OPCW

Executive Council

Eighty-Fifth Session
11 – 14 July 2017

EC-85/DG.12
26 May 2017
Original: ENGLISH

NOTE BY THE DIRECTOR-GENERAL

IMPLEMENTATION IN 2016 OF THE RECOMMENDATIONS CONTAINED IN THE 2015 ANNUAL REPORT OF THE OFFICE OF INTERNAL OVERSIGHT

1. This report describes the compliance of the Technical Secretariat (hereinafter "the Secretariat") from 1 January to 31 December 2016 with the recommendations contained in the Annual Report of the Office of Internal Oversight (OIO) for the period from 1 January to 31 December 2015 (Annex to EC-82/DG.3 C-21/DG.4, dated 15 April 2016). It is submitted to the Executive Council (hereinafter "the Council") at the Council's request. The Note by the Director-General (EC-82/DG.3 C-21/DG.4) and the annual report of the OIO annexed thereto should be read in conjunction with this document.

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

2. The Director-General ensured that the status of implementation of the recommendations of the OIO was closely monitored. There is a regular agenda item on this subject at meetings of the Management Board.

3. The Director-General accepted all recommendations of the OIO for 2015 (EC-82/DG.3 C-21/DG.4), and the OIO received quarterly updates from the Secretariat on the status of their implementation.

4. The following table reports on the status of implementation of pending recommendations that were issued in 2015 and in prior periods, as at 31 December 2016.

IMPLEMENTATION IN 2016 OF THE RECOMMENDATIONS CONTAINED IN THE 2015 ANNUAL REPORT OF THE OFFICE OF INTERNAL OVERSIGHT

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
Administration Division (ADM)	OIO/11/04	Evaluation of knowledge management in the Technical Secretariat	Evaluation	Recommendation 4: Responsibilities of focal points The Director of the ADM should provide a statement of detailed responsibilities of focal points as stated in paragraph 6.3 of QDOC/ADM/SOP/001.	Standard	8 February 2017 DNV Consulting was engaged in December 2016 to perform a knowledge management project. The process of gathering information has been completed. Scenario planning and strategy framework development will be carried out next. It is expected that this will be completed and results published in the second quarter of 2017, which will be followed by the recruitment of a knowledge management specialist from the third quarter of 2017. It is anticipated that internal knowledge management capacity (including divisional resources) will be in place by end 2017.	Ongoing

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
Administration Division (ADM)	OIO/11/05	Audit of Identity and Access Management in the Technical Secretariat	Confidentiality audit	Recommendation 1: Establishing an identity and access management policy The Director of the ADM should establish and communicate a standard operating procedure (SOP) outlining the identity and access management policy and Secretariat procedures that will ensure that identities and access rights of users are managed in a uniform and central manner, to ensure consistency and efficiency of access control processes.	Standard	8 February 2017 The requirement of the Information Services Branch (ISB) and the Office of Confidentiality and Security (OCS) to gather information and develop SOPs has been delayed due to the significant resource constraints throughout 2016. The next step will be to scope and phase a viable solution to address this recommendation. The ISB was working with the OCS to establish SOPs for identity and access management, with a view to having a draft out for clearance no later than the fourth quarter of 2016.	Ongoing
Inspectorate Division (INS)	OIO/11/10	Audit of the Process of Mission Logistical Planning	Confidentiality audit	Recommendation 4: Mission warning orders The Head of the Operations and Planning Branch (OPB) should, with advice	Standard	28 January 2017 The SharePoint application developed by the ISB was fixed at the end of 2016 and final testing of the	June 2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				from the ISB, consider the implementation of an electronic workflow on the Security Non-Critical Network (SNCN) to prepare, authorise and distribute mission warning orders.		application is under way. It is expected that the application will go live at the start of the second quarter of 2017.	
Inspectorate Division (INS)	OIO/14/01	Audit of the Management of Mission Warning Orders	Confidentiality audit	Recommendation 4: Non-sharing of mission codes The Head of the OPB should ensure that mission warning orders meant for the Protocol and Visa Branch (PVB), OPB Movement Section, OPB Equipment Store, OCS, Secure Archive (SA), Inspectorate Management Branch (IMB), and Operations Centre (OPC) do not contain the mission code information. This will significantly reduce the risks associated with the identification of plant sites before States Parties are notified in case of reinspection missions.	Standard	28 January 2017 The electronic mission warning order will be implemented with various access rights for different branches. See recommendation 4 of OIO/11/10. All recommendations have been incorporated in the electronic mission warning order. The electronic mission warning order will be relaunched by the second quarter of 2017.	June 2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
Verification Division (VER)	OIO/14/03	Evaluation of the Implementation of Results-Based Management for the Industry Verification Branch	Evaluation	Recommendation 5: Defining and addressing quality The IVB should review its performance measures and explore new metrics, which could give a more adequate and comprehensive picture of its work. This could include indicators of both quality and quantity. The successful elements of these metrics could later be considered by the IVB as KPIs.	Standard	21 January 2016, M/VER/ODV/202353/16 The IVB held several meetings with the OSP, VER, and other branches. A list of potential IVB performance metrics was considered and is being discussed. This would benefit from further assistance from the OIO or the Office of Strategy and Policy (OSP), in order to evaluate the effectiveness of the assessment tools. The request for OIO assistance to evaluate the effectiveness of the assessment tools considered by the IVB is renewed.	Dependent on OIO review
Budget, Planning and Control Branch (BUD)	OIO/15/01	OPCW Budgeting Process	Internal audit	Recommendation 1: Budget process The Budget, Planning and Control Branch (BUD) should consider issuing an annual internal memo on the performance of the	Standard	17 January 2017 The internal memo can be drafted after the closure of the 2016 budgetary accounts, and in parallel with the Note by the Director-General entitled	February 2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				budget process in the previous year. The availability of a medium-term plan, written with guidance from the Director-General, last-moment adjustments, as well as causes for deviations from the budget should be considered.		"Transfer of Funds During 2016" (EC-84/DG.17 C-22/DG.3, dated 16 February 2017), and will be finalised in February 2017 in accordance with the official calendar for the 2016 closure activities (attached) and the timeline included in the annual document forecast for 2017.	
Office of Confidentiality and Security (OCS)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 1: Business impact analysis In order to assess the criticality of the business processes, a mechanism for performing a business impact analysis should be established.	Critical	26 January 2017 ODG and OCS are in dialogue with States Parties to solicit their assistance with the resource implications of recommendations relating to business continuity.	TBD
Information Services Branch (ISB)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 10: The availability of Security Critical Network backups After achieving for the disaster recovery location (DRL) a certain level of security standards similar to those at the primary	Critical	30 January 2017 Further action is dependent on recommendations 1, 2, and 6, and a timeline and course of action will be established when these recommendations have progressed. The ISB will	2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				location (see recommendation 8), the copy of the Security Critical Network (SCN) and other confidential or sensitive information stored on backup media should also be transferred and kept on the DRL, for the purpose of minimising the risk of forever losing the data in the case of a major disaster. These backup media are essential for the purpose of the data restoration process in case of activation of the disaster recovery plan (DRP).		make a plan with the OCS and other stakeholders after an initial assessment. The target date is therefore theoretical until further notice.	
Information Services Branch (ISB)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 11: Protection of the confidentiality of the Security Critical Network data on the backup media through encryption In order to protect the confidentiality of information stored on the backup media, the ISB should ensure that the	Critical	30 January 2017 The ISB will appraise encryption technology and seek to implement the recommendation in 2017. The solution depends on adequate training, which will be planned by the ISB.	2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				Security Critical Network (SCN) data written on the backup media is properly encrypted.			
Information Services Branch (ISB)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 2: Complete implementation of the disaster recovery plan The activities for implementing a partial business continuity/disaster recovery plan for either the Security Critical Network (SCN) or the Security Non-Critical Network (SNCN) (not both) should be carefully reassessed. The Organisation needs comprehensive business continuity and disaster recovery plans in place, which include all core activities and critical processes. The criticality of the business processes should be determined (or confirmed) by performing a business impact analysis (see recommendation 1).	Standard	30 January 2017 Further action is dependent on recommendation 1 (business impact analysis), and a timeline and course of action will be established when that recommendation has progressed. The ISB will make a plan with the OCS and other stakeholders after an initial assessment of the business impact analyses executed. The target date is therefore theoretical until further notice.	2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
Office of the Director-General (ODG)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 3: Business continuity manager The Director-General should appoint the Head of the OCS or another staff member to fulfil the role of Business Continuity Manager.	Standard	23 May 2017 The Head OCS has come on board and is considering how best to take forward this recommendation, in consultation with relevant Directors.	
Office of Confidentiality and Security (OCS)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 4: Testing the BCP (short term goals) A process of regular annual testing of the existing BCP, conducted by the BC Manager, should be established. The testing scenarios should be planned in advance, and the results of the tests should be carefully analysed.	Standard	26 January 2017 ODG and OCS are in dialogue with States Parties to solicit their assistance with the resource implications of recommendations relating to business continuity.	TBD
Office of Confidentiality and Security (OCS)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 5: Testing the BCP (mid-term goals) The tests of the BCP should not be limited to only table-top exercises. After	Standard	26 January 2017 ODG and OCS are in dialogue with States Parties to solicit their assistance with the resource implications of	TBD

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				the implementation of a fully operational DR location (DRL) site, the testing scope should be expanded, by actual testing of the IT systems on the DRL. The final iteration of the testing process (which also denotes the highest level of maturity of the testing process) should also include the full interruption test.		recommendations relating to business continuity.	
Information Services Branch (ISB)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 6: Establishing adequate and effective standard operating procedures for the disaster recovery location In the case of a major disruption or natural disaster, it is very unlikely that all of the assumptions from the SOP for modelling the site will be present, which means that QDOC/ISB/SOP/001 may not be applicable at all. The Organisation's disaster recovery plan (DRP)	Critical	30 January 2017 The ISB has planned the process to adjust the Quality Management System document (QDOC) processes for 2017. This finding will be part of the process update and redesign.	2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				should cover the implementation of the recovery strategy for both the Security Critical Network (SCN) and Security Non-Critical Network (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 at the disaster recovery location (DRL) premises.			
Information Services Branch (ISB)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 7: The role of the Information Services Steering Committee in the business continuity management process The process for business continuity management (BCM) should be established by using a top-down approach. In order for the BCM process to be effective, it should be	Critical	30 January 2017 This recommendation has been partially accepted by ISB. The BCM process will benefit from oversight at a higher organisational level that considers all the continuity aspects, rather than purely IT. Specific to the IT areas, the IT Steering Committee	2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				driven by a body with the necessary organisational-wide authority. The Information Services Steering Committee (ISSC) should take a leading role in establishing and conducting a BCM process within the Organisation. The BCM activities should also become a part of the ISSC's terms of reference and agenda.		would be the correct forum to provide guidance and monitoring of actions undertaken as part of the BCM process. This guidance, however, should be given based on the results of the business impact analyses.	
Office of Confidentiality and Security (OCS)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 8: Physical security at the disaster recovery location in Rijswijk In order to maintain the necessary level of confidentiality of the data at the disaster recovery location (DRL), the same level of physical security measures as those currently implemented at headquarters needs to be implemented. A 24-hour physical security presence	Critical	26 January 2017 This has been raised as a staffing issue, as stated in M/ODG/OCS/203006/16.	2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				should be established. The video surveillance system should be improved in order to monitor the uncovered areas that have been identified.			
Procurement and Support Services Branch (PSB)	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 9: Technical security at the disaster recovery location As an independent power supply is a necessary precondition for the effective implementation of both the business continuity plan (BCP) and disaster recovery plan (DRP), a power generator with sufficient capacity to support the functioning of the critical business processes and IT systems needs to be procured and installed. In addition, a server room meeting the widely accepted standards should be constructed on the first floor, which includes but is not limited to the implementation of:	Critical	23 January 2017 On 14 October 2016, Sakiko Hayakawa, Senior Planning Officer, submitted a report on the OPCW Strategic Capability Investment Fund, which proposes changes to the physical infrastructure of the OPCW to create a Centre of Chemical Sciences to increase training capabilities and address new challenges. The Organisation's decisions in this regard could have a significant impact on the relevant recommendation of the OIO. It would therefore be prudent to wait for a decision on the report before proceeding with any	

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				an armoured door; a restricted access control system; heating, ventilation, and air-conditioning (HVAC) systems; a raised floor; temperature sensors; smoke and fire detectors; motion detectors; video surveillance; and fire extinguishers.		of the proposed changes, which remain subject to the prior addressing of recommendations 1, 3 and 7.	
Secretariat for the Policy-Making Organs (PMO)	OIO/15/04	Evaluation of the Conference Services Unit	Evaluation	Recommendation 1: Formalisation of existing working practices The Conference Services Unit (CSU) should review, rationalise, and formalise into Quality Management System document (QDOC) procedures its existing working practices relating to regular, core activities. This should include detailed information on the division of responsibilities, timelines and deadlines, follow-up and evaluation procedures, and useful tools such as checklists and	Standard	27 January 2017 1. The CSU has reviewed the existing QMS documentation related to some of its working practices and concluded that, for the time being, there is no need for an update. However, the CSU is committed to periodically conducting an assessment of that documentation and updating it accordingly. 2. See above 3. In evaluating this recommendation, the CSU	Completed Completed Completed

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				flow-charts. Furthermore, the CSU should review and update the existing QMS documentation.		realised that there is no comprehensive QDOC for procedures related to the preparation and in-session support of the Council and Conference of the States Parties (hereinafter "the Conference"). As a consequence, a draft proposal for two new QDOCs has been submitted to the Director of the PMO, who approved the format and scope of the planned documents. 4. The CSU is currently working on drafting two new QDOCs concerning existing work practices relating to the conduct of the Council and the Conference. These include detailed information on the division of responsibilities, timelines and deadlines, follow-up and evaluation procedures, and any other information deemed relevant for the completeness of the document.	In progress

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
Secretariat for the Policy-Making Organs (PMO)	OIO/15/04	Evaluation of the Conference Services Unit	Evaluation	Recommendation 2: Reducing paper consumption The Conference Services Unit should: (a) explore current best practices and new initiatives in the delivery of information to Member States in other international organisations; (b) elaborate a plan and strategy towards a paperless conference environment; and (c) evaluate the opportunities for the phased introduction of a print-on-demand service (ensuring short delivery periods and pre-order facilities).	Standard	27 January 2017 1. In the course of 2016, the CSU continued the practice of print-on-demand services for the distribution of documents during the Eighty-Second and Eighty-Third Sessions of the Council and the Twenty-First Session of the Conference. This was successful and appreciated by the delegations of the States Parties. The CSU has therefore formally adopted this practice and will continue to implement it at future sessions. The CSU is currently in the process of creating a task force that will include representatives of different branches of the OPCW; the CSU plans to establish the force by the end of May 2017. 2. The CSU, with the support of the task force,	Partially completed 26 May 2017 31 Sept. 2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
						will contact corresponding offices in other international organisations for information on best practices and produce a summary report of best practices and lessons learned. 3. Based on the outcome of the above summary report, the task force will evaluate the feasibility of applying Paper Smart practices at the OPCW, and elaborate proposals towards the implementation of applicable practices. 4. The summary report on best practices and evaluation will be presented by the task force to the Management Board.	15 Dec. 2017 31 March 2017
Secretariat for the Policy-Making Organs (PMO)	OIO/15/04	Evaluation of the Conference Services Unit	Evaluation	Recommendation 6: Improving feedback tools The Conference Services Unit should: (a) adopt a more formalised approach to surveys; (b) institutionalise the	Standard	27 January 2017 1. The CSU reviewed the response rates of the PMO surveys conducted during the Nineteenth and Twentieth Sessions of the Conference (December	On track

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				annual conduct of customer satisfaction surveys; (c) explore ways to improve the quality, accessibility, and response rates of its surveys; and (d) obtain feedback from staff of the Secretariat, especially if surveys form the basis for reporting on the key performance indicator.		2014 and December 2015, respectively) and the Eightieth Session of the Council (October 2015) and improved the quality of the survey accordingly. The CSU will continue to implement this recommendation on an annual basis. 2. The CSU developed the annual survey and distributed it during the Twenty-First Session of the Conference, in hard copy (at the documentation counter), inside the World Forum Theater (by volunteers announced from the podium by the Director of the PMO), and online. The feedback on the services provided by the PMO has been positive in all cases. A detailed analysis, including graphics, has been prepared and is available upon request to the CSU. The results have been	Completed

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
						shared only within the PMO. 3. The CSU is in the process of developing a survey for feedback by the Secretariat. The estimated date is 28 April 2017. 4. PENDING until the next Management Board meeting. Feedback and statistics will be provided to the next Management Board meeting and further elaborated in the annual performance report as requested. 5. The CSU is in the process of compiling the requested recommendation.	26 April 2017 31 October 2017
Secretariat for the Policy-Making Organs (PMO)	OIO/15/04	Evaluation of the Conference Services Unit	Evaluation	Recommendation 7: Development of a fit-for-purpose evaluation mechanism The Conference Services Unit should establish a formalised, simple, fit-for-purpose evaluation mechanism that includes a	Standard	27 January 2017 1. Following the OIO recommendation, the CSU recognised the need to create a standard template for lessons learned, and took action. Existing lessons-learned practices and standardised lessons	Completed

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				lessons-learned database, in which all feedback may be logged, action agents assigned and tracked to closure. The mechanism should be reflected in updated Quality Management System documentation.		learned have been formalised into two logs: - Council Sessions–Lessons Learned; and - Conference Sessions-Lessons Learned. The criteria selected for the lessons learned logs as follows: session, category, problem/success, impact, recommendation, status/ follow-up, remarks, follow-up. 2. Since 2015, the lessons-learned logs for the Council and Conference sessions have been updated within two weeks of the close of each session. Up to January 2017, the logs refer to the Eightieth, Eighty-First, Eighty-Second, and Eighty-Third Sessions of the Council and the Twentieth and Twenty-First Sessions of the Conference. Lessons learned from previous Council and	29 Sept. 2017

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
						Conference sessions, which were recorded in the form of notes, are still being transferred to these logs. 3. Pending the implementation of recommendation 1, the lessons learned log will be attached as a template to the QMS documentation.	
Administration Division (ADM)	OIO/15/05	Audit of Risk Management	Internal audit	Recommendation 2: Information circular The Director of Administration should consider assigning the task of drafting an information circular on practical guidance for incorporating risk management into the day-to-day operations of the Secretariat.	Critical	1 February 2017 A meeting was held to discuss next steps, including the further consideration of drafting an information circular on risk management within the Secretariat.	Second quarter of 2017
Administration Division (ADM)	OIO/15/05	Audit of Risk Management	Internal audit	Recommendation 4: Context risk management The Secretariat can report on but cannot be held responsible for all risks, while risks for the divisions in achieving the objectives would justify special	Standard	1 February 2017 A meeting was held to discuss next steps, including the identification of potential mitigating actions against each risk.	Ongoing

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				attention. The Director of Administration should consider the context in the management of risks.			

- - - o - - -