Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2021/033

Audit of data governance, management and reporting in the Office of Investment Management of the United Nations Joint Staff Pension Fund

Internal controls over data governance and management, data security, and reporting need to be strengthened

30 July 2021
Assignment No. AT2021-801-01

Audit of data governance, management and reporting in the Office of Investment Management of the United Nations Joint Staff Pension Fund

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of data governance, management and reporting in the Office of Investment Management (OIM) of the United Nations Joint Staff Pension Fund. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over data governance, management and reporting in OIM. The audit covered the period from January 2019 to April 2021 and included a review of: (a) data strategy, governance and management; (b) data quality; (c) data privacy and confidentiality; (d) data security; and (e) reporting.

The audit showed that internal controls over data governance and management, data security, and reporting need to be strengthened.

OIOS made seven important recommendations. To address issues identified in the audit, OIM needed to:

- Establish a data quality policy and related metrics; implement a data incident reporting and tracking process; and establish training programmes on data quality for its user community;
- Establish a data quality policy and related metrics; implement a data incident reporting and tracking process; and establish training programmes on data quality for its user community;
- Undertake a data confidentiality and privacy risk assessment for its systems and records, and update the data confidentiality and retention policy for Office 365-related services;
- Develop a detailed schedule for the retention of its data and records including provisions relating to their disposal or archival upon the expiry of the retention period;
- Expand the incident management procedure to include the procedure for reporting of data incidents, and inform users of the amended procedure to ensure that data incidents are reported promptly;
- Address the information and communications technology security weaknesses relating to its website, SharePoint and email distribution list, log recording configuration, mobile devices and lack of a backup solution for Office 365 data; and
- Taking into consideration its information needs, define a comprehensive data reporting framework and deploy standardized tools to prevent duplication of effort and extensive manual intervention.

OIM accepted the recommendations and has initiated action to implement them.

CONTENTS

Audit of data governance, management and reporting in the Office of Investment Management of the United Nations Joint Staff Pension Fund

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of data governance, management and reporting in the Office of Investment Management of the United Nations Joint Staff Pension Fund (UNJSPF).

2. UNJSPF was established in 1949 by the General Assembly to provide retirement, death, disability, and related benefits for the staff of the United Nations and other organizations admitted to the membership of UNJSPF. OIM is responsible for managing the investments for UNJSPF whose market value stood at $83 billion as of 31 March 2021. While 83.5 per cent of the Fund's assets were managed internally, 16.5 per cent of its assets were managed externally.

3. OIM is composed of four main sections: (i) Office of the Representative of the Secretary-General (RSG); (ii) Risk and Compliance Section; (iii) Operations, Information Systems and Programme Administration Section; and (iv) Investment Section. The Operations, Information Systems and Programme Administration Section is headed by the Chief Operating Officer (COO) who reports to the RSG. OIM is also supported by an internal five-member legal team reporting to RSG.

4. OIM generated, collected, used, processed, and retained a wide variety of data and records in its information and communications technology (ICT) systems, including investment data, business data, financial records, and some personally identifiable information (PII) related to personal trades for compliance purposes. OIM used more than 12 different systems including cloud-based applications (e.g., Office 365-based systems for email and data storage, Trade Order Management System for investment transactions, and Risk System for storing and processing of information related to investment risk management). Additionally, OIM used the United Nations Secretariat's enterprise resource planning system (Umoja) and talent management system (Inspira) for its human resources, procurement and other administrative requirements.

5. Comments provided by OIM are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

6. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over data governance, management and reporting in OIM.

7. This audit was included in the 2021 risk-based work plan of OIOS due to risks associated with data governance, management and reporting, particularly risks relating to data privacy, confidentiality and security.

8. OIOS conducted this audit from January to May 2021. The audit covered the period from January 2019 to April 2021. Based on an activity-level risk assessment, the audit covered risks areas relating to: (a) data strategy, governance and management; (b) data quality; (c) data privacy and confidentiality; (d) data security; and (e) reporting.

9. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data obtained from ICT systems and records; and (d) ICT security tests.

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

III. AUDIT RESULTS

A. Data strategy, governance and management

The data governance and management framework needs to be strengthened

11. Best practices define data governance as control over the management of data assets[1]. Data governance ensures that data and information are consistently defined and understood across the enterprise. While data governance defines organizational structures, data management is the technical implementation of data governance. A data governance and management framework include establishing: (i) data strategy and oversight; (ii) data quality; (iii) data privacy, confidentiality and security; and (iv) reporting.

12. In April 2020, the Secretary-General promulgated a data strategy for the United Nations to build an ecosystem that unlocks the full potential of data for effective governance by building capabilities in data management and data analytics. The enablers for the Secretary-General's data strategy include people and culture, data governance and strategy, oversight, partnerships, and the technology environment.

13. OIM had developed a data strategy in April 2020 and confirmed its intention to align with the data strategy of the Secretary-General. However, OIM's data strategy did not specifically include principles related to data protection and privacy, classification, transparency, inventory and optimization which are integral to alignment with the Secretary-General's data strategy. Further, OIM's data strategy was developed without adequate consultation with business users to secure their buy-in and sensitize them on responsible data handling.

14. In November 2017, OIM initiated a data governance and management programme ("data programme") with the help of an external consultant. The programme objective was to setup a data governance framework and a data warehouse. However, implementation of the programme was paused in August 2019 after incurring expenditure of $1 million without any material benefit to OIM. The external consultant produced several documents (e.g., data dictionary, data governance manual, 68 data use cases, data incident flowchart and data architecture) which were not finalized or put to use. Additionally, in December 2020, OIM conducted an assessment which found that it was at a low level of data maturity. In response to the assessment, OIM had developed a data maturity roadmap in April 2021, but was yet to define the mechanisms to track its implementation.

15. Effective data governance and management structures are required to ensure the success of a data programme. The following gaps were noted:

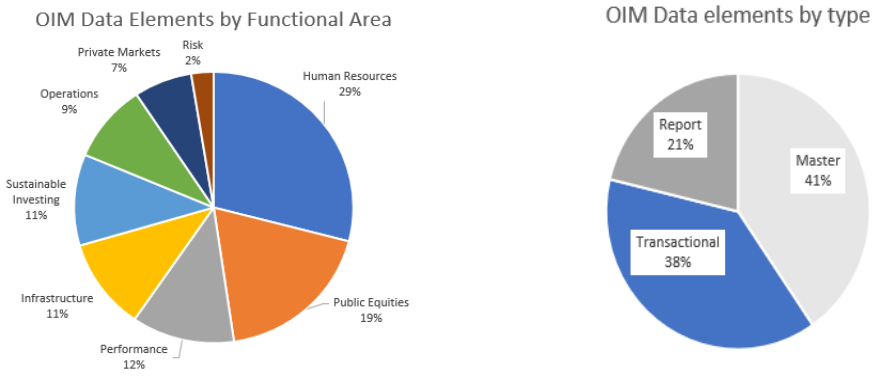
(i) Based on a OIOS recommendation (Report 2020/056), OIM had reinitiated the data programme in October 2020. However, the programme remained at an early stage without clear scope and objectives. Further, OIM was allocated a budget of $1.35 million in 2021 for the data programme, none of which was used as of May 2021.

[1] Data assets refer to a system, application output file, document, database, or web page that is used to generate value to stakeholders.

(ii) Even though the Data Governance Committee re-constituted in October 2020 to lead the data programme, its terms of reference were yet to be finalized. Further, the Committee did not have any representation from senior management. Also, the data programme was not regularly discussed in the ICT Steering Committee of OIM. Consequently, clear direction from senior management was lacking.

(iii) There was no data asset inventory for OIM with clearly defined data stewardship and oversight responsibilities. During the audit, OIM documented an initial data inventory (with 188 data assets) which could serve as a baseline for determining data stewardship and oversight responsibilities. Chart 1 shows the data types and data elements in OIM, by functional area.

Chart 1: Data types and data elements in OIM by the functional area



16. These gaps could adversely affect the implementation of the data programme and result in data quality issues, errors, misclassification, loss, and inefficient manual intervention to verify data validity and accuracy.

(1) OIM should: (i) finalize its data strategy in coordination with business users; (ii) finalize the terms of reference of the Data Governance Committee; (iii) complete the initial enterprise-wide inventory of its data assets; (iv) clearly assign roles and responsibilities over data ownership and stewardship; and (v) ensure that the senior management team and the ICT Steering Committee are provided with regular status updates on the implementation of the data programme.

OIM accepted recommendation 1. Recommendation 1 remains open pending receipt of: (i) finalized data strategy and terms of reference for the Data Governance Committee; (ii) enterprise-wide inventory of OIM's data assets; (iii) evidence of clearly assigned roles and responsibilities for data ownership and stewardship; and (iv) evidence of regular updates provided to the ICT Steering Committee on implementation of the data programme.

B. Data quality

Data quality mechanisms need to be defined

17. Data quality best practices comprising appropriate policies, guidelines, and metrics are critical to the business of an organization. OIM had not adopted an integrated approach to data quality management, with appropriate resources for ensuring data quality. The lack of data quality policies, metrics and guidelines caused the following:

(i) OIM encountered data quality issues on a frequent basis. For example: a data quality issue related to update of a benchmark; incorrect performance data due to error in a regional index; a break in the data feed from an external service provider; synchronization problems related to voluntary corporate actions; and historical data discrepancies in the customized benchmark index.

(ii) OIM received incorrect weekly reports on asset allocation from its vendor, reflecting wrong data. The weekly report is critical for asset allocation. Such data errors could have financial implications for OIM. It took OIM five months to detect and report the error to the vendor. Recurring data discrepancies caused a lack of trust in data quality amongst the OIM user community, prompting various teams to perform their own data quality checks using their own tools in the absence of a common framework, clear ownership, and an appropriate resolution process.

(iii) Performance data provided by external data service providers showed outdated data which required manual reconciliation and correction. For example, the alternative investments team noted that in the service provider's system, data relating to September 2020 was incorrectly reflected in the December 2020 reports. This required manual intervention to get the data corrected.

(iv) There were no training programmes for OIM's user community to address the risks associated with inadequate data quality.

18. Absence of a comprehensive data quality policy and programme could cause data errors, processing delays, and necessitate frequent data error corrections.

(2) OIM should: (i) establish a data quality policy and related metrics; (ii) implement a data incident reporting and tracking process; and (iii) establish training programmes on data quality for its user community.

OIM accepted recommendation 2. Recommendation 2 remains open pending receipt of evidence of: (i) establishment of a data quality policy and related metrics; (ii) implementation of a data incident reporting and tracking process; and (iii) provision of training on data quality for its user community.

C. Data privacy and confidentiality

Need to strengthen controls over data privacy and confidentiality

19. Data privacy, confidentiality and handling are integral parts of a data governance and management framework. The Secretary-General's bulletin ST/SGB/2007/6 (Information Sensitivity, Classification, and Handling) requires the classification and secure handling of confidential information. Further, in 2018, the High-Level Committee on Management adopted the ten principles on personal data protection and privacy which requires United Nations organizations to implement appropriate administrative, physical and technical safeguards to protect the security of personal data against unauthorized or accidental access, damage, loss, inadequate data retention, or other risks presented by data processing.

20. In its enterprise risk register, OIM had rated the risks relating to data privacy and confidentiality as high. Since OIM had not undertaken a full assessment of the underlying risks, these ratings were based on judgment. OIOS noted the following:

(i) OIM's policy on classification of documents and record retention was outdated as it did not contain provisions relating to Office 365 products (Outlook, Teams, and SharePoint). Office 365 presented a new set of challenges in the way data could be managed and searched, which require adequate oversight to protect sensitive data from inappropriate disclosure. Office 365 features such as content search and e-discovery could allow administrators to search and retrieve other users' emails and content. Two unapproved instances related to e-discovery of user mailbox were noted during the audit. Use of such data discovery features in breach of privacy and confidentiality norms need to be prevented and controlled through an appropriate policy framework and a RASCI (Responsibility and Accountability) matrix. OIM had drafted a RASCI matrix in December 2020 which was yet to be finalized.

(ii) Although OIM had initiated a pilot project in July 2020 on data protection to enforce system-based data classification controls and protection over its electronic data, the project may not be effective in the absence of a data inventory and assessment of the sensitivity of data assets.

(iii) Document classification was inconsistent and was considered a responsibility of OIM's compliance function instead of the concerned document owners/business users. For example, confidential documents such as minutes of the Best Execution Committee, monthly reports produced for the Investments Committee, and project briefs and business cases were not classified/tagged, even though other documents were tagged and protected with passwords. Inconsistent classification could result in inadvertent exposure of sensitive information.

(iv) Access of separated staff and retirees to their OIM email boxes was not disabled. Additionally, such email boxes kept receiving potentially sensitive information which could be misused or inadvertently exposed.

(v) Data handling and confidentiality clauses in contracts with third parties were not adequately enforced. For example, a sub-contractor of an ICT vendor which developed the OIM website maintained a webpage on its own website displaying the UNJSPF logo and a full description of work done[2]. This was not permissible in terms of section 11 of the United Nations General Conditions of the Contracts for the provision of goods and services.

(vi) The OIM website did not contain a privacy policy, cookie policy and terms of use. Further, there were unnecessary tracking cookies on OIM's main website which were not reviewed for applicability and appropriateness.

(vii) A comprehensive assessment of sensitivity in relation to physical and electronic documents was yet to be undertaken, and there was no policy on data storage (SharePoint), data sharing (OneDrive) and data communication (Teams and other related applications).

(3) OIM should: (i) undertake a data confidentiality and privacy risk assessment for its systems and records; and (ii) update the data confidentiality and retention policy for Office 365 related services.

OIM accepted recommendation 3. Recommendation 3 remains open pending receipt of: (i) a data confidentiality and privacy risk assessment for OIM's systems and records; and (ii) an updated confidentiality and retention policy.

[2] https://www.social-ink.net/portfolio/united-nations-joint-staff-pension-fund-office-of-investment-management

Data retention and handling procedures need to be strengthened

21. The Secretary-General's bulletin ST/SGB/2007/5 (Record-keeping and the management of United Nations archives) requires departments and entities to develop and implement a policy regarding the retention of their records through a records retention schedule.

22. OIM's policy on data retention (i.e., retaining records for seven years after the completion of a project) was not supported by specific assessment of data and records pertaining to its various business units. OIOS noted the following:

(i) Aspects related to data backup, archiving and/or destruction upon completion of the seven-year period were not considered in the data retention policy.

(ii) OIM had not undertaken an assessment of its data retained by vendors and external managers. For example, a contract with one vendor (providing services related to best execution analysis) allowed it to retain data indefinitely (until the termination of the contract). Similarly, contracts with external managers did not contain provisions on specific data retention requirements. It was unclear how OIM data would be dealt with if the contract with the external manager was terminated or not renewed. Storage of OIM data by vendors and external managers should be in accordance with OIM's requirements.

(4) OIM should develop a detailed schedule for the retention of its data and records including provisions relating to their disposal or archival upon the expiry of the retention period.

OIM accepted recommendation 4. Recommendation 4 remains open pending receipt of a detailed schedule for retention of OIM's data and records, including for their disposal or archival upon expiration of the retention period.

D. Data security

Data security needs to be further strengthened

23. [redacted]

[redacted]

24. Weaknesses and vulnerabilities in data security could cause potential loss of sensitive data/information.

(5) OIM should: (i) expand the incident management procedure to include the procedure for reporting of data incidents; and (ii) inform users of the amended procedure to ensure that data incidents are reported promptly.

OIM accepted recommendation 5. Recommendation 5 remains open pending receipt of the expanded incident management procedure, and evidence that users have been informed about the amended procedure.

(6) OIM should address the ICT security weaknesses relating to: (i) its website; (ii) SharePoint and the email distribution list; (iii) log recording configuration; (iv) mobile devices; and (iv) lack of a backup solution for Office 365 data.

OIM accepted recommendation 6. Recommendation 6 remains open pending receipt of evidence that the ICT security weaknesses identified in the report have been fully addressed.

E. Reporting

Need to strengthen controls over reporting

25. Reports and business intelligence (BI) provide management with data to support decision making. Further, it allows users at all levels of an organization to access and analyze data to manage the business, monitor performance, discover opportunities, and operate efficiently. OIM must have a reliable data repository with automated reporting tools, fit for purpose, to facilitate timely and efficient decision making.

26. In the absence of a well-defined reporting framework, OIM relied on manual processes to create reports for management and the investment teams. This resulted in inefficient manual data validation and reconciliation. The following issues were noted:

(i) OIM had not conducted an assessment of its data analytics and data mining capability. There was no centralized repository of validated reports that could be used for investment management. The various teams within OIM produced reports for their own internal consumption, since there were no mechanisms for data sharing and knowledge management. Data was downloaded from various systems into Excel to generate reports. Data visualization tools like Microsoft Power BI, which was included in OIM's Office 365 license, was not utilized.

(ii) OIM produced a monthly performance report (Blue Book) for senior management as well as members of the Investments Committee. The Blue Book was produced exclusively from data obtained from the Master Record Keeper. However, some validations were done manually with data contained in OIM's internal systems. The validation process was time consuming and involved manual resolution of discrepancies.

(iii) OIM was not able to develop and use data analytics and dashboards for reporting and decision-making purposes for its key commitments (i.e., sustainable investing - ESG). OIM stated in its 2019 report on sustainable investing that it planned to develop ESG dashboards by sourcing and consolidating material ESG data points for enhancing fundamental and valuation analysis. However, these dashboards were yet to be developed.

(iv) OIM had not developed the required reporting capabilities to assess the use and value of more than 28 externally purchased data feeds. This included seven data feeds specifically meant for the ESG team. This limited OIM's ability to effectively use the data feeds it was paying for.

(7) OIM should, taking into consideration its information needs, define a comprehensive data reporting framework and deploy standardized tools to prevent duplication of effort and extensive manual intervention.

OIM accepted recommendation 7. Recommendation 7 remains open pending receipt of a comprehensive data reporting framework and evidence of deployment of standardized tools to prevent duplication and extensive manual intervention.

IV. ACKNOWLEDGEMENT

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

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

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of data governance, management and reporting in the Office of the Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[3]/ Important[4]	C/ O[5]	Actions needed to close recommendation	Implementation date[6]
1	OIM should: (i) finalize its data strategy in coordination with business users; (ii) finalize the terms of reference of the Data Governance Committee; (iii) complete the initial enterprise-wide inventory of its data assets; (iv) clearly assign roles and responsibilities over data ownership and stewardship; and (v) ensure that the senior management team and the ICT Steering Committee are provided with regular status updates on the implementation of the data programme.	Important	O	Receipt of: (i) finalized data strategy and terms of reference for the Data Governance Committee; (ii) enterprise-wide inventory of OIM's data assets; (iii) evidence of clearly assigned roles and responsibilities for data ownership and stewardship; and (iv) evidence of regular updates provided to the ICT Steering Committee on implementation of the data programme.	30 June 2022
2	OIM should: (i) establish a data quality policy and related metrics; (ii) implement a data incident reporting and tracking process; and (iii) establish training programmes on data quality for its user community.	Important	O	Receipt of evidence of: (i) establishment of a data quality policy and related metrics; (ii) implementation of a data incident reporting and tracking process; and (iii) provision of training on data quality for its user community.	30 June 2022
3	OIM should: (i) undertake a data confidentiality and privacy risk assessment for its systems and records; and (ii) update the data confidentiality and retention policy for Office 365 related services.	Important	O	Receipt of: (i) a data confidentiality and privacy risk assessment for OIM's systems and records; and (ii) an updated confidentiality and retention policy.	30 June 2022
4	OIM should develop a detailed schedule for the retention of its data and records including provisions relating to their disposal or archival upon the expiry of the retention period.	Important	O	Receipt of a detailed schedule for retention of OIM's data and records, including for their disposal or archival upon expiration of the retention period.	30 June 2022
5	OIM should: (i) expand the incident management procedure to include the procedure for reporting of data incidents; and (ii) inform users of the amended	Important	O	Receipt of the expanded incident management procedure, and evidence that users have been informed about the amended procedure.	31 March 2022

[3] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.
[4] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.
[5] Please note the value C denotes closed recommendations whereas O refers to open recommendations.
[6] Date provided by OIM in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of data governance, management and reporting in the Office of the Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[3]/ Important[4]	C/ O[5]	Actions needed to close recommendation	Implementation date[6]
	procedure to ensure that data incidents are reported promptly.				
6	OIM should address the ICT security weaknesses relating to: (i) its website; (ii) SharePoint and the email distribution list; (iii) log recording configuration; (iv) mobile devices; and (iv) lack of a backup solution for Office 365 data.	Important	O	Receipt of evidence that the ICT security weaknesses identified in the report have been fully addressed	31 March 2022
7	OIM should, taking into consideration its information needs, define a comprehensive data reporting framework and deploy standardized tools to prevent duplication of effort and extensive manual intervention.	Important	O	Receipt of a comprehensive data reporting framework and evidence of deployment of standardized tools to prevent duplication and extensive manual intervention.	30 June 2022

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of data governance, management and reporting in the Office of the Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OIM should: (i) finalize its data strategy in coordination with business users; (ii) finalize the terms of reference of the Data Governance Committee; (iii) complete the initial enterprise-wide inventory of its data assets; (iv) clearly assign roles and responsibilities over data ownership and stewardship; and (v) ensure that the senior management team and the ICT Steering Committee are provided with regular status updates on the implementation of the data programme.	Important	Yes	Head of Data and Business Applications	(i) Q2 2022 (*) (ii) Q1 2022 (iii) Q1 2022 (iv) Q1 2022 (v) Q1 2022	(*) Items are aligned with Data Strategy .
2	OIM should: (i) establish a data quality policy and related metrics; (ii) implement a data incident reporting and tracking process; and (iii) establish training programmes on data quality for its user community.	Important	Yes	Head of Data and Business Applications	(i) Q2 2022 (*) (ii) Q1 2022 (iii) Q1 2022	(*) Items are aligned with Data Strategy
3	OIM should: (i) undertake a data confidentiality and privacy risk assessment for its systems and records; and (ii) update the data confidentiality and retention policy for Office 365 related services.	Important	Yes	Head of Information Systems + Compliance Officer	(i) Q2 2022 (*) (ii) Q2 2022 (*)	(*) Items are aligned with Data Strategy The privacy risk assessment is intended to be conducted by an external consultant via a RFQ
4	OIM should develop a detailed schedule for the retention of its data and records including provisions relating to their	Important	Yes	Head of Information Systems +	(i) Q2 2022 (*)	(*) Items are aligned with Data Strategy

[1] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

[2] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

APPENDIX I

Management Response

Audit of data governance, management and reporting in the Office of the Investment Management of the United Nations Joint Staff Pension Fund

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	disposal or archival upon the expiry of the retention period.			Head of Data and Business Applications		
5	OIM should: (i) expand the incident management procedure to include the procedure for reporting of data incidents; and (ii) inform users of the amended procedure to ensure that data incidents are reported promptly.	Important	Yes	Information Security Officer	(i) Q1 2022 (ii) Q1 2022	
6	OIM should address the ICT security weaknesses relating to: (i) its website; (ii) SharePoint and the email distribution list; (iii) log recording configuration; (iv) mobile devices; and (iv) lack of a backup solution for Office 365 data.	Important	Yes	Head of Information Systems + Head of Data and Business Applications	(i) Q1 2022 (ii) Q1 2022 (iii) Q1 2022 (iv) Q1 2022 (v) Q1 2022	
7	OIM should, taking into consideration its information needs, define a comprehensive data reporting framework and deploy standardized tools to prevent duplication of effort and extensive manual intervention.	Important	Yes	Head of Data and Business Applications	(i) Q2 2022 (*)	(*) Items are aligned with Data Strategy