executive summaries facilitate understanding.

▸ Stakeholders and auditees cite balance and fairness of the reporting process, usefulness and pragmatism of most recommendations.

▸ With some justifiable exceptions, usually related to the complexity and volume of findings, report drafting and finalisation delays are reasonable, while allowing adequate feedback and consultation.

▸ Audit reports are succinctly summarised in the OIO Annual Report, presented and discussed with EAAC, the Council, the SG and relevant Senior Management.

▸ Exceptionally, urgent matters can be reported to Senior Management and governing bodies outside of audit reports via "Advisory Reviews", defined in sections 10 and 15 of the Audit Manual. Two such papers were issued in 2024.

▸ Audit reports are generally published (after redaction, if necessary – see 2440). They are distributed to SG, the Council, External Auditors, EEAC. Audit reports are summarised in the Annual Report.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms

Recommendations & Suggestions

▸ **OCI#2420 (see 3.4)** Consider further exploration of presentation-styles and online or even interactive report formats, such as the current Power BI dashboards developed by OIO.

The Institute of Internal Auditors

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2421.** If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

▶ **2430.** Indicating that engagements are "conducted in conformance with the International Standards for the Professional Practice of Internal Auditing" is appropriate only if supported by the results of the quality assurance and improvement program.

▶ **2431.** When nonconformance with the Code of Ethics or the Standards impacts a specific engagement, communication of the results must disclose the:

➥ Principle(s) or rule(s) of conduct of the Code of Ethics or the Standard(s) with which full conformance was not achieved.

➥ Reason(s) for nonconformance.

➥ Impact of nonconformance on the engagement and the communicated engagement results.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ None noted. Iterative and highly collaborative audit report finalisation process defined by SOP for Audit and Evaluation Report Clearance reduces risk of such errors or omissions.

▶ Conformance is noted in the Annual Report and in individual audit reports and is appropriate.

▶ None noted.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
▶ Conforms

2440 – Disseminating Results

IPPF Mandatory Requirements

▸ **2440.** The chief audit executive must communicate results to the appropriate parties.

▸ The chief audit executive is responsible for reviewing and approving the final engagement communication before issuance and for deciding to whom and how it will be disseminated.

▸ When the chief audit executive delegates these duties, he or she retains overall responsibility.

▸ **2440.A1** The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

▸ **2440.A2** If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

  ➥ Assess the potential risk to the organization.

  ➥ Consult with senior management and/or legal counsel as appropriate.

  ➥ Control dissemination by restricting the use of the results.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Audit reports are distributed according to the OIO Communication Plan (2021). Reports are distributed to auditee management, the OSG, EAAC, the President, the Council, and External Audit, and are generally published thereafter (see below).

▸ OIO's SOP for Audit and Evaluation Report Clearance defines the process and target deadlines for agreeing and approving final results with auditee management and the OSG.

▸ Audit reports are generally published, unless they contain sensitive information, as described in OIO's Policy on Public Disclosure of Reports and SOP for Disclosure of Internal Audit and Evaluation Reports (such as a recent cyber security report). In such cases, the report may be withheld in its entirety or in part.

▸ The SG is currently required to "endorse" management action plans prior to finalisation of audit reports. This can often cause some delay in report issuance due to OSG workload.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▸ Conforms.

Recommendations & Suggestions

▸ **OCI#2440 (see 3.6)** Consider changing the necessity for the SG to endorse all management action plans to streamline the process. One possibility might be to require the SG's involvement where there is disagreement, its overall rating is low, or the subject of the audit is particularly sensitive or wide-reaching.

The Institute of Internal Auditors

| 2000 Managing the Internal Audit Activity | 2100 Nature of Work | 2200 Engagement Planning | 2300 Performing the Engagement | 2400 Communicating Results | 2500 Monitoring Progress | 2600 Resolution of Risks Acceptance |

IPPF Mandatory Requirements

▶ **2450**. When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders.

▶ The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

▶ The communication will include:

　➥ The scope, including the time period to which the opinion pertains.

　➥ Scope limitations.

　➥ Consideration of all related projects, including the reliance on other assurance providers.

　➥ A summary of the information that supports the opinion.

　➥ The risk or control framework or other criteria used as a basis for the overall opinion.

　➥ The overall opinion, judgment, or conclusion reached.

Demonstrated Accomplishments
Areas for further Conformance Action

▶ OIO does not provide an overall opinion that draws from multiple engagements, as contemplated in the IIA's *Implementation Guide 2450*.

▶ However, the 2023 Annual Report does offer thematic summaries (see sections 5 and 6.9).

▶ Individual audit conclusions are summarised in one of four categories: Effective, Some Improvement Needed, Major Improvement Needed, Unsatisfactory, as defined by convention and in the standard appendix to each report.

▶ The report ratings are not formalised in the Audit Manual.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion

▶ Conforms

Recommendations & Suggestions

▶ **OCI#2450** OIO should consider including the report rating and associated guidance in the Audit Manual currently under revision.

▶ **OCI#2450.1** As OIO moves towards adoption of an overall assurance map, OIO should consider the implications of and guidance for Standard 11.3 of the 2024 *Global Internal Standards*, relating to "Themes" and "Conclusions at the level of the business unit or organization". In doing so, OIO should consider the assurance needs and requests of the Council, EAAC and Senior Management, balanced with OIO's capacity to deliver such conclusions.

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▸ **2500**. The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

▸ **2500.A1** The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ Management recommendations derived from audit reports are approved by the auditee.
▸ Management recommendations are managed in cloud-based Symbiant software which manages auditor and auditee workflow.
▸ Updates/auditee workflow are typically managed by "focal points"
▸ 71.5% of recommendations from the last 5 years have been implemented.
▸ OIO, JIU, EA, EEAC recommendations are all administered by OIO – a practice valued by EA
▸ For OIO points, recommendations are only entered on Symbiant after the final report is issued (to avoid immature points)
▸ For OIO, the auditor first considers the auditee resolution of point, which is then approved by Chief. For others, they are updated/resolved by JIU, EEAC or EA periodically
▸ Recommendations are reviewed quarterly for progress updates. Status is reported regularly to governing bodies
▸ Recommendations are only closed on CAE's approval
▸ PowerBI dashboard is used to monitor progress by category, auditee, source of recommendation

▸ Access to OIO Power BI dashboard is accessed by OIO staff only

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
▸ Conforms

Recommendations & Suggestions
▸ **OCI#2500 (see 3.6)** Access to OIO's Power BI dashboard should be granted and encouraged amongst broader stakeholders to foster transparency and implementation of agreed action plans.
▸ **See OCI#2010 (see 3.6)**
▸ **OCI#2500.1 (see 3.5)** OIO is considering replacing Symbiant with an audit tool with management recommendation functionality.

2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicating Results	2500 Monitoring Progress	2600 Resolution of Risks Acceptance

IPPF Mandatory Requirements

▸ **2600**. When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management.

▸ If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Demonstrated Accomplishments
Areas for further Conformance Action

▸ The Annual Report contains a summary of key risks facing the organization. The OIO Chief presents and discusses these as part of regular meetings with the Council, EAAC and senior management.

▸ Where management choses to "accept" a risk that OIO considers unacceptable for the organization, the Audit Manual describes the process whereby the SG is required to endorse such acceptance. OIO also reports such matters in its Annual Report (Audit Manual, section 13. No such matters have arisen during the last 5 years.

Recommendations on
Gaps to Conformance and Opportunities for Continuous Improvement

Conclusion
▸ Conforms

Objectives of the EQA

- This External Quality Assessment was carried out by IFACI-Certification, part of the *Institut français de l'audit et du contrôle internes* (IFACI), the Intitute of Internal Auditors (IIA) in France. The EQA team comprised independent experienced audit practitioners and quality assurance professionals David Pike and Michel Millette, under the supervision of IFACI-Certification Director, Benoît Harel.

- The principal objectives of the EQA were to (1) assess the Internal Audit activity (IA) of the Office of Internal Oversight's (OIO) conformance with the Institute of Internal Auditors' *Standards* and *Code of Ethics*; (2) assess the effectiveness in providing assurance and consulting services to ICAO and other interested parties; and (3) identify opportunities, offer recommendations for improvement, and provide counsel to OIO to improve its IA performance and services and promote its image and credibility.

- The IIA team would like to thank OIO staff for their contributions to this initiative, and OIO's stakeholders for their valuable insights and evident commitment and support.

Scope of the EQA

- The scope of the EQA addressed internal audit activities described in the 2020 Charter for OIO, approved by ICAO Council. The Charter defines the authority and responsibility of Internal Audit function.

Methodology of the EQA

- To accomplish the EQA objectives, the IIA team reviewed documentation submitted by OIO at the EQA team's request; conducted interviews with 11 OIO key stakeholders including the Secretary General and President of the Council, (see Section 4 – Stakeholder Feedback); reviewed a sample of audit projects and associated work papers (see page 61); and prepared and executed eight Thematic Workshops (see page 62) with OIO team members, consistent with IIA's established methodology for EQAs.

Reporting Period

- The on-site portion of the EQA took place at ICAO headquarters in Montreal 7-8 November 2024 and 2-6 December 2024, supplemented with online sessions.

- The reporting period covered the years 2023 and 2024 up to the date of our fieldwork, and was based on information made available until 6 December 2024, when field work was substantially completed.

Opinion as to Conformance with the Standards and the IIA Code of Ethics

- The conclusion of the IIA Quality Assessment Team is that the internal audit activity of ICAO OIO generally conforms with:
  - ➥ the Institute of Internal Auditors' *Core Principles for the Professional Practice of Internal Auditing*
  - ➥ the Definition of Internal Auditing
  - ➥ the *International Standards for the Professional Practice of Internal Auditing*
  - ➥ the Institute of Internal Auditors' *Code of Ethics*

- A detailed list of conformance to individual *Standards* and the IIA *Code of Ethics* is shown in Sections 2 and 5 of this report.

The Institute of Internal Auditors

- The "generally conforms" opinion means that the IIA Assessment Team has concluded the following
  - ➥ For Individual Standards, the Internal Audit activity conforms to the requirements of the Standard or elements of the IIA Code of Ethics (both Principles and Rules of Conduct) in all material respects.
  - ➥ For the General Standards, the Internal Audit activity achieves general conformity with a majority of the individual Standards and/or elements of the IIA Code of Ethics, and at least partial conformity to others, within the General Standard.
  - ➥ For the Internal Audit activity overall, there may be opportunities for improvement, but these should not represent situations where the internal audit activity has not implemented the Standards, the IIA Code of Ethics, has not applied them effectively, or has not achieved their stated objectives.

Audit Engagements Selected for Review

- For our detailed audit engagement review, we selected 5 engagements, covering a range of topics, timings and ratings, as illustrated in the following table.

Audit Title	Reference	Year	Date of Report	OIO Rating
Payroll Management	IA/2023/2	2023	25/05/23	Effective
Enterprise Risk Management (ERM)	IA/2023/4	2023	12/12/23	Some Improvement Needed
IT Asset Management	IA/2024/1	2024	5/05/24	Major Improvement Needed
Statement of Internal Controls	IA/2024/2	2024	31/05/24	Effective
Procurement	IA/2024/4	2024	not finalised at time of fieldwork	-

10 Core Principles for the Professional Practice of Internal Auditing

Updated as of 1st January 2017

	Attribute Standards				Performance Standards							IIA Code of Ethics
General Standards	1000 Purpose, Authority, and Responsibility	1100 Independence and Objectivity	1200 Proficiency and Due Professional Care	1300 Quality Assurance Improvement Program	2000 Managing the Internal Audit Activity	2100 Nature of Work	2200 Engagement Planning	2300 Performing the Engagement	2400 Communicat° of Results	2500 Monitoring Progress	2600 Communicat° Acceptance of Risks	

Standards Categories

General Standards

Individual Standards

1 Documentary Review	■	■	■	■	■	■	■	■	■	■	■	■
2 **Workshop #1** - Methodology Supervision Quality												
2 **Workshop #2** - Building, Approval and Monitoring of the Audit Plans												
2 **Workshop #3** - Monitoring of Corrective Actions												
2 **Workshop #4** - Mission, Positioning and Monitoring of Internal Audit												
2 **Workshop #5** – GRC Processes Assessment and Interaction with other assurance providers												
2 **Workshop #6** - Ethics, Compliance, and Antifraud Management												
2 **Workshop #7** - Auditing in IT Environment												
2 **Workshop #8** - Management of Human Resources												
3 Stakeholder Sessions												
4 File Walkthroughs												
5 Brainstorm and Benchmark												

Overall Evaluation of Conformance with the IIA IPPF & Overall opinion on the Internal Audit activity's compliance with the IAC Audit Manual

- **CAE :** Chief Audit Executive / Chief, OIO
- **COBIT:** Control Objectives for Information Technologies, published by the Information Systems Audit and Control Association (ISACA)
- **COSO:** Committee of the Sponsoring Organizations of the Treadway Commission's standard for Enterprise Risk Management and internal control.
- **CPE :** Continuous Professional Education
- **EAAC:** Evaluation and Audit Advisory Committee
- **EQA:** External Quality Assessment (of internal audit)
- **ERM :** Enterprise Risk Management
- **ERP:** Enterprise Resource Planning project with TO to adopt the cloud-based Oracle solution under Quantum
- **GRC:** Governance, risk and compliance
- **IAD:** Internal Audit
- **ICAO:** International Civil Aviation Organization
- **IFACI / IFACI-Certification / IIA**: *Institut français de l'audit et du contrôle internes* (the IIA in France) who performed this EQA / the Institute of Internal Auditors
- **IPPF**: International Professional Practices Framework of The IIA
- **OIO:** ICAO Office of Internal Oversight
- **ISO/ 27000:** Standard for information security, International Organization for Standardization
- **IT/ICT:** Information Technology / Information and Communications Technology
- **ITIL:** Information Technology Infrastructure Library
- **PowerBI:** a suite of business analytics tool from Microsoft, designed to help organizations connect a wide range of data sources.
- **QAIP:** Quality Assurance & Improvement Program (of internal audit)
- **Quantum:** A consortium led by United Nations Development Programme (UNDP) to provide an Oracle cloud-based ERP solution.
- **SG:** Secretary General
- **Standards:** International Standards for the Professional Practice of Internal Auditing (2017) issued by the Institute of Internal Auditors
- **TO:** Transformational Objective program, a strategic, multi-faceted initiative designed to transform ICAO's Secretariat to enable ICAO to deliver an enhanced service to Member States.
- **Three Lines Model:** a widely adopted framework for organizational governance, risk management, and internal control, developed by the IIA and COSO.
- **UNDP:** United Nations Development Programme
- **UN OIOS:** the oversight function (internal audit and investigations) of the United Nations Secretariat.

IFACI
Certification