OPCW

Eighty-Eighth Session
10 – 13 July 2018

EC-88/DG.6
C-23/DG.3
16 May 2018
Original: ENGLISH

NOTE BY THE DIRECTOR-GENERAL

ANNUAL REPORT OF THE OFFICE OF INTERNAL OVERSIGHT
FOR THE PERIOD FROM 1 JANUARY 2017 TO 31 DECEMBER 2017

INTRODUCTION

1.   Financial Regulation 12.5 of the OPCW Financial Regulations and Rules requires the Director of the Office of Internal Oversight (OIO) to prepare a summary report on internal oversight activities for each calendar year, "including on the status of implementation" of the OIO's recommendations. This report is to be transmitted through the Executive Council (hereinafter "the Council") to the Conference of the States Parties by the Director-General, together with such comments as he and the Council deem appropriate. The requirements and guidelines regarding the contents of the report are detailed in Financial Rule 12.5.01.

2.   The Director-General appreciates the added value of the work carried out by the OIO during the year under review, which has contributed significantly to enhancing transparency and accountability throughout the Organisation by strengthening the systems of internal controls, risk management, and governance.

INDEPENDENCE OF THE OFFICE OF INTERNAL OVERSIGHT

3.   The Director-General and the Management of the Technical Secretariat (hereinafter "the Secretariat") are fully committed to ensuring the independence of the OIO, in accordance with the OPCW Financial Regulations and Rules, the OIO Charter, and the auditing standards of the Institute of Internal Auditors (IIA).

COMPLIANCE OF THE OFFICE OF INTERNAL OVERSIGHT WITH THE AUDITING STANDARDS PROMULGATED BY THE INSTITUTE OF INTERNAL AUDITORS

4.   The Director-General notes that the OIO has worked in accordance with the auditing standards stipulated in Financial Regulation 12.6.

5.   The IIA (Netherlands) conducted a quinquennial quality assessment of the OPCW's internal audit function in 2015 and concluded that the OIO conforms with the generally accepted professional practices regulations that comprise the IIA's International Professional Practices Framework. This is the highest rating offered by the IIA and means that "the relevant structures, policies and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual Standard or element of the Code of Ethics in all material respects".

PROGRAMME OF WORK FOR 2017

6.   The Director-General notes with appreciation that the OIO carried out its annual programme of work for 2017 diligently and professionally, despite constraints related to staffing and extra work owing to unplanned assignments, the advisory role played by the Office, and other internal Secretariat matters. OIO staff members continued to provide valuable advice through their participation as observers in meetings of various committees, such as the Committee on Contracts, the Investment Committee, the Property Survey Board, the Information Services Steering Committee, and the Enterprise Resource Planning Project Board. In addition, the OIO conducted a training programme for Secretariat staff on the Quality Management System (QMS). The OIO annual report, which is included as an annex to this Note, reflects in a comprehensive and accurate manner the various tasks performed by the Office in 2017.

REPORTS OF THE OFFICE OF INTERNAL OVERSIGHT

7.   In accordance with the annual programme of work for 2017, the OIO carried out the following eight audit/evaluation assignments:

(a)   Audit of the Management of the Procurement System;

(b)   Audit of the System for the Statement of Internal Control;

(c)   Audit of the Governance of Evaluation in the Technical Secretariat;

(d)   Audit of the Developed Selection Methods for Schedule 3 Plant Sites;

(e)   Audit of the IT Change Management Process;

(f)   Audit of the Implementation of the Secure Information Exchange System for the Electronic Transmission of Declarations;

(g)   Advisory Review of the Design of the Established Data Migration Process for the Unit4 Business World Enterprise Resource Planning System Project; and

(h)   Evaluation of the Activities of the External Relations Division.

8.   As a result of these eight reports on audits and evaluations, a total of 58 recommendations were issued.

QUALITY MANAGEMENT SYSTEM

9.   Six internal audits of activities under the scope of the International Organization for Standardization (ISO) accreditation were conducted in the OPCW Laboratory, the Documents, Registration and Archiving Section, and the OIO:

(a)   Organisation of the OPCW Central Analytical Database and On-Site Databases and Preparation and Testing of Gas Chromatography-Mass Spectrometry Inspection Equipment;

(b)   Organisation of OPCW Proficiency Tests;

(c)   Management of the Quality Management System Document Central Registry and Control of Quality Management System Documents;

(d)   Certification of the OPCW Central Analytical Database and On-site Databases and Certification of Testing, Preparing, and Packing of Gas Chromatography-Mass Spectrometry Inspection Equipment;

(e)   Management Requirements-Handling of Complaints, Control of Non-Conformities and Related Corrective Actions and Management Review Process; and

(f)   Organisation of OPCW Biomedical Proficiency Tests.

10.   The results of the six QMS internal audits were positive. One non-conformity was identified and corrected; a number of valuable observations and suggestions for improvement were also issued.

11.   In 2017, the Dutch Accreditation Council (RvA) performed two assessments of the OPCW and, as a consequence, both ISO 17025:2005 and 17043:2010 accreditations were extended until 1 April 2021. In addition, the scope of ISO 17043:2010 now includes the activities of the OPCW Laboratory related to the biomedical proficiency tests.

12.   The Director-General appreciates the work carried out by the OIO in respect of the QMS, noting that the RvA is now applying a less intensive assessment programme for the accredited processes, which represents an exceptional recognition of the OPCW's professionalism. The next RvA assessment visit will take place in April 2019.

MONITORING THE IMPLEMENTATION OF THE RECOMMENDATIONS OF THE OFFICE OF INTERNAL OVERSIGHT

13.   The Director-General closely monitored the status of the implementation of the OIO recommendations during the year and fully supported the work of the Office. The OIO continued to submit follow-up reports on the implementation of recommendations on a quarterly basis. The Director-General notes that, as at 31 December 2017, the cumulative rate of implementation of the audit and evaluation recommendations was 77.1%.

14.   At meetings of the Management Board, the Director-General, following the guidance of the OIO, advised Directors to prioritise the implementation of pending recommendations. Particular attention was given to critical and long-standing recommendations in order to expedite their implementation.

15.   The Director-General welcomes the new section in the report on the assessment of the impact of implemented audit and evaluation recommendations, which contributed significantly to adding value to the Organisation by enhancing compliance with existing regulations and procedures, strengthening internal controls, and improving the allocation of resources and the effectiveness of programmes and policies.

Annex: Annual Report of the Office of Internal Oversight for the Period from 1 January to 31 December 2017

Annex

**ORGANISATION FOR THE PROHIBITION
OF CHEMICAL WEAPONS**

Office of Internal Oversight

ANNUAL REPORT OF THE

OFFICE OF INTERNAL OVERSIGHT

FOR THE PERIOD FROM

1 JANUARY TO 31 DECEMBER 2017

TABLE OF CONTENTS

APPENDICES

1.   INTRODUCTION

The Office of Internal Oversight (OIO) is pleased to provide the Conference of the States Parties (hereinafter "the Conference") with its annual report on the internal oversight activities for 2017. This report is submitted in accordance with OPCW Financial Regulation 12.5, which provides that "the Head of Internal Oversight shall prepare a summary report on the internal oversight activities" for each calendar year, including the status of implementation of recommendations issued. This report is to be transmitted through the Executive Council (hereinafter "the Council") to the Conference by the Director-General, together with such comments as the Director-General and the Council may deem appropriate. Financial Rule 12.5.01 further elaborates on the content of the summary report. In compliance with those requirements, this report provides an overview of the main activities of the OIO in 2017 and information on the implementation status of the recommendations issued.

2.   MANDATE, SCOPE, AND FUNCTIONS OF THE OFFICE OF INTERNAL OVERSIGHT

Mandate, scope, and charter of the Office of Internal Oversight

2.1   The internal oversight function has been established on the basis of Article 12 of the OPCW Financial Regulations and Rules, which defines its scope and functions. Regulation 12.1 stipulates that "[t]his mechanism will assist the Director-General in the management of the OPCW's resources, through internal audit, inspection, evaluation, investigation and monitoring in order to enhance the efficiency, and economy of the operations of the OPCW". According to Regulation 12.2, "[t]he purpose of internal oversight audits shall be to review, evaluate and report on the soundness, adequacy and application of systems, procedures and related internal controls".

2.2   The scope, responsibility, accountability, and standards of the OPCW internal oversight function are further defined in the OIO Charter approved by the Director-General in 2011. The Charter is being revised to keep it up to date with the International Standards for the Professional Practice of Internal Auditing (issued by the Institute of Internal Auditors (IIA), United States of America).

2.3   While discharging its mandate in accordance with the OIO Charter and the governing rules and regulations relating to internal oversight, the OIO continued to support the OPCW in achieving its objectives. It also continued to enjoy the full support of the Director-General, senior officers, and OPCW staff members.

2.4   The OIO's mission is to enhance and protect organisational value by providing risk-based and objective assurance, advice, and insight. The OIO helps the OPCW achieve its objectives by applying a systematic approach to evaluating and enhancing the adequacy and effectiveness of risk management, internal control, and governance processes.

Confirmation of Office of Internal Oversight independence

2.5   As Director of the OIO, I can confirm the organisational independence of the Office in the conduct of its duties in accordance with the relevant standards of the IIA.[1]

Compliance with Institute of Internal Auditors standards

2.6   OPCW Financial Regulation 12.6 stipulates that "[i]nternal oversight activities shall be conducted in accordance with best professional practice and, in the case of internal audits, in accordance with the auditing standards promulgated by the Institute of Internal Auditors". The audits conducted in 2017 were performed in compliance with the International Standards for the Professional Practice of Internal Auditing of the IIA, its code of ethics, and its definition of internal auditing.

Membership of the Institute of Internal Auditors and United Nations Evaluation Group

2.7   During the reporting period, the OIO was a member of the IIA (United States of America) and its chapter in the Netherlands. Such membership provides OIO staff with knowledge of the latest professional standards in the conduct of audits, and access to the IIA's vast resources of auditing materials and guidance.

2.8   In 2017, the OIO was also a member of the United Nations Evaluation Group. (UNEG). This is an interagency professional network that brings together the evaluation units of the United Nations system, including United Nations departments, specialised agencies, funds and programmes, and affiliated organisations. Such membership provides OIO staff with opportunities to share knowledge about best practices in the United Nations system in respect of evaluation techniques and methodologies.

3.   RESOURCES

Budget

3.1   The total budget of the OIO for 2017 was EUR 979,900.[2] As against this, the actual expenditure was EUR 968,790. Accordingly, the OIO managed to carry out its activities within the available budget resources.

Staffing

3.2   As at 31 December 2017, the OIO had eight budgeted staff positions, consisting of one Director, three professional audit staff, and four general service staff. All staff positions were filled.

---

[1]   IIA Standard 1110 (Organizational Independence) reads as follows: "The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity".

[2]   EUR 931,900 was initially budgeted for the OIO in 2018, and this amount was supplemented by a transfer of EUR 48,000 to meet additional anticipated requirements.

Training

3.3   Staff members of the OIO continued their professional development in 2017 to fulfil the requirements of the International Professional Practices Framework.

3.4   The Office organised a Quality Management System (QMS) training course with an external instructor for 15 staff members of the Technical Secretariat (hereinafter "the Secretariat"). The course, which took place in September 2017, focused on the International Organization for Standardization/International Commission (ISO/IEC) standard ISO 9001:2015, as well as on the requirements of ISO/IEC 17043:2010 and ISO/IEC 17025:2005. The course addressed the latest tools and techniques that allow auditors to conduct, report, audit, and follow up on the findings of internal audits. It also included the guidelines for auditing quality systems and qualification criteria for auditors, with reference to ISO 19011:2011. The course met the requirements of the International Register of Certificated Auditors.

3.5   In June 2017, the Senior Evaluator and Quality Assurance Officer completed the Lean Six Sigma Green Belt Course organised by The Knowledge Academy. The training programme provides extensive knowledge about process management, including its control, measurement, analysis, and improvement.

3.6   The Senior Quality Assurance Assistant attended the ISO 9001:2015 QMS Auditor/Lead Auditor course, organised by TMS Insight (Training & Development) Limited, from 18 to 22 September 2017. The course focused on the understanding of ISO 9001:2015 together with the guidelines for auditing quality systems and the phases of the audit process with reference to ISO 19011:2011.

4.   EVALUATION OF OFFICE OF INTERNAL OVERSIGHT PERFORMANCE

4.1   The OIO was subject to an evaluation of its performance by the IIA, the External Auditor, and the Dutch Accreditation Council (RvA). The two 2017 sessions of the Advisory Body on Administrative and Financial Matters (ABAF) and the facilitation meetings on the OIO and External Auditor's reports also provided States Parties with an opportunity to evaluate and comment on the performance of the Office.

External quality assessment by the Institute of Internal Auditors

4.2   The OIO is subject to external quality reviews every five years that independently validate the quality of its work and ensure that the Office complies with the above-mentioned international standards promulgated by the IIA. Such reviews are performed in accordance with Standard 1312 of the International Standards for the Professional Practice of Internal Auditing issued by the IIA. In accordance with this standard, "[e]xternal assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization". The IIA (Netherlands) conducted a quality assessment of the OPCW's internal audit function in the last quarter of 2015 in accordance with the said standards.

4.3   The OIO is pleased to report that the internal audit activity of the OPCW was assessed by the IIA to "generally conform" to the aforementioned standards and to be in compliance with the IIA Code of Ethics. This is the highest rating offered by the IIA and means that "the relevant structures, policies and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual Standard or element of the Code of Ethics in all material respects". The next external quality assessment will be conducted in 2020.

External Auditor's recommendations

4.4   The OIO continued to coordinate its activities and communicate the outcome of its oversight work with the External Auditor. Furthermore, the OIO's annual planning process included consultation with the External Auditor, in order to avoid duplication and to develop mutual synergies.

4.5   In the year under review, the OIO implemented two of the External Auditor's recommendations made in its reports for 2015 (EC-83/DG.1 C-21/DG.5, dated 8 August 2016) and 2016 (EC-86/DG.3 C-22/DG.5, dated 24 July 2017) respectively. Both recommendations focused on the OIO's work programme. The External Auditor expected the OIO to play a greater role in providing Management with assurance over its significant risks within its annual programme of work and recommended that the OIO should ensure that its internal audit work programme is risk based and focused on the key areas of the business where internal control may fail. The OIO has revamped its risk assessment methodology for its 2018 annual programme of work in line with best international practices. The programme of work focuses on the high risk processes, which are now identified through a robust risk assessment model that takes into account several risk parameters and relative weightages. The OIO has developed an audit strategy that will continue to provide assurance to Management over its significant risks in accordance with its staff and budget resources by auditing all the high and high-medium risk processes over a period of three years.

4.6   Five recommendations issued in previous years regarding the operation of the OIO continued to be addressed in 2017:

        (a)   The first recommendation was that the OIO should consider its current staffing and resourcing model within its overall level of resources, ensuring that it has the structure, skills, experience, and capacity to deliver a core level of assurance over the key risks to the OPCW. The OIO will prepare a document and submit it for Management's consideration in the fourth quarter of 2018.

        (b)   The External Auditor recommended that the governance arrangements overseeing the production of the Statement of Internal Control (SIC) should be strengthened. Senior Management need to be more involved in challenging the SIC to ensure that the statements made are supported by assurance work and highlight areas in which control improvements are planned. Furthermore, the SIC should be subject to review by the Director of the OIO and provide some summary that captures the outcomes from the work of the OIO, and the overall conclusion in respect of internal controls. To this end, the OIO conducted a

comprehensive review of the SIC process in 2017 and recommended that a structured and systematic process be set up by Management to support the assertions made in the SIC.

(c)   The remaining three recommendations were related to establishing a small, independent, objective, and expert audit committee to enhance the assurances to States Parties, focusing on internal control, risk management, and audit provision. The OIO should have a direct reporting line to the Audit Committee and the risk management processes should be subject to a clear challenge process; ideally, this could be conducted by the Audit Committee. In this regard, the OIO explored options available for introducing an audit committee function in the most efficient and cost-effective manner, given the relative size and budgetary constraints of the OPCW. The OIO has prepared several reports and briefings on this subject for the ABAF's consideration. The issue remains under consideration by the ABAF.

4.7   The OIO briefed States Parties on its implementation of the External Auditor's recommendations in two facilitation meetings held in 2017. There was an extensive exchange of views and the role of the oversight function was well appreciated.

Reporting to the Advisory Body on Administrative and Financial Matters and the Executive Council

4.8   In 2017, one facilitation meeting was held with States Parties wherein the Director of the OIO presented the Annual Report of the OIO for 2016 (EC-85/DG.10 C-22/DG.4, dated 24 May 2017). During the meeting, the Office also highlighted the programme of work for 2017, the status of implementation of audit recommendations, and other activities to be prepared during the year.

4.9   The Director of the OIO also made a presentation to the ABAF on the OIO annual report and the activities to be carried out in 2017. The ABAF was also briefed on the OIO's risk assessment process, and expressed its appreciation for the fact that the annual audit plan was developed based on an assessment and prioritisation of organisational risks. The ABAF commended the OIO for its vision and is looking forward to future updates.

Surveys

4.10   As part of the requirements to maintain the Secretariat's ISO accreditation, the OIO conducted an annual satisfaction survey to assess the level of its performance. More than 80% of the responses received rated the OIO as positive (either excellent or good), and only 5% rated it as unsatisfactory. The survey will be further refined in 2018.

Key performance indicators

4.11   The OIO's key performance indicators (KPIs) for 2017 were in line with the results in previous years. The OIO's performance with respect to the KPIs for 2017 is provided in Appendix 1. The OIO plans to review and update these KPIs in line with best

international practices and the guidance provided by the IIA (United States of America). This will provide a better assessment of OIO performance.

Results-based management

4.12   The OIO continued to develop its own results-based management (RBM) system to enhance the achievement of its outputs, outcomes, and impacts in 2017.

4.13   In 2017, 75 tasks were performed by the OIO through the completion of 238 activities covering nine sections: audits, evaluations, and certifications; implementation of recommendations; consulting services; OIO documentation; training; participation in international events; reporting to States Parties and other activities; budget, staff, and administration; and evaluation of performance. These tasks and activities generated 49 outputs which resulted in the achievement of 11 outcomes. These outcomes were intended to be consistent with two expected impacts: the continued trust and credibility of the OIO vis-à-vis States Parties by securing the highest standards of efficiency, competence, and integrity, and strengthened oversight practices to enable the OIO to achieve its mandate and goals with the necessary skilled staff and budgetary resources. Thus, the Office contributed to the achievement of OPCW core objectives 1, 2, and 7. The RBM tool will also be used to prepare a results-based budget for 2018.

Strengthening of the oversight function

4.14   In 2017, the OIO worked to compile all documents related to its role in the OPCW. Volumes include the regulatory framework that guides the OIO (rules, regulations, and international standards and norms); OIO annual reports; and a glossary of terms, definitions, and concepts of technical expressions used in the audit profession. Four volumes are dedicated to professional standards and guidance in the fields of internal audit, information technology (IT) and confidentiality audit, evaluation, and QMS.

4.15   In 2017, the OIO continued to update its strategic vision intended to delineate its prospective role in the future of the Organisation, including coping with new developments in auditing techniques, particularly in the context of emerging technologies and the establishment of a new enterprise resource planning (ERP) system.

5.   OFFICE OF INTERNAL OVERSIGHT PROGRAMME OF WORK FOR 2017

Key tasks of the programme of work for 2017

5.1   The OIO carried out various tasks in the course of 2017. Besides the conduct of internal audits, confidentiality audits, evaluations, and QMS audits, the OIO devoted its time and budget resources to following up on the action taken by the Management to implement the audit recommendations; providing various advisory services to strengthen management processes; participating in several management meetings in an observer capacity; providing certification of inspection equipment; participating in meetings of the Representatives of Internal Audit Services of the United Nations

Organizations (RIAS), UNEG, and other international organisations; training; updating of internal policies and procedures; budget management; staff and administration; and preparing various reports and presentations to governing bodies.

5.2   The percentage of time resources devoted to each group of activities is illustrated in the chart below.
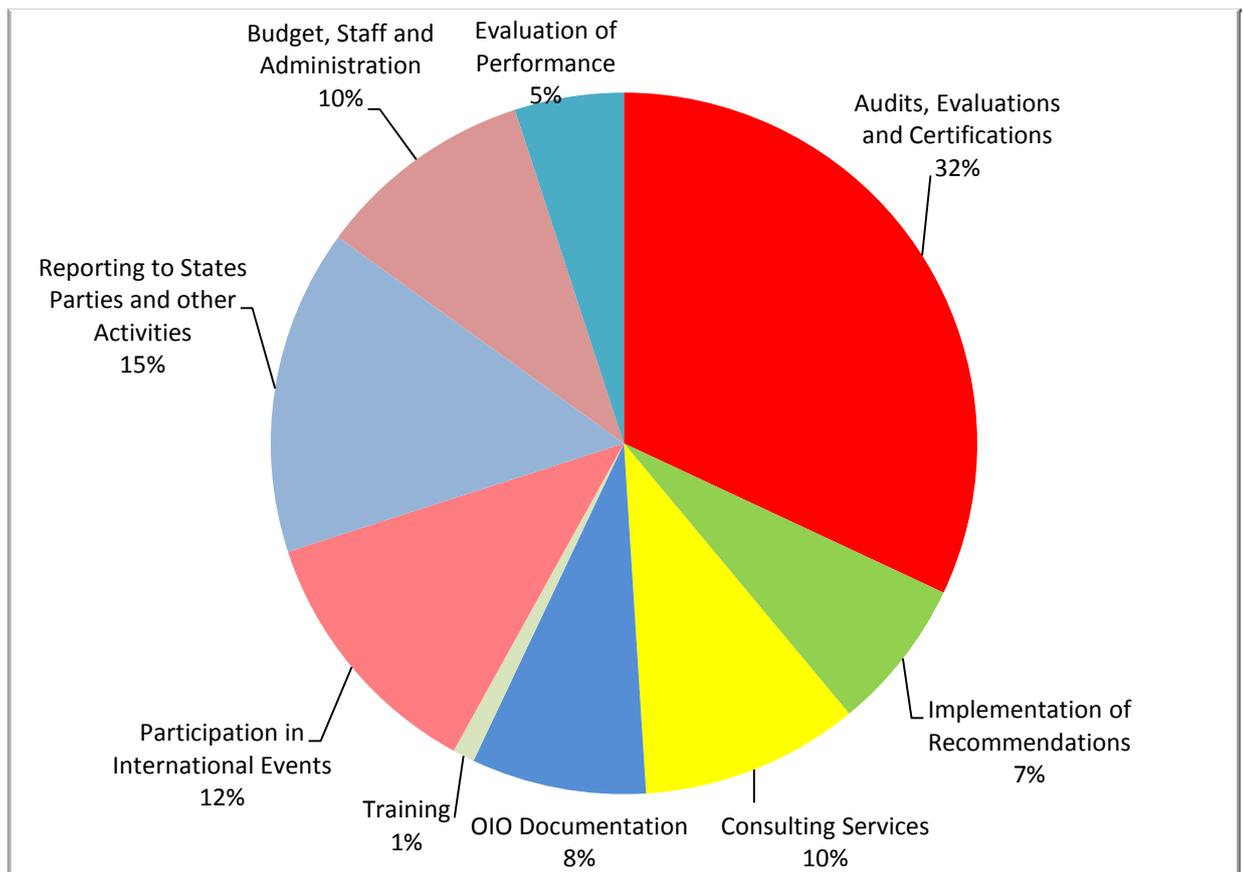
Status of audit/evaluation reports

5.3   The subjects of audits and evaluations for 2017 were identified using the OIO Risk Assessment Framework, applying the methodology of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In addition, the Office took into account requests and concerns expressed by OPCW stakeholders during official meetings, as well as risk assessments made by the Management. In accordance with Financial Rule 12.3.01, the Director-General requested the OIO to address specific issues and concerns that were also considered when drafting the annual programme of work.

5.4   The internal audits, confidentiality audits, evaluations, and QMS assignments for the year 2017 were as follows:

(a)   Audit of the Management of the Procurement System;

(b)   Audit of the System for the Statement of Internal Control;

(c)   Audit of the Governance of Evaluation in the Technical Secretariat;

(d)   Audit of Asset Management (this will be considered in the next OIO Risk Assessment after the implementation of the ERP asset module in 2018);

(e)   Audit of the Developed Selection Methods for Schedule 3 Plant Sites;

(f)   Audit of the IT Change Management Process;

(g)   Audit of the Implementation of the Secure Information Exchange System for the Electronic Transmission of Declarations;

(h)   Advisory Review of the Design of the established Data Migration Process for the Unit4 Business World Enterprise Resource Planning System Project;

(i)   Identity and Access Management in the IT Infrastructure (this audit was replaced by the data migration review, as there was an ongoing project to improve identity and access management (IAM). Some aspects of IAM will be covered in 2018 audits);

(j)   Evaluation of the Activities of the External Relations Division;

(k)   Evaluation of the OPCW Document and Records Management System related to QDOCs[3] (to be considered in the 2018 OIO Risk Assessment after the Secretariat's new Quality Manual is issued);

(l)   Evaluation of the Management of Training Activities (as training activities were under reorganisation in 2017, this evaluation will be included in the 2018 annual programme of work);

(m)   Organisation of the OPCW Central Analytical Database and On-Site Databases and Preparation and Testing of Gas Chromatography-Mass Spectrometry Inspection Equipment;

(n)   Organisation of OPCW Proficiency Tests;

(o)   Management of the Quality Management System Document Central Registry and Control of Quality Management System Documents;

(p)   Certification of the OPCW Central Analytical Database and On-Site Databases and Certification of Testing, Preparing, and Packing of Gas Chromatography-Mass Spectrometry Inspection Equipment;

(q)   Management Requirements: Handling of Complaints, Control of Non-Conformities and Related Corrective Actions, and Management Review Process; and

---

[3]   QDOC = quality-management system document.

(r)   Organisation of OPCW Biomedical Proficiency Tests.

Management acceptance of Office of Internal Oversight recommendations

5.5   In the eight final reports of audits and evaluations carried out in 2017, a total of 58 recommendations were made. Of these, 32 recommendations that were issued up to December 2017 have become due for implementation. These have been included in the database for the follow-up exercise.

5.6   The Director-General approved all of the OIO recommendations issued during the reporting period and instructed the programme managers concerned to take appropriate action, in accordance with Financial Rule 12.3.04.

Quality Management System

5.7   The OIO reviews the quality assurance policy and strategy in order to maintain a comprehensive programme aimed at meeting the requirements of the following international standards, which are subject to the assessment of the RvA:

(a)   ISO/IEC 17025:2005 (General requirements for the competence of testing and calibration laboratories); and

(b)   ISO/IEC 17043:2010 (Conformity assessment—General requirements for proficiency testing).

5.8   To maintain both certificates, three units of the OPCW are accredited, namely, the OPCW Laboratory, the OIO, and the Documents, Registration and Archiving Section (DRA) in the Verification Division (VER).

5.9   The RvA conducted a regular assessment visit in April 2017 to evaluate the efficiency and effectiveness of the Secretariat's QMS and its capacity to perform the accredited activities. The RvA team concluded that the OPCW staff were competent and that the management system was effective and well documented. Only one non-conformity was identified, for which the appropriate corrective action was taken. The result was positively approved by the RvA.

5.10   An extension of the accreditation of the OPCW Laboratory with 17043:2010 for conducting biomedical proficiency testing (BioPT) activities also took place in April 2017.

5.11   The OIO organised two meetings of the QMS Technical Committee (QMSTC). Topics discussed included management review of accredited activities; presentation of the final draft of the Secretariat's Quality Manual, including the updated Quality Policy Statement; mapping of key processes documented in QDOCs and standard operating procedures (SOPs); and assisting Directors with identifying the critical QMS processes, their possible improvements, and the possible application of other ISO standards.

5.12 The OIO issued certificates for the OPCW Central Analytical Database (OCAD) and the on-site analytical databases, as well as certificates for the gas chromatography-mass spectrometry (GC-MS) inspection equipment in accordance with the mandate given by the Council.

5.13 In order to maintain the Secretariat's QMS and ISO accreditation, the OIO needs to organise six audits covering the activities that are subject to accreditation in the OPCW Laboratory, the OIO, and the DRA.

6. SUMMARY OF AUDIT AND EVALUATION REPORTS AND KEY RECOMMENDATIONS

Internal audits

Audit of the Management of the Procurement System (OIO/17/02)

6.1 The OIO conducted an audit of the management of the procurement system in the Organisation as part of its annual programme of work for 2017.

6.2 The audit objective was to evaluate whether the internal control system in the General Services and Procurement Branch is adequate and effective in providing transparency and accountability to the operations and whether the policies, procedures, and tools in place are conducive to efficient management of the procurement function. The audit scope covered the activities of the procurement function from January 2016 to April 2017.

6.3 The audit report contained 16 audit recommendations (eight critical and eight standard). The key audit recommendations were as follows:

(a) develop a procurement strategy, keeping in view the risk/value profile of procurements planned for the year;

(b) clearly define the procurement principles and include "sustainability" as such a principle;

(c) monitor the implementation of procurement plans by developing the procurement planning tool on Sharepoint;

(d) integrate risk management into the procurement function and review the risk register;

(e) develop a suitable monitoring system and KPIs for the procurement function, such as those mentioned in the audit observation;

(f) prescribe delegation of authority separately for the awarding of contracts and signing of contractual documents, as well as for approving requisitions;

(g) finalise the revised increased thresholds for delegation of authority for the awarding of contracts and Committee on Contracts (COC) review, and consider

lower thresholds for delegation of authority for the awarding of contracts for exception/waiver cases;

(h) review the staffing structure and resource level so as to optimise the resource capacity to have sufficient positions with the knowledge and experience required to deliver on the General Services and Procurement Branch objectives and the additional key responsibilities, as noted in the audit observation;

(i) develop a medium-term plan for three to five years for strengthening procurement capacity by acquiring professional certifications related to procurement, such as various levels of Chartered Institute of Procurement and Supply qualifications;

(j) further define the role of the COC by elaborating on the responsibilities of observers, and prescribe procedures such as submission of chronology of events, checklists, and supplier performance evaluation reports;

(k) consider using the system of "ex-post facto" and "retroactive" approvals by the authorised procurement authority instead of "regularisation" and ensure that these are carried out only in a limited number of exceptional cases;

(l) prescribe separate procedures for emergency procurements/exigencies;

(m) develop a Procurement Manual and/or SOPs to provide detailed internal controls and guidelines for managing the different stages of the procurement process, as detailed in the audit observation, with supporting templates/formats in a time-bound manner;

(n) strengthen vendor management practices by establishing a roster of prequalified suppliers; establishing procedures for vendor due diligence, background checks, blacklisting, requiring vendors to adhere to a code of conduct and declare conflicts of interest, and performing evaluations of supplier performance;

(o) effectively use IT tools such as e-procurement, e-approval workflow, and e-signatures to enhance process efficiency and improve accountability;

(p) use a standard coding system for goods and services, such as the United Nations Standard Products and Services Code system;

(q) develop an information database to capture the recurring nature of goods and services procured and develop long-term agreements for such procurements proactively; and

(r) strengthen the file management system by developing a standard index for the content of procurement files.

6.4   All the recommendations were accepted for implementation by the Head of the General Services and Procurement Branch and action is being taken to implement them, so as to strengthen the procurement system in the Organisation.

Audit of the System for the Statement of Internal Control (OIO/17/04)

6.5   The OIO conducted an audit of the process for preparation of the Statement of Internal Control (SIC) as part of its annual programme of work for 2017.

6.6   The audit objective was to evaluate whether the process for preparation of the SIC is adequate and effective in providing transparency and accountability and whether the policies, procedures, and tools in place are conducive to efficient management of the SIC. The audit scope covered the activities related to the preparation of the SIC for the period between its inception (in the 2014 Financial Statements) and 2016.

6.7   The audit report contained five audit recommendations (one critical and four standard). The key audit recommendations were as follows:

(a)   Develop an internal control framework in accordance with COSO guidelines (critical);

(b)   Prepare a control self-assessment methodology and toolkit for managers (standard);

(c)   Revise the format of Director attestations on internal controls (standard);

(d)   Regularly update the risk register with actions taken to improve internal controls (standard); and

(e)   Develop a training module for Directors and Branch Heads education and outreach (standard).

6.8   The recommendations will add value to the Organisation by helping Management in setting up a structured and systematic process to support the assertions made in the SIC. Action is being taken by Management to implement the audit recommendations.

6.9   It is important to emphasise that the SIC, and the implementation of a structured and systematic process to support it, is a cross-cutting responsibility of Management. The education and outreach for the SIC and the use of the associated tools (attestations, self-assessment, risk register, among others) are important to successful implementation of the SIC process. Risks and related controls to be assessed should cascade down from senior managers to junior managers in the reporting line. The implementation of the process may be phased and should be refined over time. Sufficient resourcing (staff and financial resources) should be available to ensure the implementation of the process for preparation of the SIC.

Audit of the Governance of Evaluation in the Technical Secretariat (OIO/16/03)

6.10   In the context of resource constraints and new challenges that require new approaches, the Secretariat is faced with increasing demand from States Parties to justify use of resources and demonstrate the results of and lessons learned from its activities.

6.11   Evaluation has become increasingly central to the programme planning, budgeting, and implementation cycle since the introduction of RBM in 2011. The Secretariat has taken measures to improve the RBM process and has strengthened the monitoring and evaluation of programmes.

6.12   The objective of the audit was to identify and assess the current capacity and utility of evaluation in the Secretariat and to determine to what extent the Secretariat has set up and developed a governance framework for the evaluation function. The audit sought to make recommendations on how to strengthen the governance of evaluations in the Secretariat.

6.13   In this audit report, evaluation was divided into two broad categories: "central evaluations", which are conducted by the OIO and generally support overall Organisation-level policy and strategic decision making; and "decentralised evaluations", which are planned, managed, and conducted outside the OIO and are generally embedded in programmes supporting line management decision making. Decentralised evaluations are further differentiated by self-evaluations and evaluations commissioned to external consultants.

6.14   The OIO reviewed each type of evaluation and the framework governing the evaluation function in the Secretariat. The OIO recommended that the OPCW evaluation policy and guidelines need to be either enhanced or developed in alignment with the latest edition of the UNEG Norms and Standards. There is also a need for incorporating good practices from other Divisions by engaging staff with programmatic experience from other operational units: for this, the OIO should organise training courses on evaluation techniques and processes for the staff members, with support from the Human Resources Branch, to build evaluation expertise in the Organisation. The OIO should also prepare evaluation tools (glossary, templates, questionnaires, checklists) which could be used by OPCW staff members involved in evaluation activities.

Confidentiality audits

Audit of the Developed Selection Methods for Schedule 3 Plant Sites (OIO/15/08)

6.15   The audit of Developed Selection Methods for Schedule 3 Plant Sites was conducted by the OIO during the period from November 2016 to February 2017. The audit covered the plant site selection (PSS) sessions held in the years 2014, 2015, and 2016. It focused on the methodology for the selection of Schedule 3 plant sites for inspection, related processes, and the algorithm in the PSS module of the Verification Information System (VIS).

6.16   In selecting Schedule 3 plant sites for inspection, the Secretariat complied with Council decision EC-XVII/DEC.7 (dated 1 December 1999), entitled "Methodology for Selecting Schedule 3 Plant Sites for Inspection", the formula of which was correctly represented in the algorithm of the PSS module in the VIS. The algorithm incorporated the requirement for equitable geographical distribution of inspections. The results of the random selections from the PSS module and incorporation of selected plant sites into the subsequent year's inspection plan provided evidence of the attainment of equitable geographical distribution in the selection of plant sites. Furthermore, the preparation, conduct, and completion of the PSS process complied with set procedures.

6.17   In order to further improve the PSS process, the OIO has made four main standard recommendations. Due to potential impacts on the PSS process, it is recommended that the VER enhance corroboration when analysing and identifying potential mixed plant sites. Accordingly, ongoing or regular data cleaning should be performed once reports on potential mixed sites have been generated. It is important to finalise the documentation of business process requirements relating to the accurate transfer of relevant site inspection histories in cases where a parent plant site is split into offshoot sites and where several sites are merged. The Data Analytics, Reporting and Quality Control Section (DARQ) should utilise this input to consider implementing enhancements in the VIS. To further positively impact the integrity of data used in the PSS, the Data Quality Management Framework developed should be implemented in full. DARQ should compile technical documentation for the PSS module and its algorithm. In addition, the Industry Verification Branch should finalise internal documented guidelines on the process of incorporating selections of Schedule 3 plant sites into the subsequent year's inspection plan.

6.18   The VER agreed with the recommendations and has begun to make progress on a number of the recommendations. The detailed responses are included in specific sections of this report.

Audit of the IT Change Management Process (OIO/17/01)

6.19   The IT change management process (ITCMP) is important as it is an inherently high-risk area that affects IT infrastructure and applications in the entire Organisation. Ineffective controls could result in a range of risks, including compromises in system security and functionalities, as well as operational disruptions.

6.20   The main objectives of the audit of the ITCMP were to assess the adequacy and effectiveness of the ITCMP, as well as security and management oversight regarding production programs. The audit scope covered the ITCMP in the IT infrastructure and applications for the period from January 2016 to April 2017.

6.21   It was noted that a number of controls had been implemented. Policies and procedures for the ITCMP, which are based on an internationally recognised Information Technology Infrastructure Library (ITIL) framework, are documented and applied in practice. In accordance with ITIL, a Change Advisory Board (CAB) provided an oversight role in respect of IT changes during the period under review. A module for

change management was included in the IT service management software, TOPdesk, which went live in June 2016. TOPdesk has enabled the recording, tracking, and reporting of change requests, thereby providing more transparency. The CAB held both regular and ad-hoc meetings to assess, authorise, and prioritise requested IT changes.

6.22 In order to further mature the ITCMP, the OIO made a total of eight recommendations (three critical and five standard). It was recommended that the Information Services Branch (ISB) ensure that policies and procedures for IT configuration management and release management are completed, as a precedent to the enhancement of the related processes and their overall integration in the ITCMP. In order to ensure that inter-dependencies among different items are fully taken into account during the change process, the configuration management database should be completed and a plan documented accordingly. To obtain assurance on the confidentiality of information on the ITCMP, which is hosted externally, the Office of Confidentiality and Security (OCS) should consider conducting a security risk assessment on TOPdesk. At the change initiation stage, there should be more rigorous verification of the appropriateness of change requesters and approvers. The ISB and DARQ should ensure that incompatible functions are appropriately segregated with regard to the testing and migration of programs into production environments. Rollback plans should be devised prior to implementing those changes that are expected to significantly impact business processes and/or the IT environment, in case unintended impacts materialise. The documentation of user acceptance test results should be a mandatory requirement, with the results attached to relevant change records. Finally, post-change evaluations should be performed and documented for those IT changes with significant impacts on business processes and/or the IT environment.

6.23 The recommendations in this report were discussed with members of the CAB, ISB, OCS, and DARQ. All parties agreed to implement the relevant recommendations in their respective areas.

Audit of the Implementation of the Secure Information Exchange System for the Electronic Transmission of Declarations (OIO/17/03)

6.24 The secure information exchange (SIX) system for the electronic transmission of declarations was set up to provide a secure channel for transmitting documents that contain confidential information between a State Party that has registered to use it and the Secretariat. The system was also expected to improve efficiency in the submission of declarations under Articles III and VI of the Convention and relevant parts of the Verification Annex, as well as in the processing of documents by the Secretariat. The SIX project was initiated in 2012 and launched in July 2014.

6.25 The main audit objectives of the audit of the implementation of the SIX system were to assess the adequacy and effectiveness of established procedures for the management of information, cryptographic keys and user accounts, compliance with procedures, and the adequacy and effectiveness of IT security measures. The audit scope covered the implementation of the SIX system during the period from July 2014 to July 2017.

6.26   In response to promotion initiatives taken by the Secretariat, the number of registered SIX system users has increased steadily since its launch. Accordingly, the initiatives have been supported by training courses and e-learning materials. There are effective controls to ensure that new user accounts are created only for authorised State Party representatives and access is discontinued for those users who no longer require it.

6.27   To support system users, the SIX User Manual provides comprehensive instructions on the initial set up of the encryption tool, the configuration of the State Party, the encryption keys of the Organisation, how to log in to the SIX internet portal, how to transmit and receive documents, and good practices for the management of cryptographic keys and use of encryption systems. DARQ provides first-line support to system users both during the set-up and operational phases. As a SIX system optimisation project commenced in 2017, DARQ initiated a review of the SIX User Manual. The revised manual will be made available to system users once changes that arise from use of the project have been implemented in the production environment.

6.28   The presence of the Head of DARQ and at least one authorised representative from the ISB and OCS is required during the generation of the Declarations Branch key pair (public-private pair) by the Key Management Administrator.

6.29   Encryption keys are managed through a key management server, which is a stand-alone secure server on the Security Critical Network (SCN). The private portion of the key is stored on a physically secured smart card. Access to the server, card reader, and card is limited to authorised individuals. Furthermore, the private portion of the key is stored with an administrator access code configured as a shared secret between the OCS and DARQ. The key management server chooses a recoverable code for retrieving the private key in case of loss of the administrator code. The specified encryption key length of 2048 bits has been assessed as sufficiently strong to cover the period from 2016 to 2030.

6.30   Additionally, the most recent technical risk assessment (in December 2016) indicated that the SIX system adequately mitigated several security risks, including two critical risks that have been consistently ranked in the top three tiers since the year 2007.

6.31   In order to mitigate risks identified during the audit, the OIO made the following eight recommendations (two critical and six standard):

(a)   The VER should define, in broad terms, a strategic direction on the future use of the SIX system. This should take into account potential uses, as well as the nature of acceptable changes in the use of the system. Relevant milestones should be clarified (standard).

(b)   The VER should facilitate the inclusion of a banner in the SIX system to alert users in advance to consider the justification for sending unclassified information (standard).

(c)   In 2018, the VER should conduct a survey of current and potential SIX system users to elicit feedback that would inform future system enhancement efforts and help resolve issues experienced by users (standard).

(d)   The OCS should commission a technical risk assessment exercise on the SIX system in 2018 (critical).

(e)   The ISB should conduct a review of the SIX system's architecture, with a view to incorporating redundancy. This would ensure that the system as a whole is protected from instances of a single point of failure (critical).

(f)   The ISB should identify the cause of delays in responsiveness of the SIX internet portal and encryption/decryption portal (standard).

(g)   DARQ should formalise a practice whereby at least two staff members initiate and approve a SIX user account creation form (standard).

(h)   The DRA and DARQ should collaborate in reviewing and potentially streamlining SIX procedures performed in the DRA (standard).

6.32   The recommendations in this report were discussed with the VER, ISB, and OCS. All parties agreed to implement the relevant recommendations in their respective areas.

6.33   Furthermore, the OIO will follow up on any additional recommendations arising from the conduct of a technical risk assessment of the system once the optimisation project has concluded in 2018.

Advisory Review of the Design of the Established Data Migration Process for the Unit4 Business World Enterprise Resource Planning System Project (OIO/17/05)

6.34   The OIO conducted an advisory review of the design of the established data migration process (DMP) in the Unit4 Business World ERP system project. Consistent with the IIA's International Standards for the Professional Practice of Internal Auditing relating to acceptance of consulting services, the OIO accepted the recommendation of the External Auditor to conduct a review of the DMP in the ERP project. Accordingly, the review was included in the annual programme of work for 2017 and was conducted from December 2017 to January 2018.

6.35   The scope of the DMP review included all source systems in the designated system of records.

6.36   The OIO proposed six recommended actions to be considered by the ERP Project Board, the ERP Project Steering Committee, the Project Manager, and data migration specialists.

6.37 The recommended actions were intended to facilitate proactive mitigations to help improve the success of the DMP, and involved:

(a) updating and finalising the data migration strategy document;

(b) requiring business process owners to sign off on actions related to data profiling, validation, and migration;

(c) reviewing, updating, and monitoring data migration risks within the main project risk register;

(d) the use of a data analytics tool for verifying the completeness and accuracy of the source data loaded into the production environment of the ERP system;

(e) the use of a data quality monitoring tool for the purpose of monitoring the quality of data in the ERP system for a specified period in the post go-live period; and

(f) finalising decisions on the timing of decommissioning legacy systems relative to the go-live date.

Evaluation

Evaluation of the Activities of the External Relations Division (OIO/17/06)

6.38 The evaluation of the activities of the External Relations Division (ERD) was conducted as part of the OIO's annual programme of work for 2017 and covered the activities from 2014 to 2017. The main objectives of this engagement were to review the process of planning, monitoring, and evaluating ERD activities; to assess the relevance and adequacy of procedures and practices within the Division; and to identify opportunities to improve the efficiency of activities and implement lessons learned.

6.39 Review and analysis of the programmes, activities, and achievements revealed that the management of programmes and activities can be further improved by strengthening planning and programming of activities to effectively monitor and measure performance, as well as by updating existing procedures.

6.40 For the last 17 years, the number of States Parties to the Convention has increased from 128 to 192. This increase has been presented for many years as an achievement and significant progress towards meeting one of the main objectives related to the ERD's work. As there are only four States not Party left, universality has become a lower priority for the Political Affairs and Protocol Branch (PPB). Given the progress made on universality, the ERD should look at ways of restructuring its work to utilise all resources available in the most effective ways possible, devising and implementing strategies to this end.

6.41 A number of good practices have been identified within the ERD, including organisation of successful campaigns and events, standardisation of the OPCW image,

and use of dedicated microsites. The planning process appeared to be based mainly on the Programme and Budget process, which has left little opportunity so far to reflect strategic guidance.

6.42   As a result of this evaluation, seven recommendations have been issued. The one critical recommendation relates to the need for strengthening the RBM framework, showing a clear link between objectives, strategies, activities, and resources, particularly in the PPB.

6.43   The six standard recommendations aim at strengthening monitoring, the evaluation of activities, and communication channels both within and outside the ERD. The OIO also recommends improving the allocation of human resources for large events organised by the ERD and reinforcing training opportunities for ERD staff in the most undertrained areas. In addition, the ERD should update its operational quality system documentation, to include current practice.

QMS audits

Organisation of the OPCW Central Analytical Database and On-site Databases and Preparation and Testing of Gas Chromatography-Mass Spectrometry Inspection Equipment (QS/17/01)

6.44   Both processes of the organisation of the OCAD and on-site databases and preparation and testing of GC-MS inspection equipment are well established, with strong controls in place, working adequately and efficiently. The audit team reviewed the applicable QMS procedures.

6.45   The documentation was found to be complete and in compliance with the requirements described in the relevant QMS documents and ISO/IEC 17025:2005. The audit team appreciates the commitment of the OPCW Laboratory to make continuous improvements.

6.46   The RvA conducted a two day reassessment within the scope of this audit (Ref: L338/PT011) in October 2016. As a result, three small non-conformities were identified. Corrective actions have been taken by the Laboratory and the OIO, and the assessors accepted the proposed solutions.

6.47   The auditors issued two new observations relating to the existing complaints and appeals procedure and to reconsideration of the applicability of (parts of) annexes to the Laboratory Quality Manual. In addition, the audit team accepted corrective actions taken by the OPCW Laboratory to address the audit findings from previous engagements.

Organisation of OPCW Proficiency Tests (QS/17/02)

6.48   The audit team reviewed the applicable QMS procedures. The available records were sampled, based on professional judgement. As a result, the Thirty-Ninth Proficiency Test was selected for a more detailed analysis. In addition, a detailed checklist was prepared.

6.49   The audit team arrived at the conclusion that the process of the organisation of the proficiency tests was adequate and efficient. The maturity of the process, which has been conducted for many years, and the quality of existing controls in place guarantee compliance with the requirements described in the relevant QMS documents and ISO/IEC 17043:2010.

6.50   The auditors also noted the continuous efforts by the OPCW Laboratory to improve the proficiency testing process, taking into account feedback received from various customers, namely, the RvA, evaluating and participating laboratories, OPCW Laboratory staff members, and internal auditors.

6.51   As a result of the audit, no non-conformities were identified. The audit team formulated two observations and one suggestion for improvement. Both observations proposed including clear reference in the existing proficiency testing procedures to the QMS document (QDOC) (QDOC/SOP/OIO/005) managing complaints, appeals, and corrective actions within the Secretariat. The suggestion for improvement is related to communication with participating laboratories.

6.52   Furthermore, the audit team followed up on findings from previous engagements. As a result, the suggestion for improvement, which concerns the gathering of feedback from proficiency test customers, could be considered as closed.

6.53   The audit team decided to keep open the suggestion for improvement related to the training plan. The text has been slightly redrafted.

Management of the Quality Management System Document Central Registry and Control of Quality Management System Documents (QS/17/03)

6.54   The audit proceeded as planned. The audit team reviewed the applicable QMS procedures, concentrating on the SOP for "Quality Management System Documentation" (QDOC/ODG/SOP/001) and WI for "Uploading Quality Management System Documents" (QDOC/DEB/WI/001). A dedicated checklist was prepared. In addition, the audit team obtained the list of document controllers and the list of outdated documents during the preliminary review process of this audit. During the audit, the auditors randomly selected a QDOC for performing a walk-through test, and checked whether reminders had been sent to document controllers and process owners.

6.55   The audit team arrived at the conclusion that the process of management of the QDOC Central Registry and control of QDOCs is working properly. The auditors did not come across any serious non-compliance or any other systematic error.

6.56   The auditors also noted the attempts of the DRA to improve the documents and records management system by sending regular updates to all organisational units on revised QDOCs.

6.57   The audit team followed up on the QMSTC requirements presented in its meeting of 12 December 2016 regarding the suggestion to send automatic reminders for outdated QDOCs. In this respect, the DRA informed the audit team that reminders regarding

out of date QDOCs are sent approximately every four months and that the current system does not have the capability to send automatic reminders.

6.58   Furthermore, the audit team followed up on the findings of audit QS/16/3. The observation issued in 2016, which is related to the list of document controllers, remains relevant and requires further action by the DRA. The audit team noted that only fixed-term staff have been appointed as document controllers, as suggested during the QMSTC meeting held on 12 December 2016. The observation remains open but the text has been slightly redrafted. The two suggestions for improvement were closed.

6.59   Additionally, the audit team formulated two new observations. The first one proposed transferring the ownership of the QDOC/ODG/SOP/001 to the DRA, which would allow for the proper improvement of the system. The second one is related to the migration of the QDOCs from Lotus Notes to SharePoint, with the ISB's assistance.

Certification of the OPCW Central Analytical Database and On-Site Databases and Certification of Testing, Preparing, and Packing of Gas Chromatography-Mass Spectrometry Inspection Equipment (QS/17/04)

6.60   The audit was conducted in accordance with the annual programme of work for 2017, in a professional atmosphere. A detailed audit checklist was used to steer the interview. All documents requested were provided within the timeframe agreed. Overall, the audit team was satisfied that the audited processes provided reasonable assurance of product quality.

6.61   No non-conformities were found during the audit. The audit team had four suggestions, which were related to archiving, destruction of documents, file maintenance, and requests for certification in emergency situations, and identified ad hoc initiatives.

Management Requirements: Handling of Complaints, Control of Non-Conformities and Related Corrective Actions and Management Review Process (QS/17/05).

6.62   The audit proceeded as planned. In addition to the audit plan, the Lead Auditor provided the auditee with the draft QMS checklist, which was used as the basis for the audit. The auditee was very cooperative during audit preparations as well as during the interviews and discussions. All requests for additional information and documentation were addressed by the auditee in a timely and efficient manner.

6.63   The audit team noted that the OIO has successfully managed to maintain the RvA accreditation for the relevant units of the OPCW (the Laboratory, OIO, and DRA).

6.64   To achieve the audit objectives, the audit team examined the four QMS SOPs and the Quality Manual, as well as a number of other relevant documents, including the minutes of the latest QMSTC meeting and the report on the latest satisfaction survey.

6.65   Similarly to the 2016 audit QS/16/5, the audit team followed up on the QMSTC requirements (outlined in paragraph 9.1 of QDOC/OIO/SOP/002) to conduct

management reviews on items listed on the agenda, including the development of a long-term plan, and on how strategic issues are handled within the QMS. The audit team noted that a number of steps have been taken to address those issues, including the holding of management reviews by the DRA, as well as by the QMSTC in 2016.

6.66   Furthermore, the audit team followed up on the 2016 QS/16/5's three observations and one suggestion for improvement. Two of the observations and the suggestion remain relevant and require further action by the OIO.

6.67   One of the previous observations, regarding the need to formalise the QMSTC decision not to integrate ISO 9001:2015 into the OPCW QMS, could be considered as closed. The audit team noted that the amended Quality Policy Statement issued on 20 January 2017 removed the reference to ISO 9001:2015, which may be viewed as an action that formalises the aforementioned QMSTC decision.

6.68   In addition to previous observations and suggestions, the audit team formulated three new observations and two suggestions. These concern the need to hold regular QMS reviews outside the OIO, to set deadlines for the QMSTC decisions, to inform customers about the complaint procedures, and to bring improvements to the satisfaction surveys.

Organisation of OPCW Biomedical Proficiency Tests (QS/17/06)

6.69   The Secretariat successfully conducted the second BioPT and achieved its objective to create a network of designated laboratories for the analysis of biomedical samples for off-site analysis. In total, 25 laboratories (nominated by 20 Member States) participated in the test. Two laboratories performed the test on a trial basis.

6.70   The OPCW Laboratory outsourced the organisation of sample preparation and evaluation of results to two provisionally designated laboratories. The auditors also assessed these activities against relevant clauses of ISO/IEC 17043:2010.

6.71   The audit team reviewed the applicable QMS procedures. In addition, a detailed checklist was prepared. The auditors arrived at the conclusion that the process of the organisation of the second BioPT was adequate and efficient.

6.72   Despite having conducted the BioPT for the second time, the OPCW Laboratory has already shown its willingness to further improve the process. Different meetings with other laboratories have been scheduled regularly. All comments were discussed and taken into account while planning for future improvements to the system.

6.73   The audit team came to the conclusion that the QMS system within the BioPT is working properly and needs only some further adjustments. Auditors found evidence of effective and efficient operations within the BioPT process. Services required by the participants have been identified and are provided. The Laboratory has also coped well with a challenging period involving a significant increase of work related to the preparation for the scope extension of ISO 17043:2010. Clear efforts have also been made to strengthen the feedback mechanism.

6.74   As a result of the audit, 10 findings were identified, including one minor non-conformity (Category B). Recommendations should be viewed as a tool to introduce improvements to the existing QMS.

6.75   Furthermore, the audit team followed up on the previous audit (QS/16/6) findings, in particular three observations and two suggestions for improvement. The audit team examined the latest version of QDOC/LAB/SOP/BioPT01, issued on 28 December 2016, and noted that the necessary reference (concerning complaints, appeals procedure, and corrective actions) to QDOC/SOP/OIO/005 was included in the aforementioned QDOC/LAB/SOP/BioPT01. Therefore, all three observations of audit QS/16/6 can be considered as closed. In addition, the audit team noted that paragraph 29.6 of the latest version of QDOC/LAB/SOP/BioPT01 better reflects the requirements of paragraph 4.10 of ISO 17043:2010 concerning the existing policy and procedures in respect of the confidentiality regime. Therefore, all three observations of audit QS/16/6 can be considered as closed.

6.76   Concerning the two suggestions for improvement issued in 2016, the auditors recommended gathering all records related to competence of employees of the Laboratory in one place. During this audit, all records requested by the auditors were presented to the audit team. However, the auditors wish to keep the recommendation open. The text has been slightly changed and is included in Suggestion for Improvement 7.

6.77   In addition, the auditors also suggested updating existing procedures communicating changes in programme design and operation. The audit team positively assessed changes made in QDOC/LAB/SOP/BioPT01. Thus, Suggestion for Improvement 2 could be closed.

Other assignments

6.78   In 2017, the OIO prepared a briefing on the different approaches for the setting up of an audit committee, for the ABAF's consideration. A briefing by the Director of Internal Oversight of the International Atomic Energy Agency (IAEA) was also arranged. The ABAF expressed appreciation for the work done by OIO on this presentation and noted that the issue remained a complex one. The ABAF noted that its members function independently in their individual capacity, and expressed reservations about setting up another layer with additional costs for the Organisation but without significant added value. The ABAF recommended that further work was required before it could make an informed recommendation to the Council.

7.   STATUS OF IMPLEMENTATION OF AUDIT AND EVALUATION RECOMMENDATIONS

7.1   The International Professional Practices Framework for internal auditing issued by the IIA (United States of America) requires "a follow-up process to monitor and ensure that management actions have been effectively implemented". The annual programme of work of the OIO includes provision for such follow-up. The OIO has set up an Excel-based tool designed to enable managers to report action taken on the status of

implementation of audit recommendations, and desk reviews are performed by the OIO in consultation with managers on actions taken to address them.

7.2   In addition, the OIO maintains regular contacts with Directors and Branch Heads to assist them in finding the best way to implement pending recommendations. The Office has included in the follow-up exercise a clear description of what is expected from units and managers to address each recommendation.

7.3   During the year 2017, 24 recommendations (including seven critical) were implemented by the Secretariat. Of the 262[4] audit and evaluation recommendations issued between 2012 and 2017, 202 were implemented, bringing the cumulative rate of implementation of OIO recommendations to 77.1% as at 31 December 2017, compared to 84.2% as at 31 December 2016.

7.4   The total number of recommendations for which implementation was pending as at 31 December 2017 was 60. A yearly breakdown is provided in Appendix 2.

7.5   The status of the recommendations issued and implemented from 2012 to 2017 is presented in Table 1 below.

TABLE 1:   STATUS   OF   IMPLEMENTATION   OF   OIO RECOMMENDATIONS FROM 2012 TO 2017

	OIO Recommendations				
Year	**Opening balance (A)**	**Issued during year (B)**	**Total** **C = (A) + (B)**	**Implemented: Cumulative (D)**	**Closing Balance E = C - D**
2012	75	82	157	85	72
2013	72	44	116	58	58
2014	58	40	98	28	70
2015	70	27	97	51	46
2016	46	27	73	21	52
2017	52	32[5]	84	24	60

7.6   Reports on the status of implementation of recommendations were submitted to the Director-General and the Management Board on a quarterly basis. As in previous years, the Director-General paid close attention to this matter and instructed the programme managers concerned to expedite the implementation of pending recommendations.

8.   IMPACT OF IMPLEMENTED AUDIT AND EVALUATION RECOMMENDATIONS

8.1   Of the 24 recommendations closed in 2017, two related to internal audit reports, 19 to confidentiality audit reports, and three to evaluation reports.

---

4   Including 10 recommendations contained in one pending audit report of 2011.

5   Includes recommendations contained only in the four audit reports issued up to December 2017, which have become due for implementation.

8.2   The OIO conducted an assessment of the impact of its recommendations implemented during the year. They contributed significantly to adding value to the Organisation by enhancing compliance with existing regulations and procedures, strengthening internal controls, and improving the allocation of resources and the effectiveness of programmes and policies.

8.3   The OIO closed two internal audit recommendations in 2017. In its report on the OPCW budget process, it was recommended that the Budget and Finance Branch should consider issuing an annual internal memo on the performance of the budget process in the previous year.   The recommendation was implemented; the performance in terms of the budget process in the previous year is now being reported to the Deputy-Director-General each year. Implementation of this recommendation has enhanced the OPCW budget process.

8.4   An audit recommendation contained in the report on procurement systems was also closed. As a result, the system of "regularisation" of irregular procurement cases has been dispensed with and the system of emergency procurement and ex-post facto/retroactive approvals has now been introduced in the applicable administrative directive.

8.5   The OIO closed 19 audit recommendations arising from confidentiality audits, out of which five were rated "critical" and 14 were rated "standard". The relevant recommendations were issued in the following audits: IT Infrastructure in the OPCW Laboratory; Manpower Planning in the Inspectorate Division; Developed Selection Methods for Schedule 3 Plant Sites; and the IT Change Management Process.

8.6   Four recommendations that arose from the audit of IT Infrastructure in the OPCW Laboratory were closed in 2017. In response to the recommendation for the OCS to coordinate periodic vulnerability assessments in the Secretariat, the OCS began to conduct regular vulnerability scans on the Security Non-Critical Network (SNCN) beginning in the first quarter of 2017. This has improved the identification, prioritisation, and remediation of vulnerabilities in the information systems. Through a review of successive vulnerability assessment reports, the resolution or otherwise of identified vulnerabilities is more easily tracked. Corrective actions can be planned based on informed analysis. This minimises the potential for vulnerabilities to be exploited by unauthorised parties. Should such an attempt still succeed, timely awareness of existing vulnerabilities enables the OPCW to respond quickly.

8.7   It was recommended that the ISB, in liaison with the Head of the OPCW Laboratory, should consider securing administrator event logs in the OCAD in a separate log server, away from the administrator's access. This was implemented in the new OCAD, version 20_2018, which was released in January 2018. Thus, all changes made to the OCAD could be tracked with full confidence in the integrity of the related database logs.

8.8   Another closed recommendation was for the OPCW Laboratory to define required retention periods for data held in its shared network folders. Subsequently, an internal memorandum entitled "The procedures for the control of quality records of the

OPCW Laboratory Quality Management System" (QDOC/LAB/QR/D012/Rev.11, dated 17 January 2017) was issued. This has had the effect of reducing both the risk of undesirable destruction of information and the continued storage of outdated information and/or documents.

8.9   Furthermore, the OIO recommended that the OCS recirculate the SNCN Active Directory Access Assessment Matrix to all Divisions, including the OPCW Laboratory, in order to enhance controls over OPCW network user accounts. Thus, periodic validation of user access rights on the SNCN was restarted in 2017. Directors and Branch Heads are prompted to update the matrix of authorised users of information systems and to ensure that the access rights of authorised users are aligned with their job roles. In addition, users who no longer need access are identified and removed, thereby securing the OPCW from abuse of unauthorised user accounts.

8.10   The OIO closed nine recommendations arising from the audit of Manpower Planning in the Inspectorate Division. The first closed recommendation required the Operations and Planning Branch to ensure that all mission planning checklists were completed in full. This was rectified, as a mechanism was implemented to ensure that inspection team leaders routinely completed all planning checklists, thereby improving compliance with mission planning procedures.

8.11   A second recommendation was for the Head of the Capacity-Building and Contingency-Planning Cell (Inspectorate Division (INS)) to assess and continue to monitor the impact on the integrity and effectiveness of the training programmes of changes arising from the rationalisation of training costs for inspectors. In response, the Head of the Capacity-Building and Contingency-Planning Cell continued to monitor the impact of rationalising training costs on training programmes. Although costs were reduced, as reflected in the 2018 budget for the INS, the effectiveness of training offered to inspectors was maintained.

8.12   The INS introduced a revised calculation methodology in 2017 for the number of inspectors and distribution of inspector specialisms, to address the following three recommendations: mission-planning coordinators should align deployment of inspectors with the working schedules for inspectors, within justifiable deviations; uneven utilisation of inspectors should be smoothened as much as possible to optimise the utilisation of inspectors; and inspector head counts in each specialism should be gradually realigned with each specialism's relative requirements. To support the revised calculation methodology, a corresponding new WI was prepared. This provides full transparency regarding the calculation of the number of inspectors required and aligns the calculated number of inspectors with the actual identified needs. The parameters used in the WI were followed by mission planners in the implementation of the 2017 inspection plan and will also be implemented going forward. This will optimise the utilisation of inspector human resources and ultimately the effectiveness of inspections. In order to further realign the number of inspectors according to specialisms, the same calculation methodology was used as the basis for the recruitment of the Group Q inspectors in October 2017. That recruitment covered only two specialisms that required replacement. The realignment

of the number of inspectors per specialism will continue to be applied in future recruitments of inspectors, thus ensuring the best composition of the workforce according to mission's needs and other requirements, and reducing imbalances in the deployment of inspectors.

8.13　Two further recommendations involved the update of the working schedules for inspectors to take into account lessons learned in inspector deployment practices over 20 years, as well as to monitor compliance with the specified maximum number of days per deployment and, if this was found to be insufficient, propose a revised limit. The recommendations were addressed through the INS adopting 135 days out per year as a limit to deploying inspectors on missions. This was based on 20 years of health monitoring of inspectors. The adopted maximum is to be incorporated in an SOP to calculate the number of inspectors required to conduct Article IV and V inspections. This will minimise the accumulation of unusually high numbers of days out for a particular group of inspectors and benefit their well-being. A reduction in disparities in the number of days out for inspectors complements the objective of reducing, as much as possible, uneven utilisation of inspectors.

8.14　It was also recommended that the INS should propose measures to reduce the possibility of failure to deploy inspectors recruited under special services agreement (SSA) contracts due to lack of clearance received from some States Parties. In response, the INS put in place a formal procedure to check whether any SSA contractor may be subject to a possible rejection by a State Party. The mechanism would involve conducting an assessment of the contractor's past experience with the State Party to which he or she may be deployed, and the political problems between the SSA contractor's country of origin and the inspected State Party, among other possible actions.

8.15　With regard to the recommendation for the Health and Safety Branch to consider the sufficiency of annual medical testing of inspectors, the Branch responded by affirming that medical testing of inspectors was being performed without fail, according to schedule, in compliance with the testing regime. Where there are underlying conditions, additional tests were also being conducted. Additional follow up is also done for all inspectors who are about to reach the maximum threshold of days out on mission.

8.16　During the audit of Developed Selection Methods for Schedule 3 Plant Sites, the OIO recommended that the VER enhance corroboration in the process of identifying and analysing potential mixed plant sites; perform ongoing or regular data cleaning for potential mixed plant sites; and facilitate the sharing of an administrative window in the VIS across the relevant Branches. The VER completed the initial process of identifying potential mixed plant sites. Shared access was provided across Branches in the Division to enable continuous review and update of mixed plant site data. This has improved the integrity of data used in the PSS process and reduced the need to perform extensive post-selection checks. Correspondingly, the efficiency in the selection of Schedule 3 plant sites for inspection will improve.

8.17   The OIO closed five recommendations from the audit of the IT Change Management Process. In order to enhance the control for change requests to be approved by business process owners, an enhancement was implemented in the service management system, TOPdesk: an approval of the manager or his/her alternate is explicitly requested in the change request forms. This will minimise the risk of unauthorised changes being implemented.

8.18   The OIO recommended the implementation of a mandatory requirement for user acceptance testing (UAT) results to be documented and attached to relevant change records. Since September 2017, the Change Manager on the Change Advisory Board (CAB) implemented a mandatory requirement for UAT results to be documented and attached to relevant change records in the service management system, TOPdesk. The template for executing, testing, and documenting a change in TOPdesk was updated to require the upload of UAT results. A change is planned for a CAB meeting, and thus for deployment, only if the relevant UAT results have been uploaded to TOPdesk, except in rare cases. For those exceptional circumstances, a mandatory post change evaluation is performed. This ensures that changes implemented in the IT environment are in accordance with user requests and address the underlying issues.

8.19   The OIO recommended that rollback plans should be devised prior to implementing changes that are expected to significantly impact business processes and/or the IT environment. Following this, the CAB approved an amendment of the procedures to require that a rollback plan be described prior to implementing such changes. This amendment became effective in September 2017. The template for executing, testing, and documenting a change in TOPdesk was updated to reflect the mandatory description of a rollback plan. As a consequence, should a change result in unintended effects, it is then possible to follow a rollback plan to restore the IT environment to its original state prior to the implementation of the change, thus improving the stability of IT operations during the change process.

8.20   Following the recommendation for post-change evaluations of IT changes with significant impacts on business processes and/or the IT environment to be performed, all such extensive changes are now flagged in TOPdesk so that the CAB can conduct post-change evaluations of them. The result is greater appreciation of the full impacts of changes implemented.

8.21   The OIO also recommended that a security risk assessment be conducted on TOPdesk with respect to hosted OPCW information. In this regard, assurance regarding the security of OPCW information uploaded to TOPdesk was provided through an on-site inspection of the facility at which TOPdesk is hosted. The result of the risk assessment with respect to the confidentiality, integrity, and availability of OPCW information was a residual risk of "low".

8.22   As regards evaluation reports, three (standard) evaluation recommendations were closed in 2017. A review of the results of the closed recommendations revealed that they contributed significantly to improving the programme of work and the management of resources within the units in question. The OIO acknowledges the establishment of the knowledge management project, resulting in an endorsed

strategic framework and the hiring of a Knowledge Officer in the VER. In addition, a network of "knowledge management champions" within each Division was created to establish cultural change alongside tenure and technical-skills sharing.

8.23   Following an OIO recommendation, the Conference Services Unit established a fit-for-purpose evaluation mechanism, including a lessons learned database in which all feedback can be logged, action agents assigned, and tracked to closure. Currently, the lessons-learned logs for sessions of the Council and Conference are updated within two weeks of the closure of each session.

9.   ADVISORY SERVICES

9.1   In accordance with the requirements of OPCW Financial Rule 12.3.01, the OIO ensured its operational independence and reported to the Director-General on the adequacy and effectiveness of the systems of internal control in place in the Secretariat. The Director of the OIO held regular meetings with the Director-General on this matter. In accordance with Financial Regulation 12.1, the Office assisted the Director-General in the management of the OPCW's resources in order to enhance the efficiency and economy of OPCW operations. The Director of the OIO participated in the meetings of the Directors and Management Board.

9.2   The OIO continued to receive requests for advice and comments in 2017 related, among other issues, to the revision of administrative directives, the improvement of internal controls, risk assessment, confidentiality policy, and IT governance.

9.3   The OIO staff members participated as advisers or observers in meetings of the Investment Committee, the Property Survey Board, the Committee on Contracts (COC), the Information Services Steering Committee (ISSC), the ERP Project Board, the ERP Working Group on Financial Rules and Regulations, and the Risk Management Working Group. The fact that the Management frequently consults the OIO for advice reflects the key role that the Office plays in the Secretariat.

9.4   The Senior Confidentiality Auditor attended, as an observer, two meetings of the IT Strategy Advisory Committee, five meetings of the IT Steering Committee, and one meeting of the VER IT Steering Committee.

9.5   The Senior Internal Auditor attended, as an observer, 14 meetings of the COC in 2017 to review the cases submitted to the Committee and provide advice to the Director-General on procurement issues. He also attended seven meetings of the Investment Committee, one meeting of the Property Survey Board, two meetings of the Risk Management Working Group, and several meetings of the Financial Regulations and Rules Working Group.

9.6   Throughout the year, the OIO provided information, upon request, to members of the ABAF during their meetings and to delegates from States Parties during informal consultations held by the facilitator for administrative and financial matters.

10. CERTIFICATION OF THE OPCW CENTRAL ANALYTICAL DATABASE AND INSPECTION EQUIPMENT

10.1 The OIO continued to provide assurance for the testing, preparing, and packing of inspection equipment for sampling missions in accordance with Council decision EC-62/DEC.3 (dated 6 October 2010).

10.2 At the request of the OPCW Laboratory, in 2017 the OIO issued 11 certificates for the GC-MS inspection equipment and 19 certificates for the OCAD (version 20) for 2018.

11. EXTERNAL RELATIONS

Representatives of Internal Audit Services of the United Nations and Other International Organizations

11.1 In August 2017, the OIO hosted, for the first time, the annual meeting of the Representatives of Internal Audit Services (RIAS) of United Nations organisations and multilateral financial institutions and other associated intergovernmental organisations. The meeting was attended by 82 participants from 44 organisations. The mission of RIAS is "to strengthen internal auditing practices and professionalism by providing a forum for development of methodologies and their related innovation, promoting and supporting independence, collaboration and common positions of its members to add value to their organisations".

11.2 Many subjects were discussed at the meeting, including big data analytics, auditing organisational culture, financial audits, IT security audits, the role of the internal audit function in the implementation of sustainable development goals, enterprise architecture, the use of social media to transform internal audits, cyber security, innovation and creativity in internal audit, collaborating better with other oversight functions, management self-disclosure within the audit process, and global trends in internal auditing.

11.3 The OIO conducted a survey of the RIAS participants to seek their feedback on the deliberations and the arrangements for the conference. The overall satisfaction rate was 95% and several participants commented that the organisation, arrangements, facilities, social events, conference programme, and presentations were outstanding, and that this was one of the most systematically organised RIAS events.

United Nations Evaluation Group

11.4 The Senior Evaluator and Quality Assurance Officer participated in the annual general meeting (AGM) of UNEG (its decision-making body) in Vienna, Austria, in May 2017. UNEG is an interagency professional network that brings together the evaluation units of the United Nations system, including United Nations departments, specialised agencies, funds and programmes, and affiliated organisations. It currently has 46 members and observers. The OIO is a full member of UNEG, representing the OPCW at AGMs.

ISACA

11.5   In May 2017, the Senior Confidentiality Auditor attended the annual ISACA conference for Europe, which was held in Munich, Germany. Sessions presented at the conference included: Data Analytics; Auditing the Digital Enterprise; Machine Learning; "Internet of Things" and Artificial Intelligence: New Threats and Mitigations; Enterprise Risk Management Frameworks; IT Security, including cyber security; Cryptography; Auditing IT Service Management; Top Privacy Risks in Web Applications; The Nature and Management of Shadow IT; ISO 27001:2013 – Statement of Applicability; Risk Driven Control Approach to General Data Protection Regulation; and Implementing COBIT 5.

Meeting of OPCW, IAEA, and CTBTO[6] internal oversight services

11.6   In 2017, the OIO took the initiative to organise, for the first time, a meeting of the internal audit and evaluation services of the three organisations dealing with disarmament. Several good practices were shared among these organisations, such as those relating to key performance indicators, use of audit management software, IT auditing tools, auditing practices to detect fraud, whistle-blowing policies, auditing ERP systems, and techniques and methodologies for centralised evaluations, which helped to strengthen and improve the OIO's internal audit and evaluation policies and procedures.

Meeting of OPCW – ICC[7] oversight services

11.7   The first OPCW – ICC oversight services annual meeting took place on 5 April 2017 at the OPCW Headquarters. This mechanism is intended to share experiences and relevant information between the two audit teams. The subjects discussed included the role of the Audit Committee at the ICC; latest techniques in auditing and evaluation; recent developments in audit software; oversight of the SIC; auditing fraud; whistle-blowing policies; key performance indicators for oversight offices; structure and content of oversight annual reports; and cooperation between the two offices for the RIAS 2017 meeting at the OPCW Headquarters.

The Hague Evaluation Network

11.8   The Hague Evaluation Network was established in 2017. It creates a local space for those interested in sharing evaluation-related experiences in an international environment. Several meetings were organised to present an innovative evaluation concept by evaluation practitioners, commissioners, and instructors from various contexts: international organisations based mainly in The Hague, the Government of the Netherlands, and independent consultants. The OIO acts as a full member of that network.

---

[6]   CTBTO = Comprehensive Nuclear Test Ban Treaty Organisation.

[7]   ICC = International Criminal Court.

NATO Sorbonne Conference

11.9   On 4 October 2017, the Director of the OIO participated in the "External Audit, Performance and Risk Management in International Organizations" conference, a joint initiative by the International Board of Auditors for NATO (IBAN) and the Université Paris 1 – Panthéon-Sorbonne, which took place at the Cour des Comptes in Paris, France. The programme of the conference included discussions on the role of audit for a better governance, as well as panels on "performance" and "risk" as universal concepts for management and auditors; financial management and audit committees; the challenges for the measurement of performance; effective follow-up of recommendations; and drivers for improvement in international organisations.

Alberto E. Dojas
Director, Office of Internal Oversight

Appendix 1

KEY PERFORMANCE INDICTORS IN 2017

PROGRAMME: EXECUTIVE MANAGEMENT – OFFICE OF INTERNAL OVERSIGHT

Primary Alignment to Core Objective(s):	*Core objective 7: Full, effective, and non-discriminatory implementation of all provisions of the Convention by the OPCW*

OPCW Programme Objectives	Key Performance Indicators	Target for 2017	Results Achieved	Explanation of Variances
1. Effective oversight of the OPCW policy and programme management.	1.1 Ratio of coverage of identified risks	71.4%	75%	Coverage was as defined in the OIO annual programme of work
	1.2 Rate of implementation of the total recommendations of the OIO	85%	77.1%	Increase in the number of recommendations issued in 2017, and a longer timeline required to implement systemic recommendations of past years.
	1.3 Absence of non-conformities with applicable ISO standards	100%	100%	N/A
	1.4 Percentage of acceptance of OIO advice by Management	95%	100%	All of the recommendations issued in audit reports in 2017 were accepted by the Director-General.

Appendix 2

**NUMBER OF OUTSTANDING AUDIT AND EVALUATION
RECOMMENDATIONS BY YEAR**

Year	Number of Pending Recommendations
2011	1
2012	1
2013	0
2014	1
2015	21
2016	11
2017	25
Total	**60**
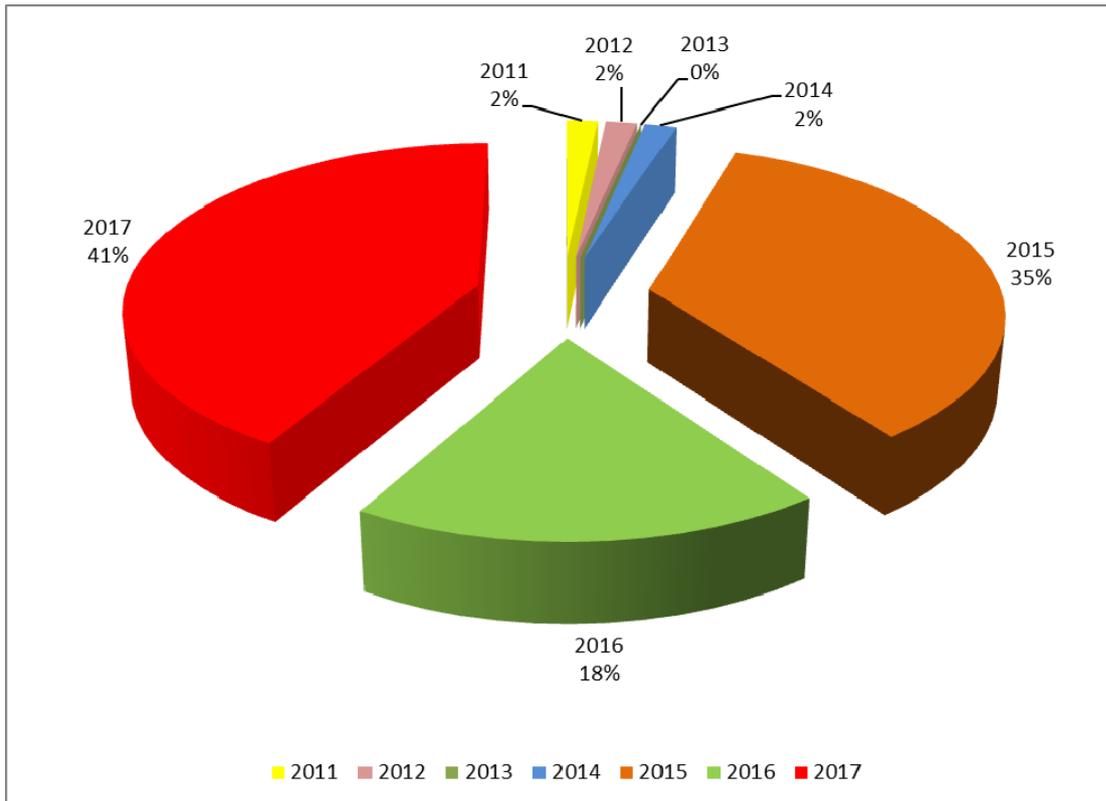
Appendix 3

**CRITICAL RECOMMENDATIONS MADE IN PREVIOUS REPORTS
ON WHICH CORRECTIVE ACTION HAS NOT BEEN COMPLETED**

**Audit report number OIO/15/02: Evaluation of Outreach Activities Conducted
in the International Cooperation and Assistance Division**

1. Develop a high-level guidance document for the International Cooperation and Assistance Division (ICA), which clearly describes the ends (goals, objectives) and how they will be achieved by the means (resources) allocated to the ICA, as well as the evaluation and impact assessment mechanisms to be used.

2. Establish a suitable evaluation mechanism (applied to all ICA outreach activities) which would define:

   • Areas and activities to be evaluated,
   • Type, purpose, and use of data to be collected,
   • Frequency, form, and audience of reporting,
   • Monitoring of implementation of recommendations (lessons learned),
   • Link of performance with costs,
   • Deadlines and responsibilities for evaluation activities.

Audit report number OIO/15/03: Audit of IT Business Continuity

3. Establish a mechanism for performing a business impact analysis.

4. Copy of the SCN (and other confidential or sensitive information) backup media should be transferred and kept on the disaster recovery location (DRL) for the purpose of minimising the risk of losing the data forever in the case of a major disaster. Evidence of finalised plan on SCN backup media on a DRL to be provided.

5. SCN data written on the backup media should be properly encrypted. Provide evidence of completed test for the encryption of SCN data written on the backup media on the DRL.

6. Update QDOC/ISB/SOP/001 to cover recovery strategies for both the SCN and SNCN. This plan should include the development and implementation of a so-called "hot site" with all the necessary network and IT equipment already in place on the premises of the DRL.

7. The ISSC should take a leading role in establishing and conducting a business continuity management process for the whole Organisation; these should also become a part of the ISSC's terms of reference and agenda.

8. Improve security at Rijswijk by implementing 24 hour physical security and improving video surveillance. In order to maintain the necessary level of confidentiality of the data in the DRL, the same level of physical security measures as those currently implemented in OPCW Headquarters has to be implemented at Rijswijk.

9.   Improve technical security at Rijswijk through an independent power supply system as well as an actual server room with the necessary environmental conditions.

Audit report number OIO/15/05: Audit of Risk Management

10.   Finalise risk management framework.

Audit report number OIO/16/01:   Audit of IT Infrastructure in the OPCW Laboratory

11.   Finalise update of the Information Security Policy in alignment with the current ISO/IEC 27002:2013 "Information Technology – Security Techniques – Code of Practice for Information Security Management".

Audit report number OIO/16/03: Audit of OPCW Governance of the Evaluation Function in the Secretariat

12.   Update the evaluation policy.

Audit report number OIO/17/01: IT Change Management Process

13.   Document a plan for the completion of the configuration management database, incorporating required resources and related milestones.

14.   Update the SOP for release management with procedures for ensuring that developers do not test and migrate own programs.

Audit report number OIO/17/02: Audit of Procurement Systems

15.   Develop an appropriate procurement strategy, keeping in view the risk/value profile of procurements planned over a period of time based on the policy mentioned in AD/FIN/1/Rev.4 (dated 31 January 2018).

16.   Issue instructions for preparing procurement plans, and monitor implementation by developing the procurement planning tool on Sharepoint.

17.   Issue instructions for separate delegation of authority for signing of contracts, revised thresholds (lower for waiver cases), delegation only to one authority, copy of revised template for award, and IT/Sharepoint tool for determining cumulative values.

18.   Strengthen the functioning of the Committee on Contracts (COC by:

    (a)   reviewing the composition of the COC, to facilitate due diligence in carrying out its role of providing independent and objective review and advice. Provide timeline by which Management plans to review the composition of the COC;

    (b)   clarifying the role and status of observers so as not to dilute the responsibility of the committee members to render independent and objective advice;

    (c)   strengthening internal controls, as mentioned in the audit observation; and

(d)   expanding the role of the COC so as to focus more on a macro-level perspective of the status of procurement cases, and not only on individual transactions.

19.   Strengthen internal controls in the procurement process by:

(a)   developing a Procurement Manual and/or SOPs to provide detailed internal controls and guidelines for managing the different stages of the procurement process, with supporting templates/formats in a time-bound manner. Confirm in a checklist whether all detailed internal controls as mentioned in the audit observation are included in AD/FIN/1/Rev.4; and

(b)   preparing process flow charts, to cover all stages of the procurement process, and defining the segregation of duties for the procurement process.

20.   Strengthen vendor management practices by:

(a)   establishing a roster of prequalified suppliers, establishing procedures for vendor due diligence and background checks, blacklisting, and requiring vendors to adhere to a code of conduct and declare conflicts of interest; and

(b)   performing evaluations of supplier performance and maintaining a suitable database of supplier performance evaluations for future contracts.

21.   Use IT tools such as e-procurement, including e-tendering, to enhance the efficiency of the procurement process and provide an information database to monitor performance. Also, consider using e-approval workflow and e-signatures for paperless workflows to improve process efficiency and accountability.

- - - o - - -