IOM International Organization for Migration

**EXECUTIVE SUMMARY**

**INTERNAL AUDIT REPORT**

**IOM Country Office Brussels**

**BE201801**

**12 - 16 March 2018**

**Issued by the Office of the Inspector General**

**Report on the Audit of IOM Country Office Brussels**
**Executive Summary**
**Audit File No. BE201801**

The IOM Office of the Inspector General (OIG) conducted an internal audit of the IOM Brussels, Belgium (the "Country Office") 12 to 16 March 2018. The internal audit aimed to assess adherence to financial and administrative procedures in conformity with IOM's regulations and rules and the implementation of and compliance with its internal control system.

Specifically, the audit assessed the risk exposure and risk management of the Country Office's activities, in order to ensure these are well understood and controlled by the local management and staff. Selected samples from the following areas were reviewed:

a. Management and Administration
b. Personnel
c. Finance and Accounting
d. Procurement and Logistics
e. Contracting
f. Information and Technology
g. Programme and Operations

The audit covered the activities of the Country Office from March 2016 to March 2018. The Country Office recorded the following expenses based on IOM financial records:

- 2016 - USD 9,744,048 representing 1 per cent and 4 per cent of IOM Total and European Economic Area Region, respectively.
- 2017 - USD 9,708,712 representing 1 per cent and 3 per cent of IOM Total and European Economic Area Region, respectively.

Because of the concept of selective testing of data and inherent limitation of the internal audit work, there is no guarantee that all matters of significance to IOM will be discovered by the internal audit. It is the responsibility of local management of the Country Office to establish and implement internal control systems to assure the achievement of IOM's objectives in operational effectiveness and efficiency, reliable financial reporting and compliance with relevant laws, regulations and policies. It is also the responsibility of local management to determine whether the areas the internal audit covered and the extent of verification or other checking included are adequate for local management's purposes. Had additional procedures been performed, other matters might have come to internal audit attention that would have been reported.

The internal audit was conducted in accordance with the Charter of the Office of the Inspector General and in general conformance with the *International Standards for the Professional Practice of Internal Auditing.*

**Overall audit rating**

OIG assessed the Country Office as **partially effective** which means that "while the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or, some of the controls do not seem correctly designed in that they do not treat root causes *and* those that are correctly designed are operating effectively".

This rating was mainly due to weaknesses noted in the following areas:

1. Shared web server
2. Physical security
3. Risk management standards
4. Backup software
5. Information technology data protection
6. Information and Communication Technology (ICT) business continuity plan
7. Information technology security patch management
8. Internet provider for regional and Country Offices
9. VoIP and bandwidth management
10. Information technology data centre
11. ICT structure
12. Dependence on ICT global user support
13. Programme management and implementation

There was satisfactory performance noted in Contracting.

**Key recommendations: Total = 29; Very High Priority = 1; High Priority = 12; Medium Priority = 16**

**Very High Priority Recommendation**

Prompt action is required within one month to ensure that processes will not be critically disrupted, and IOM will not be ***critically*** adversely affected in its ability to achieve its strategic and operational objectives.

There is one (1) Very High Priority recommendation in information technology, as follows:

- Immediate migration to IOM corporate hosting platforms and decommissioning of all existing solutions not compliant with IOM infrastructure standards.

**High Priority Recommendations**

For the high priority recommendations, prompt action is required within three months to ensure that IOM will not be adversely affected in its ability to achieve its strategic and operational objectives.

Two (2) recommendations for Management and Administration, nine (9) recommendations in Information Technology, and one (1) recommendation in Programme and Operations. These recommendations aim to ensure that assets of IOM are properly safeguarded and that IOM operations are effective and efficient.

- Enhance access controls to the building and IOM offices.
- Formulate comprehensive business continuity plan integrating IOM risk management standards and communicate the plan to all staff.
- Coordinate with the head office to update the standard backup software to the newest version.
- Security and access controls must be established for the reintegration database and data protection mechanisms must be put in place.
- Immediately finalize the ICT business continuity plan and conduct simulation exercise to test the effectiveness of the business continuity plan and update the plan, as necessary.
- The ICT division must advise the regional office and Country Office about interim solutions to patch third-party applications on workstations and provide a clear roadmap for full implementation of a patch management solution for workstations and servers.
- With support from ICT division, Brussels information technology team must plan for complying with the requirement of having two internet links with different providers.
- Ensure that VoIP devices are compliant with IOM ICT standards.
- Identify a proper solution for the fire detection system in the information technology data centre.
- Assess the feasibility of the suggested options to address the challenges faced by the Belgium information technology team.
- ICT division should ensure adequate resources are allocated to reduce the processing time and heavy reliance on the ICT global user support team.
- Establish an effective monitoring mechanism and better coordination between the Project Managers and Resource Management Unit to ensure project costs are adequately budgeted, aligned with operational spending and correctly projectized.

Except in the area of Contracting, there remain another 16 Medium priority recommendations consisting of 3 recommendations in Management and Administration, 2 recommendations in Personnel, 5 in Finance and Accounting, 2 in Information Technology, and 1 recommendation in Programme and Operations, which need to be addressed by the Country Office within one year to ensure that such weaknesses in controls will not moderately affect the Country Office's ability to achieve its entity or process objectives.

There are no Low priority recommendations noted.

**Management comments and action plans**

All 29 recommendations were accepted. Management is in the process of implementation. Comments and/or additional information provided have been incorporated in the report, where appropriate.

This report is intended solely for information and should not be used for any other purpose.

## I. About the Country Office

The main office is located in Brussels, Belgium. As of March 2018, the Country Office has 37 personnel categorized into: 1 official and 36 staff. The Country Office recorded the following expenses based on IOM financial records for the following periods:

- 2016 - USD 9,744,048 representing 1 per cent and 4 per cent of IOM Total and European Economic Area Region, respectively.
- 2017 - USD 9,708,712 representing 1 per cent and 3 per cent of IOM Total and European Economic Area Region, respectively.

The Country Office has a total portfolio of 83 projects and total budget of USD 20,978,656. The top 2 projects by type:

- 17 Projects for Return of Migrant Activities amounting to USD 1,752,951 million or 8 per cent of the budget.
- 31 Projects on Reintegration of Migrant Activities amounting to USD 17,093,799 million or 81 per cent of the budget.

## II. Scope of the Audit

### 1. Objective of the Audit

The internal audit was conducted in accordance with the Charter of the Office of the Inspector General and in general conformance with the *International Standards for the Professional Practice of Internal Auditing.* The focus of the audit was adherence to financial and administrative procedures in conformity with IOM's rules and regulations and the implementation of and compliance with its internal control system.

### 2. Scope and Methodology

In compliance with Internal Audit standards, attention was paid to the assessment of risk exposure and the risk management of the Country Office activities in order to ensure that these are well understood and controlled by the local management and staff. Recommendations made during the internal audit fieldwork and in the report aim to equip the local management and staff to review, evaluate and improve their own internal control and risk management systems.

## III. Audit Conclusions

1. **Overall Audit Rating**

   OIG assessed the Country Office as **partially effective** which means that "while the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or, some of the controls do not seem correctly designed in that they do not treat root causes, *and* those that are correctly designed are operating effectively."

2. Satisfactory performance was noted in Contracting.

## IV. Key Findings and Very High and High Priority Recommendations

Very High Priority Recommendations

1. Shared web server
   The regional office and Country Office share a local/old web server running on solutions, which do not follow IOM infrastructure standards.

   Very High Priority Recommendations
   - Immediate migration to IOM corporate hosting platforms and decommissioning of all existing solutions not compliant with IOM infrastructure standards.

High Priority Recommendations

1. Physical Security
   Some security deficiencies have been noted, which could represent a possible threat, in particular with the Country Office situated in an area where regular demonstrations occur.

   High Priority Recommendation:
   - Enhance access controls to the building and IOM offices.

2. Risk Management Standards
   There was no comprehensive business continuity plan and integrated Risk Management Standards following IOM guidelines.

   High Priority Recommendation:
   - Formulate comprehensive business continuity plan integrating IOM risk management standards and communicate the plan to all staff.

3. Backup software
   The Regional Office and Country Office backup software version in place has been upgraded by a newer version and since May 2018 will no longer receive automatic security and quality updates.

High Priority Recommendation:

- Coordinate with head office to update the standard backup software to the newest version.

4. Information technology data protection
   The Country Office's reintegration database in place does not have the necessary security/authentication, user roles/management module and audit logs for application changes.

   High Priority Recommendation:
   - Security and access controls must be established for the reintegration database and data protection mechanisms must be put in place.

5. ICT business continuity plan
   The Country Office has not finalized and implemented its ICT business continuity plan despite recent security incidents that have occurred.

   High Priority Recommendation:
   - Immediately finalize the ICT business continuity plan and conduct simulation exercise to test the effectiveness of the business continuity plan and update the plan, as necessary.

6. Information technology security patch management
   It was observed that information technology security patches and application updates can only be done one workstation at a time.

   High Priority Recommendation:
   - The ICT Division must advise the regional office and Country Office about interim solutions to patch third-party applications on workstations and provide a clear roadmap for full implementation of a patch management solution for workstations and servers.

7. Internet provider for regional and Country Offices
   The regional and Country Offices have only one internet connection each, wherein other Country Offices are required to segregate traffic in two links (one for corporate applications, one for internet/guest browsing).

   High Priority Recommendation:
   - With support from ICT Division, Brussels information technology team must plan for complying with the requirement of having two internet links with different providers.

8. VoIP and Bandwidth management
   Both the Regional and Country Office's VoIP and bandwidth management appliances had not undergone security patching or operating systems update since initial implementation.

High Priority Recommendation:

- Ensure that VoIP devices are compliant with IOM ICT standards.

9. Information technology data centre

   There is no fire detection system and alarm notification in the Country Office information technology data centre. Instead, there is an existing temperature sensor and email alert system in place.

   High Priority Recommendation:

   - Identify a proper solution for the fire detection system in the information technology data centre.

10. ICT structure

    The Brussels information technology team operates without a senior team leader and has limited capacity to support the increasing demand for information technology support from the Regional Office, Country Offices and European Union - Electoral Observation Missions commitment.

    High Priority Recommendation:

    - Assess the feasibility of the suggested options to address the challenges faced by the Belgium information technology team.

11. Dependence on ICT global user support

    Despite the regional office and Country Office being fully migrated to IOMINT domain, user account creation always requires involvement from ICT global user support, to fully commission the account with a mailbox.

    High Priority Recommendation:

    - ICT division should ensure adequate resources are allocated to reduce the processing time and heavy reliance on the ICT global user support team.

12. Programme management and implementation

    There was no documented and systematic budget monitoring/expenditure review done in coordination with the Project Managers/Operations.

    High Priority Recommendation:

    - Establish an effective monitoring mechanism and better coordination between the Project Managers and Resource Management Unit to ensure project costs are adequately budgeted, aligned with operational spending and correctly projectized.

*Management agreed with the recommendations and is implementing them.*

**ANNEXES**

**Definitions**

The overall adequacy of the internal controls, governance and management processes, based on the number of audit findings and their risk levels:

| Descriptor | Guide |
|---|---|
| **Fully effective** | Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, address the root causes and Management believes that they are effective and reliable at all times. |
| **Substantially effective** | Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or Management has doubts about operational effectiveness and reliability. |
| **Partially effective** | While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or, some of the controls do not seem correctly designed in that they do not treat root causes, those that are correctly designed are operating effectively. |
| **Largely ineffective** | Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively. |
| **None or totally ineffective** | Virtually no credible controls. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness. |

**Audit Recommendations – Priorities**

The following internal audit rating based on **IOM Risk Management** framework has been slightly changed to crystalize the prioritization of internal audit findings according to their relative significance and impact to the process:

| Rating | Definition | Suggested action | Suggested timeframe |
|---|---|---|---|
| **Very High** | Issue represents a control weakness which could cause ***critical*** disruption of the process or ***critical*** adverse effect on the ability to achieve entity or process objectives. | Where control effectiveness is not as high as 'fully effective', take action to reduce residual risk to 'high' or below. | Should be addressed in the short term, normally within 1 month. |
| **High** | Issue represents a control weakness which could have ***major*** adverse effect on the ability to achieve entity or process objectives. | Plan to deal with in keeping with the annual plan. | Should be addressed in the medium term, normally within 3 months. |
| **Medium** | Issue represents a control weakness which could have ***moderate*** adverse effect on the ability to achieve entity or process objectives. | Plan in keeping with all other priorities. | Should be addressed normally within 1 year. |
| **Low** | Issue represents a minor control weakness, with ***minimal*** but reportable impact on the ability to achieve entity or process objective. | Attend to when there is an opportunity to. | Discussed directly with management and actions to be initiated as part of management's ongoing control. |