INTERNATIONAL TRAINING CENTRE OF THE ILO

Board of the Centre

74th Session, Turin, 1-2 November 2012

CC 74/4/3

FOR DISCUSSION AND GUIDANCE

FOURTH ITEM ON THE AGENDA

Report of the Chief Internal Auditor for the year ended 31 December 2011

Introduction

1. The Office of Internal Audit and Oversight (the IAO) of the Centre fulfils an internal independent oversight function established under article 14.10 of the Centre's Financial Rules. The Rules specify that "the Internal Auditor shall carry out such independent examinations and make such reports to the Director or persons designated by the Director….. in order to ensure an effective internal audit in accordance with Chapter VII of the Financial Regulations." Chapter VII, article 19(d) of the Financial Regulations stipulates that the Director of the Centre shall maintain an internal financial control and internal audit.

2. The IAO's mission is to provide the Director and the Board with an independent, objective assurance activity designed to add value and improve the Centre's operations. In its work, the IAO adopts a proactive approach to facilitating the assessment of risks and internal controls, and promotes a cohesive approach to risk management in support of management's processes to enhance efficiency, effectiveness and value for money in the activities of the Centre.

3. The IAO conducts its audits in accordance with the Institute of Internal Auditors International Standards for the Professional Practices of Internal Auditing.

4. The IAO does not develop or install procedures or engage in any activity that it would normally review or appraise or which could be construed as compromising either its independence or objectivity. The IAO has full and free access to all records, personnel, operations, functions and other material relevant to the subject matter under review.

5. The results of the IAO's 2011 activities have not indicated any material weakness in the Centre's system of internal control in those areas that were subject to an audit. The IAO cannot, however, provide comment on those areas that have not been subject to an internal audit in 2011.

Summary of audit results

6. In 2011, IAO undertook two audits. The first audit reviewed the management and controls over the Centre's income generated from its training activities; and the second was an IT security audit. IAO reported on its findings with respect to the first audit at the 2011 Board.[1] The IT security audit was conducted in the period October to November 2011 and the final report was issued in January, 2012.

IT Security

7. The objectives of the IT security audit were as follows:

   I. an IT risk and security assessment, aiming to identify gaps related to IT security, benchmarking against best practices and international standards such as COBIT and ISO 27001; and

   II. a vulnerability assessment, aiming to assess the exposure of the Centre's Information Technology Systems to external threats.

8. The IT risk and security assessment identified many positive aspects of the Centre's IT security environment. It found that the management of IT follows a structured process, involving senior management, to define IT strategy and manage IT costs. A Business Continuity Plan (BCP) has been defined to ensure the continuity of critical IT activities in case of disaster. Adequate back-

[1] CC 73/5/3: Report of the Chief Internal Auditor on significant findings resulting from internal audit and investigation assignments.

up systems are in place to ensure not only daily back up, but also continuity of systems should a catastrophic event occur. Physical security, system development and project management were also found to be appropriately managed. Major IT projects were found to include adequate steps in terms of specifications, development, tests and transport in production. Developments, which are outsourced, are adequately managed through third party services.

9. The main areas identified for improvement related to asset classification and IT risk assessment; access control; security policy framework; development of key performance indicators with respect to IT; and security of the Centre's information system. Recommendations were made in each of these areas,

10. A vulnerability assessment was conducted, identifying a number of medium and low risk vulnerabilities. The medium risk vulnerabilities would enable an external attacker to access and exploit information contained in a number of the Centre's web servers, or even upload videos. This form of attack, if successful, could increase the Centre's reputational risk exposure. To make the Centre less vulnerable, it was recommended that the Centre strengthen its password policy on all systems and applications; sensitive information should not be accessible from the Internet unless under strict control; and all data should be sent encrypted.

Audits underway during 2012

11. In October, 2011, the Director requested IAO to undertake an investigation into a number of substantial outstanding debts in relation to its training activities. At the time of writing this report, IAO was concluding this investigation.

12. IAO will undertake two audits in 2012. One will review the costing of the Centre's training activities, and the other will review the cost-sharing mechanisms in place for the two UN entities based on the campus (i.e. the United Nations Staff System College and the United Nations Interregional Crime and Justice Research Institute). The results of these audits will be reported to the Board at its 2013 session.

Follow up of internal audit recommendations

13. IAO welcomes the introduction by the Centre of a formal follow-up mechanism on the implementation of internal audit recommendations. A separate paper on this matter is before the Board.[2]

This report is submitted to the Board for discussion and guidance.

Turin, 6 June, 2012

[2] CC 74/4/4: Follow-up to internal audit recommendations.