INTERNATIONAL TRAINING CENTRE OF THE ILO

Board of the Centre

75th Session, Turin, 17 - 18 October 2013 **CC 75/5/4**

FOR INFORMATION

FIFTH ITEM ON THE AGENDA

Follow-up to the recommendations of the Chief Internal Auditor for the year ended 31 December, 2012

Introduction

1. The Chief Internal Auditor of the International Labour Office (ILO), who is also the Internal Auditor of the Centre, presented to the Board during its 74th Session in November 2012, a report on significant findings resulting from its internal audit assignments undertaken at the Centre in 2011. Based on a risk assessment of the Centre's business operations, the Internal Auditor's Office (IAO) performed an IT security audit in the period October to November 2011 and issued its final report in January 2012.

2. This paper addresses follow-up action taken by the Centre on IAO's recommendations on main areas identified for improvement on IT security contained in its report to the Board in 2012.

3. The Internal Auditor did not indicate any material weakness in the Centre's system of internal control in IT security. All high priority recommendations in the 2012 report and the remaining audit recommendations on the management and controls of the Centre's income generated from its training activities, along with the Centre's responses and details of completed follow-up actions, are set out in Appendix I.

4. The Centre will continue to work with the IAO and keep the Chief Internal Auditor informed of progress on the implementation of outstanding recommendations.

Turin, 13th September, 2013

Appendix I[1]

Recommendation no	Recommendation	Centre response	Implementation Status	Completion date
Audit of income generated from training activities				
1	The Centre cannot presume that it can continue to generate surpluses, nor can it expect to benefit from windfall funding from elsewhere. Therefore, it is imperative that it budgets adequately for all of its training activities and has adequate systems in place to ensure that income is complete and received on a timely basis.	A circular regarding the review, clearance, signature and process flow of agreements for training related activities has been issued to implement the recommendations concerning the establishment of more centralized functions in the area of resource mobilization. The circular establishes the process flow for keeping records of funding agreements as the basis for tracking and monitoring the status and balance of funding agreements. The Business Process Review (BPR) Project Team has developed and implemented a budgeting tool, enhanced the Accounts Receivable Module in Oracle to record and keep track of funding agreements and developed reports to ensure that income is complete and received on a timely basis.	Completed	15 March, 2013

[1] *Recommendations No. 5 and No. 6 were already completed by September, 2012 and their outcomes reported to the Board in document CC 74/4/4.*

Recommendation no	Recommendation	Centre response	Implementation Status	Completion date
2	In 2011, the Centre commissioned a business process review (BPR) of its activities, which had begun while the audit was taking place. The terms of reference of the BPR cover aspects of income generated from training activities. Therefore, the implementation of any changes as a result of IAO recommendations and findings will need to be considered after the conclusion of the BPR.	The BPR Team is concluding its work on the recommendations made by the Geneva Project Team. Tools developed so far are a budgeting tool, guarantees module for recording and monitoring funding agreements, enhanced invoicing tool and a new version of MAP (an activity planning tool) which no longer requires a manual update of certain data but can read them automatically from Oracle. The last BPR item, a tool to manage revenue transfer across years, is currently under test and should be deployed in September.	On-going implementation (95%)	30 September, 2013
3	IAO reviewed the workflow governing the processing of income generated from training activities and found scope for simplification in certain areas, especially regarding the role of technical training departments. There would also appear to be scope for the Financial Services Department (FinServ) to be directly involved in setting the Centre's contribution to its fixed costs, as well as reviewing the role of the Programme Development and Regional Cooperation (COORD) unit in approving the issuance of invoices.	The integration of functions of the former COORD and the Billing and Cost Control Unit under the Budget Management and Financial Reporting Section (BMFR) of FinServ simplified and streamlined the processing of income generated from training activities. The use of standard costs, which accelerated the processing of income, was fully implemented in November 2012. FinServ continues to review the pricing policy and recommend any adjustments in standard cost elements of the pricing policy, as necessary. All issuance of invoices and all cash call down now pass through BMFR.	Completed	15 March, 2013

Recommendation no	Recommendation	Centre response	Implementation Status	Completion date
4	The various IT systems in place at the Centre related to managing costs of training activities, such as catering and accommodation services, are not integrated with the ORACLE financial management module, which has contributed to delays in collecting all information on the costs of each training activity; thus impacting on the time taken to issue an invoice. The lack of integrated systems has also led to the risk of duplication of effort and input errors as the database used predominantly to generate management information on training participation is not linked to the ORACLE financial management system.	As part of the BPR implementation, a tool to speed up the issuance of open-course invoices obtaining the information from MAP was developed. This integration mitigated the risk of input errors and minimized the duplication of effort. In addition, if a budget has been released and uploaded in Oracle, the data in MAP is automatically updated and mirror all transactions concerning an activity in Oracle resulting in data integration between MAP and Oracle. The accommodation and catering services software (SoftSolutions) and Oracle ERP are two different systems in terms of scope and features. SoftSolution is a hotel management software, while Oracle is the Centre's financial management system. No direct feeding of information between the two systems is possible, since the Oracle based activities are initiated only after the SoftSolutions data are checked and validated. In the absence of a direct data feed, a report has been developed from SoftSolutions summarizing course data by activity to reduce the time and effort required to collect data and supplement data needed in Oracle, thereby accelerating activity closing and invoicing processes.	Completed	31 August, 2013

Recommendation no	Recommendation	Centre response	Implementation Status
IT Security Audit			
1	*Asset classification* Perform a classification, inventory and assignment of the IT assets to the corresponding business process and assessment of the impact on loss of confidentiality, integrity and availability may have on IT assets based on business, legal and regulatory requirements.	An inventory of IT assets has been performed and a corresponding IT asset management policy was issued as part of the IT Use Policy. The Information and Communications Technology Service (ICTS) has implemented a Component Failure Impact Analysis (CFIA) to document the assessment of the impact on loss of confidentiality, integrity and availability on assets.	Fully implemented
2	*IT risk assessment* Formalize a methodology for risk management, which includes all security aspects such as confidentiality, integrity and availability. Implement the risk analysis at the Centre's level, extending the one already performed for the Management Information System Business Continuity Plan (MIS BCP).	An ICTS Strategic Plan 2012-15 was issued in 2012, which also addressed IT risk assessment and management processes. An Information Communications Technology (ICT) Governance framework was put in place as part of the strategy; the Centre's Management Team serves as the ICT Governance Board. An IT Risk Register, identifying potential risks and establishing risk mitigation strategies, is maintained. The Chief Information Officer is a member of the Risk Management Committee. Major IT risks are incorporated into the Centre’s Risk Register. ICTS also performed a Component Failure Impact Analysis (CFIA) and Business Impact Analysis (BIA) and continuously maintains and improves its Business Continuity Plan.	Fully implemented

Recommendation no	Recommendation	Centre response	Implementation Status
3	*Access control* Formalize the process of logical access control (including remote access), defining the workflow to manage accounts and profiles, to grant, remove and regularly review access rights. Strengthen the password policy (password length, complexity, expiration) on all applications and systems. Conduct with the appropriate business stakeholders a regular review of the users and access rights. Sensitive information should not be accessible from the Internet unless under strict control and all data should be sent encrypted.	An ICTS Service Catalogue, addressing the formal procedures on granting, changing and removing user accesses to the IT systems, has been prepared. A password policy is documented and included in the "IT Use Policy". ICTS is in the process of migrating the network domain from Novell to Microsoft. Upon completion of the project in 2013, ICTS will be able to implement a strengthened password policy on all application and systems. ICTS regularly coordinates and reviews with HRS any staffing changes and their access rights. User accounts and their access rights are reviewed on a monthly basis. ICTS started identifying systems which would require additional cryptographic controls. It is also implementing a solution for encryption of laptops and shared drives, in addition to providing encrypted communication channels and exchange documents with secure file transfer.	On-going implementation (95%)
4	*Security policy framework* An access control and security policy framework, including the missing policies and procedures regarding IT security such as incident management, log management, access control, network security, disposal of material, change management, etc., should be formalized. Define and implement a training and awareness program to educate users on IT security.	A circular on "IT Security Policy" was issued covering all the domains defined in the international standard ISO/IEC 27001. More specific technical and administrative controls are specified in the "IT Use Policy". A log management policy and IT change management procedures have been issued in 2012. ICTS conducted its first IT security awareness training in mid-2013. This training is also included in the Centre's Staff Development Programme Catalogue and is intended to be taken by all staff.	Fully implemented

Recommendation no	Recommendation	Centre response	Implementation Status
5	*Development of key performance indicators with respect to IT* Identify key performance indicators with the appropriate business stakeholders (Training, Administration, Management) in order to measure the performance and the efficiency of the IT service provided (applications, systems, services). Such indicators may be focused on key risks area and performance (operations, projects, security, investment, personnel, etc.). Define the modality for collecting the information necessary to produce these indicators and the corresponding measurement tools. Establish a dashboard in order to report IT performance and highlight eventual problems.	Key indicators have been identified for business critical system/process. A system of metrics are based on: - Service Catalogue and Service Level Target - ISO 27001 - Component Failure Impact Analysis - Risk Management process - Project Status reporting - Change Management - Incident/Problem Management - IT Security Policy (S.o.A.) - Security metrics A dashboard is in place which regularly documents performance and alerts for problems or incidents requiring action, if any.	Fully implemented
	Security of the information system Define the role of Security Officer with a formal responsibility for management and control of IT security.	As defined in the ICTS Strategic Plan 2012-15, the Chief Information Officer acts as the IT Security Officer and directly reports to Centre's Management.	Fully implemented