OPCW

Executive Council

Eighty-Eighth Session
10 – 13 July 2018

EC-88/DG.10
1 June 2018
Original: ENGLISH

NOTE BY THE DIRECTOR-GENERAL

IMPLEMENTATION IN 2017 OF THE RECOMMENDATIONS CONTAINED IN THE 2016 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 2017 with the recommendations contained in the Annual Report of the Office of Internal Oversight (OIO) for the period from 1 January to 31 December 2016 (Annex to EC-85/DG.10 C-22/DG.4, dated 24 May 2017). It is submitted to the Executive Council (hereinafter "the Council") at the Council's request. The Note by the Director-General (EC-85/DG.10 C-22/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 2016 (EC-85/DG.10 C-22/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 2016 and in prior periods, as at 31 December 2017.

IMPLEMENTATION IN 2017 OF THE RECOMMENDATIONS CONTAINED IN THE 2016 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/11/05	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	5 February 2018 The Information Services Branch (ISB) is working with the Office of Confidentiality and Security (OCS) to establish SOPs for identity and access management. A draft SOP for access to the Security Critical Network (SCN) has been created and is being reviewed.	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 from the ISB, consider the implementation of an electronic workflow on the Security Non-Critical Network (SNCN) to prepare, authorise	Standard	9 February 2018 The electronic mission warning order workflow went live in January 2018.	2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				and distribute mission warning orders.			
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	9 February 2018 See audit OIO/11/10. Testing of this capability will follow in the next few weeks.	2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
International Cooperation and Assistance Division (ICA)	OIO/15/02	Evaluation of Outreach Activities Conducted in the International Cooperation and Assistance Division	Evaluation	Recommendation 1: High-level strategic document The OIO recommends the development of a high-level guidance document for the 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, thereby backing up and underpinning its activities.	Critical	25 January 2018 Consultations within the ICA are still ongoing in order to finalise a strategy and framework in support of States Parties in implementation of the relevant Articles of the Chemical Weapons Convention (VII, X, and XI). The fourth phase of the Programme to Strengthen Cooperation with Africa on the Chemical Weapons Convention (hereinafter "the Africa Programme") (2017-2019) contains elements that meet parts of this recommendation.	Ongoing
ICA	OIO/15/02	Evaluation of Outreach Activities Conducted in the International Cooperation and Assistance	Evaluation	Recommendation 2: Formalisation of the annual planning process The OIO recommends formalising existing planning activities into a consolidated and transparent annual planning process for all three	Standard	25 January 2018 The current budget cycle is conducted on a yearly basis and developing indicative multi-annual programming would require the interest and commitment of States Parties to provide the	

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
		Division		Branches. The ICA should evaluate the feasibility of the introduction of multi-annual programming, which should allow for greater advance notice of planned activities and ensure continuity of the efforts.		necessary resources to cover the anticipated multi-annual period.	
ICA	OIO/15/02	Evaluation of Outreach Activities Conducted by the International Cooperation and Assistance Division	Evaluation	Recommendation 3: Application and selection process for ICA events For event planning, the OIO recommends analysing best practises already developed within the ICA (e.g. knowledge testing, application process) and applying them across the Division, where appropriate. The specification of detailed criteria to be met by applicants should be standardised (to the extent possible) for all Notes by the Secretariat and calls for nominations in order to make the application and selection process more efficient and transparent.	Standard	25 January 2018 The selection process is being continuously reviewed and improved. It is not possible, however, to have a standard selection procedure in the ICA applying across all the Branches, as activities are very different in nature, respond to different objectives, and require different treatment. Calls for nominations and invitation letters clearly set out any selection criteria and/or prerequisites for participation in the respective events; a web-based platform for the management of ICA	

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
						activities is being developed in the Assistance and Protection Branch as a pilot, in coordination with the ISB.	
ICA	OIO/15/02	Evaluation of Outreach Activities Conducted by the International Cooperation and Assistance Division	Evaluation	Recommendation 4: Evaluation mechanism The OIO recommends establishing a suitable evaluation mechanism (applied to all ICA outreach activities) which would define, at least: (a) areas and activities to be evaluated; (b) type, purpose, and use of data to be collected; (c) frequency, form, and audience of reporting; (d) monitoring of implementation of recommendations (lessons learned); (e) link of performance with costs; and (f) deadlines and responsibilities for evaluation activities (including coordination of the process at the divisional level).	Critical	25 January 2018 A second training course was organised in December 2017. The process is ongoing to implement monitoring and evaluation in ICA activities. A consultant will be hired to support this effort. The first elements of the monitoring and evaluation system are expected to be developed in the first half of 2018. The knowledge gained from the first course, held in December 2017, was included in developing the next phase of the Africa Programme and will be applied later to all ICA activities.	Third quarter 2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
ICA	OIO/15/02	Evaluation of Outreach Activities Conducted by the International Cooperation and Assistance Division	Evaluation	Recommendation 5: Alignment of existing procedures The OIO recommends that the Director of ICA: (a) initiate a review of various procedures to align their content insofar as is possible, draw upon best and current practices, to elaborate and apply consistent procedures for the conduct of ICA activities by all Branches; and (b) encourage all Branches to enhance the use of existing tools such as checklists and templates, in order to align processes and increase efficiency.	Standard	25 January 2018 Efforts are still continuing to develop a Division SOP to align the procedures and mechanisms of the three Branches.	Third quarter 2018
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 the business impact analysis should be established.	Critical	24 January 2018 Budgetary support will be sought this year for a business impact analysis and risk assessment.	2019

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
ISB	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 10: The availability of SCN backups After achieving for the disaster recovery location (DRL) a certain level of security standards similar to those at the primary location (see recommendation 8), the copy of the 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).	Critical	26 February 2018 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 make a plan with the OCS and other stakeholders after an initial assessment.	TBD
ISB	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 11: Protection of confidentiality of the SCN data on the backup media through encryption	Critical	26 February 2018 A solution has been developed for backup encryption and has been tested successfully at	2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				In order to protect the confidentiality of information stored on the backup media, the ISB should ensure that the SCN data written on the backup media is properly encrypted.		OPCW Headquarters by the ISB and OCS. The solution still needs to be tested on the DRL; if successful, this recommendation can be closed.	
ISB	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 2: Complete implementation of the DRP The activities for implementing a partial business continuity plan (BCP)/DRP for either the SCN or the SNCN (not both) should be carefully reassessed. The Organisation needs a comprehensive BCP and DRP 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	26 February 2018 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 analysis executed.	TBD
Office of the Director-General	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 3: Business Continuity Manager	Standard	2 March 2018	TBD

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				The Director-General should appoint the Head of the OCS or another staff member to fulfil the role of Business Continuity Manager.		It has been agreed that we should look again at how best to manage business continuity, and once funding has been found, a consultant will be engaged to review the issue.	
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 Business Continuity Manager, should be established. The testing scenarios should be planned in advance, and the results of the tests should be carefully analysed.	Standard	24 January 2018 The BCP will undoubtedly be revised as a result of the previous requirement. This will be investigated when the business impact analysis and follow-up action are complete.	TBD
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 the implementation of a fully operational DRL site, the testing scope should be	Standard	24 January 2018 The BCP will undoubtedly be revised as a result of the business impact analysis. This will be investigated when the business impact analysis and follow-up action are complete.	TBD

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				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.			
ISB	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 6: Establishing adequate and effective SOPs for the DRL 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 DRP should cover the implementation of the recovery strategy for both the SCN and the 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 DRL premises.	Critical	26 February 2018 QDOC/ISB/SOP/001 describes disruptions of more than two weeks. To update this procedure completely, a business impact analysis on OPCW business systems need to be available and the disaster recovery plan updated to the latest version. As soon as these conditions have been fulfilled, the ISB will be able to update QDOC/ISB/SOP/001 as requested.	TBD

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
ISB	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 7: The role of the Information Services Steering Committee (ISSC) in the business continuity management (BCM) process The process for BCM should be established by using the top-down approach. In order for the BCM process to be effective, it should be driven by a body with the necessary organisational-wide authority. The 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.	Critical	26 February 2018 This recommendation has been partially accepted by the ISB. The BCM process will benefit from oversight at a higher organisational level that considers all continuity aspects, rather than purely IT. Specific to the IT areas, the IT Steering Committee 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 a business impact analysis, for which budgetary support is being sought.	TBD
OCS	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 8: Physical security at the DRL in Rijswijk In order to maintain the necessary level of confidentiality of the data at	Critical	24 January 2018 This has been raised as a staffing issue. We have an extant temporary solution: Since 6	2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				the DRL, the same level of physical security measures as those currently implemented at Headquarters has to be implemented. A 24-hour physical security presence should be established. The video surveillance system should be improved in order to monitor the uncovered areas that have been identified.		April 2017, uniformed security officers have been posted at the Rijswijk facility during weekday evenings and weekends.	
General Services and Procurement Branch	OIO/15/03	Audit of IT Business Continuity	Confidentiality audit	Recommendation 9: Technical security at the DRL As an independent power supply is a necessary precondition for the effective implementation of both the BCP and 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	Critical	3 May 2018 A business impact analysis and associated risk assessment would address this recommendation as well as other business continuity issues. The necessary budgetary support for a comprehensive business impact analysis and risk assessment will be sought this year.	TBD

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				implementation of: an armoured door; a restricted access control system; heating, ventilation, and air-conditioning systems; a raised floor; temperature sensors; smoke and fire detectors; motion detectors; video surveillance; and fire extinguishers.			
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. These should include detailed information on the division of responsibilities, timelines and deadlines, follow-up and evaluation procedures, and useful tools such as checklists and flow-charts. Furthermore, the CSU should review and	Standard	30 January 2018 The CSU revised the following QDOCs: QDOC/PMO/SOP/001 QDOC/PMO/WI/001 QDOC/PMO/WI/010 PMO is currently working on the drafting of a QDOC for procedures related to the preparation and in-session support of the Council and Conference of the States Parties (hereinafter “the Conference”). The targeted period for submission is July 2018.	Completed In progress, July 2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				update existing QDOCs.			
PMO	OIO/15/04	Evaluation of the Conference Services Unit	Evaluation	Recommendation 2: Reducing paper consumption The CSU 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	30 January 2018 In 2016, the CSU formally adopted the practice of print-on-demand services for the distribution of documents and continues to follow this practice during all regular and special sessions of the Council and Conference. At the same time, the CSU continues to promote the use of the Extranet and has succeeded in achieving a considerable reduction of the use of paper at the documentation counter. Moreover, the CSU coordinated the establishment of an OPCW Paper Smart task force, which includes representatives of each Division of the OPCW tasked with drafting a plan and strategy to reduce the use and waste of paper in the	Pending consultation with the OIO.

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
						OPCW as a whole.	
PMO	OIO/15/04	Evaluation of the Conference Services Unit	Evaluation	Recommendation 6: Improving feedback tools The CSU should: (a) adopt a more formalised approach to surveys; (b) institutionalise the annual conduct of customer satisfaction surveys; (c) explore ways to improve the quality, accessibility, and response rates of its surveys; (d) obtain feedback from staff of the Secretariat, especially if surveys form the basis for reporting on the key performance indicator.	Standard	30 January 2018 (a) and (b): The CSU continues to implement this recommendation, conducting annual surveys that are distributed at the documentation counter during formal meetings. (c) and (d): The CSU is constantly looking into improving accessibility and quality of the surveys and is currently exploring an on-line system to be included on the CSU internal portal to obtain feedback from Secretariat staff.	On track On track
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	Critical	5 February 2018 A risk framework is being drafted.	Ongoing

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				operations of the Secretariat.			
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 attention. The Director of Administration should consider the context in the management of risks.	Standard	5 February 2018 The risk register review using the modified template is ongoing.	Ongoing
Health and Safety Branch (HSB)	OIO/15/06	Evaluation of the Programmes and Activities of the Health and Safety Branch	Evaluation	Recommendation 1: Review of HSB objectives The Head of the HSB should review the relevance of the outlined objectives established in 2005 and consider updating them to reflect the shifts in organisational priorities and available resources.	Standard	9 February 2018 This issue will be reviewed along with all other HSB documentation, in accordance with Recommendation 6 below.	Ongoing
HSB	OIO/15/06	Evaluation of the Programmes and Activities of the Health and Safety Branch	Evaluation	Recommendation 2: Strengthen the Health and Safety Committee (HSC) As the Secretary of the HSC, the Head of the HSB should make a proposal on how to	Standard	9 February 2018 This was discussed on 21 March 2017, as part of the agenda of the 2016 HSC meeting. The Committee has agreed on the expansion	Pending release of an information circular to this effect.

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				strengthen the guiding role of the HSC in order to better reflect and encompass more strategic issues related to the health and safety mandate of the HSB. An update of the terms of reference, including the composition, responsibilities, and scope should follow.		of membership. The recommendation will be made to the Director-General. A proposal will then be put forward on the methodology to strengthen the Committee.	
HSB	OIO/15/06	Evaluation of the Programmes and Activities of the Health and Safety Branch	Evaluation	Recommendation 3: Enhance MARS® functionality HSB medical staff should work together with the ISB to enhance the MARS® platform to include data collection and audit capabilities. If modification is not possible, the ISB should assist the HSB with developing an alternative solution to meet the needs of medical staff.	Standard	9 February 2018 This is outside the scope of the HSB alone, and involves coordination between the ISB, OCS, and the enterprise resource planning (ERP) project team.	Awaiting implementation by the ERP project team.
HSB	OIO/15/06	Evaluation of the Programmes and Activities of the Health and Safety	Evaluation	Recommendation 4: Develop a coherent well-being strategy The Head of HSB should develop a coherent well-being	Standard	9 February 2018 The well-being strategy was discussed at and presented to the HSC meeting on 21 March 2017.	In progress

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
		Branch		strategy that takes into account both the physical and mental health needs of OPCW employees. Such a document should be aligned with organisational goals and HSB objectives while setting up clear reporting lines for the Staff Welfare Officer. The implementation of the well-being strategy should result in better integration of this function with the HSB and, thus, a more stable environment in which to perform these tasks.		Though work is already in progress, a formal proposal will be made to the Director-General in the course of the year.	
HSB	OIO/15/06	Evaluation of the Programmes and Activities of the Health and Safety Branch	Evaluation	Recommendation 5: Strengthen oversight of OPCW medical personnel Together with the Directors of the ICA and INS, the Head of the HSB should propose an arrangement that allows for effective oversight of all medical personnel who carry out clinical and advisory duties.	Standard	9 February 2018 Coordination will also be required with the ADM, for possible amendments to the relevant work requirements.	TBD
HSB	OIO/15/06	Evaluation of the Programmes	Evaluation	Recommendation 6: Review and update QDOCs	Standard	9 February 2018	Review of safety- related documents

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
		and Activities of the Health and Safety Branch		The HSB should continue to review, update, and align operational QDOCs with current practice, in order to mitigate risks and ensure process reliability, prioritising those documents that are more than three years old.		This process, though under way, has been hampered by a shortage of staff in the HSB and reorganisation within the Secretariat, in terms of Branches/Sections, such as the creation of new cell structures in the INS. All QDOCs will be reviewed and updated before the end of 2017.	completed. Review of medical documents ongoing.
INS	OIO/15/07	Audit of Manpower Planning in the Inspectorate Division	Confidentiality audit	Recommendation 6: Review of AD/PER/12/Rev.1 and harmonisation with QDOC/INS/WI/IM503 The Director of the INS should consider initiating, for the Director-General's consideration, a review and update of AD/PER/12/Rev.1: "Working Hours, Arrangement for Replacement Days and Compensation for Overtime for Inspectors and Other Staff Members on Inspection Mission or involved in Inspection-Related Training" (April 2005). This could include consideration of	Standard	9 February 2018 The administrative directive has been revised and is pending release.	Ongoing

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				its possible harmonisation with QDOC/INS/WI/IM503: "Work Instruction on the Management and Oversight of Inspection Replacement Days" (May 2012).			
INS	OIO/15/07	Audit of Manpower Planning in the Inspectorate Division	Confidentiality audit	Recommendation 7: Enhancement of reports on replacement days The Head of the Operations and Planning Branch should initiate a request for the ISB to consider enhancing the capability to view or extract reports on replacement days from the Quintiq inspection roster application. The reports should include details of replacement days earned, utilised, and unutilised for all inspectors individually and collectively. Such a decision should be supported by a cost-benefit analysis.	Standard	9 February 2018 Areas for improvement have been identified and were included in the new version of Quintiq.	Pending consultation with the OIO.
OCS	OIO/16/01	Audit of IT Infrastructure in the OPCW Laboratory	Confidentiality audit	Recommendation 1: Updates to the Information Security Policy (ISP): (a) The OCS should plan to review and update the ISP (2007).	Critical	24 January 2018 The ISP will be revised this year (after the Manual of Confidentiality Procedure).	Fourth quarter 2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				(b) The updated ISP should be aligned with the current ISO/IEC 27002:2013 "Information Technology – Security Techniques – Code of Practice for Information Security Management." (c) The OCS should define and conduct subsequent reviews at regular intervals or when significant changes occur to ensure that each current version of the ISP continues to be suitable, adequate, and effective.			
ISB	OIO/16/01	Audit of IT Infrastructure in the OPCW Laboratory	Confidentiality audit	Recommendation 5: Supervisory oversight of and documented procedures on the processes of tape media custody and movements between storage sites The ISB should provide for additional oversight on the processes of tape media custody and movements between Headquarters and the Rijswijk facility. The processes should be documented. This supervisory	Standard	26 February 2018 The ISB has planned the adjustment of the QDOC processes for 2018. The working instruction on the procedure of moving backup tapes is under review, to be finalised by August 2018.	2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				oversight would ensure that backup tapes are stored appropriately and accounted for. Documented procedures would provide the basis of this oversight.			
ISB	OIO/16/01	Audit of IT Infrastructure in the OPCW Laboratory	Confidentiality audit	Recommendation 6: Movement of monthly backup tapes from Rijswijk to Headquarters (a) The ISB should enhance its efficiency in transporting monthly backup tapes on the Rijswijk Laboratory Network from the Rijswijk Secure Archive (RSA) to the Headquarters computer centre. This could reduce the amount of actual data loss in the event that the Rijswijk Laboratory Network (RLN) is impacted by a disruptive event. (b) The ISB should update the OPCW ADM/ISB Network and Systems Log with full details of the descriptions of the monthly tape backups that are withdrawn from the RLN for transport to Headquarters.	Standard	26 February 2018 The ISB is updating all QDOCs and harmonising them in consultation with the OIO. This will be part of the process update/redesign for the SOP on disaster recovery. The ISB procedures should follow the disaster recovery plan for the OPCW. The work instruction on the procedure for moving backup tapes is under review, to be finalised by August 2018.	2018

Responsible Unit	Audit Ref. Number	Audit Title	Audit Type	Recommendation	Category	Management Response	Implementation Target Date
				(c) The ISB should create an equivalent log to the OPCW ADM/ISB network and systems log and maintain this in the Headquarters computer centre.			

- - - o - - -