CORTE DEI CONTI

External Auditor Report

Presentation to Financial Advisory Committee

6 June 2024

CORTE DEI CONTI

The report: focus on structure

Audit report on FS 2023

The report 2024 is presented in two parts, the first part contains our "Opinion" on the FS 2023, the second part contains the long-form report.

The long-form report has been divided into three sections (A,B,C) to facilitate the communication of the audit findings. A dedicated section (C) contains the outcomes of the IT audit and Cybersecurity.

The follow-up to previous recommendations – Annexes

Annex I contains the follow-up to the recommendations issued in previous financial audit reports.

Annex II contains the follow-up to the recommendations and suggestions issued in 2023 Cyber-security audit .

Annex III contains the follow-up to the recommendations issued by the SFAO.

Presentation of the report

Audit report on FS 2023

Including the IT audits, we have issued 19 recommendations and 3 suggestion.

In addition to the audit activity on FS 2023, we have also carried out the follow-up to the previous recommendations and the assessment. In accordance with non- surprise approach, all findings of our audit activities were discussed with Management, not only during the audit, but also through the due cross-examination.

The WMO's comments to our recommendations, approved by the Secretary-General, are included in the report.

1. The findings

Section A.

Assets register and management

On this subject, we recommended that Management ensure that the new ERP is compatible with the current system of acquisition and updating of the asset register. We also issued two suggestions on the assets management.

Employee Benefits and Personnel

We examined the aspect of liabilities by “benefits related to the ASHI, leaves and grants”, how they are influenced by actuarial assumptions. We issued one recommendation, that the actuarial assumptions be made more adherent to inflation rate and to the data owned by WMO.

Regarding the hiring of consultants, we recommended that the organisation should link the financial strategies with a preventive evaluation of the needs of skills and work forces.

Section B.

The three lines of defence

We examined the three lines of defence mechanism. Our recommendation was that organization should make a comprehensive revision of the accountability and internal control framework, setting clear roles and responsibilities for different WMO functions and allocating them to different offices and persons , to ensure an effective and clear segregation of duties within the three lines of defence mechanism.

Travel Policy and Sustainability Reporting

We mainly focused on the strategy on sustainable travel policy and reporting. We issued a suggestion to improve a “low-emission approach” in organisation’s travel policy.

Rental Policy

On this aspect , following our previous financial analysis, we recommended that WMO sets out transparent criteria and clear guidelines on sensitive issues – including tenants’ eligibility, and economic and logistic conditions applied to different categories on tenants - to enhance effective and perceived transparency and accountability and to minimise risks (i.e. reputational, security, etc.).

Procurement

In this area, we examined and made recommendations on the following issues:

- The development of the Procurement Plan and Activity Tracking Tool and the use of guidelines.
- The relationship between the General Terms and Conditions and the requirements of the UN Supplier Code of Conduct.
- The use of the Request for Quotation (RFQ) and disclosure to suppliers.
- The contracts budget estimation and the ex- post increases of contractual amount.
- The compliance with the WMO Standing Instructions chapter 10

Staff sourcing

We considered the approach regarding staff sourcing and the mitigation of subsequent risks (i.e. understaffing, turn-over, need for consultants, etc.) and we recommended that WMO adopt an integrated comprehensive staffing policy.

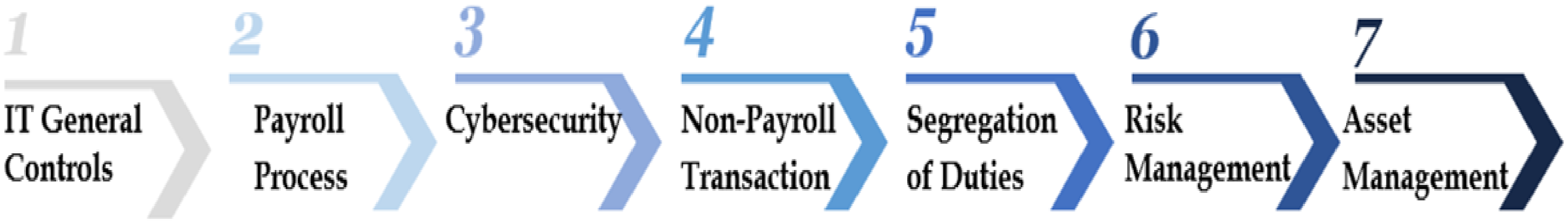
Data Protection and Privacy Policy

We observed that WMO doesn’t have a tailored dedicated data protection and privacy policy and therefore we recommended that WMO adopt a specific policy, in line with the UN policies, and subsequently update all impacted internal rules and policies.

Section C.

IT Control areas and overview findings

The IT control approach was developed in relation to the current system and also in a "forward-looking perspective", taking into account the imminent implementation of the new ERP in 2025, and covered the following IT areas:



IT controls regarded also the assessment of the status of 2022 recommendations and suggestions.

IT General Controls

We evaluated the ensuring data security, integrity, and availability in the design and management of an information system were evaluated through a series of controls implemented across the following IT processes on Oracle E-Business Suite application:

Manage Change: controls aimed at ensuring that changes to systems are appropriate and properly authorized and tested before they are implemented;

Manage Access: controls aimed at ensuring that only authorized users with appropriate roles/profiles to perform activities have access to systems;

Manage IT operations: controls aimed at ensuring a reliable processing environment and management of routine operational problems.

We observed that

FY2022 = audit deviation has been effectively addressed for the review of all Business accounts of the Oracle E-Business Suite application

FY 2023 = no deviations were noted for FY2023.

Payroll process

The objective was to verify the adequacy of the payroll process to ensure compliance of transactions and to identify potential risks that could lead to errors, omissions, or non-compliance with existing payroll policies and procedures, as well as possible fraud or abuse in the use of the Organization’s funds. Follow-up on the walkthroughs and operating effectiveness testing the design and operating effectiveness of the Organization’s Payroll Process were assessed.

A recommendation was issued on :

- automating steps in the payroll process currently performed manually (e.g., updating salary scales and exchange rates) for increased efficiency;
- setting up automated controls to prevent errors and improve management (e.g., implementing blocks for duplicate master data, mandatory fields for employee identification, etc.).

Cybersecurity

The activities focused on verifying the actions taken by the organisation to address the identified recommendations/suggestions.

In particular, the steps were followed:
Understanding the process by analysing the organisation's procedures and conducting interviews with key stakeholders;
Monitoring the management actions taken in response to the recommendations and suggestions identified in the previous cybersecurity audit, which was achieved by analysing the documentation related to the implemented recommendations/suggestions.

We recommended to :

- Complete the Business Impact Analysis (BIA), including disruption scenarios for IT;
- Close the other suggestions/recommendations within the specified timelines.

Non –Payroll Transaction

The objectives of “non-payroll transactions” was specifically related to travel and voluntary contributions IT procedure.

The audit works was conducted to verify the transparency, accuracy and compliance with the organisation's policies and applicable regulations.

The IT audit revealed that :
- most of the steps within the processes are currently done manually (e.g., updating standard costs and DSA);
- no- adequate automated controls to prevent

We recommended to :

- Automating steps in processes currently performed manually (e.g., updating standard costs and DSA for travels) to streamline operation;
- Implementing automated controls to prevent errors and enhance efficiency (e.g., blocking overrides for voluntary contributions

Segregation of duties (SoD)

The activities focused in understanding the actual level of segregation at both "functional" and "systemic" levels and IT control measures implemented by the Organization to segregate users' operational responsibilities on the ERP system to prevent errors and fraud.

The IT audit revealed that the SoD framework provides for the formalization of "Authorization Matrices," which take into account rules defined at the "process" level, but not at the "systemic" level, including associations between organizational roles/processes and access rights granted in the system (roles/profiles/authorizations, etc.).

We recommended to improving the SoD framework by including the associations between organizational roles/processes and access rights granted in the system (roles/profiles/authorizations, etc.).

In addition, the revised SoD framework based on the above suggestion, should be described within a procedure that details the entire process:
- From “functional” to "systemic" segregation of duties;
- From defining/updating SoD rules and compensatory controls to mitigating risks for the “Medium compatibility”.

Risk Management

The audit assessed the controls put in place by the Organization and identify, assess and manage risks. The following steps were taken: understanding the process, by analyzing organization's procedures and conducting interviews with key stakeholders; understanding the framework implemented and the approach used to perform risk assessments (quantitative and qualitative elements);understanding the implemented measures in place to mitigate risks identified (preventive and/or detective); analyzing the risk control matrix through an assessment of inherent and residual risks and an analysis of controls implemented to mitigate them.

The IT audit revealed that the risk assessment that can currently be performed on the organisational process can be classified as qualitative rather than quantitative;
Due to the lack of automatic controls in the ERP system for most of the organisational processes, it is not possible to collect sufficient data for a quantitative analysis of the risks;
The lack of an ad hoc risk assessment tool makes the process time consuming and difficult;
The process does not include predictive risk assessment for organisational processes.

We recommended implementing :

- automation for organizational processes currently performed manually to ensure sufficient data availability for conducting quantitative risk analysis;
- a tool for conducting risk assessments;
- a predictive approach in risk assessment.

Asset Management

IT control measures implemented by the Organization for tracking, classifying, and monitoring Organization assets were analyzed through understanding of the asset management process within the ERP system (and its technical parameters), including asset insertion, asset changes, and asset deletions; analysis of the asset register and the mandatory fields defined on the system; analysis of the access rights associated with users authorized to register, modify and delete assets and verification of the process of assigning user access rights.

The IT audit revealed:
- Oracle responsibilities "WMO Fixed Assets Chief User" and "WMO Fixed Assets user" both allow the creation and change of asset records, assigning asset values in the register, editing the depreciation table etc. The separation between the duties of the actors involved in the process appears not strong enough to ensure proper segregation among them;
- The fields in the asset register are all inserted manually and aren't always filled (e.g., "purchase order number", "original cost", "assigned to", etc.);
- System does not categorize assets as "capitalized" or "not capitalized" automatically based on their value.

We recommended :
- Enhancing segregation of duties between the actors involved in the process;
- Enforcing mandatory completion of all relevant fields in the asset register to ensure data accuracy and integrity;
- Automating the categorization of assets as "capitalized" or "not capitalized" based on predefined value thresholds.

2. Annexes Follow-up – Statistics

Report on FS	2021	2022	2023
	Issued	Issued	Issued
Recommendations	30	23	19
Suggestions	1	1	3

TOTALS	ISSUED	CLOSED	
Recommendations of previous years	74	59	
Recommendations issued by the SFAO (still pending at the beginning of our mandate)	12	10	

Thanks for the attention