Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2016/156

Audit of electronic mail and information and communications technology security in the Department of Field Support

While some good controls were in place, improvements are required in the management of logs, configurations, email records and security procedures

12 December 2016
Assignment No. AT2016/615/01

Audit of electronic mail and information and communications technology security in the Department of Field Support

EXECUTIVE SUMMARY

The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the management of electronic mail (email) and information and communications technology (ICT) security in the Department of Field Support (DFS). The audit covered the period from January 2014 to June 2016 and included a review of risk management, ICT support systems, and security policies.

DFS had implemented some good controls and practices such as network segmentation, multiple layers of security built into the ICT infrastructure, best practice certifications, and active-active disaster recovery infrastructure. However, some control weaknesses were identified in the management of email and ICT security, which needed to be addressed.

OIOS made nine important recommendations. To address the issues identified, DFS needed to:

- Formalize and implement its centralized log management and audit architecture procedures.
- Implement the journaling feature in the email server.
- Update the preventive maintenance schedule to include the review and clean-up of unused/obsolete email boxes, and the incident management procedure to identify security anomalies for implementing timely management actions.
- Define responsibilities for configuration management; update the configuration management database with all service assets; establish procedures to update the comprehensive network diagram; and implement policies and standards to manage the security configuration of the email server.
- Define a policy for regulating the configuration and management of security settings for email clients; implement and configure email in accordance with a mobile device management policy; and assess and mitigate ICT security threats posed by the use of unlicensed old email boxes.
- Document a schedule for the conduct of periodic vulnerability assessment of its entire ICT infrastructure to proactively identify and address ICT security vulnerabilities in a timely manner.
- Assess the ICT security policy settings for the Active Directory and periodically monitor their implementation status; document the backup policy for the Active Directory; and establish control over the audit tool for monitoring the Active Directory.
- Establish criteria and implement procedures for granting privileged access rights; conducting regular reviews of privileged access; and reviewing and establishing controls over conflicting roles.

Additionally, the United Nations Archives and Record Management Section (UNARMS) needed to document policies/standards to ensure that email records are identified, managed and stored in accordance with the applicable requirements for record-keeping.

DFS and UNARMS accepted the recommendations and have initiated action to implement them.

CONTENTS

Audit of electronic mail and information and communications technology security in the Department of Field Support

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of electronic mail (email) and information and communications technology (ICT) security in the Department of Field Support (DFS).

2. DFS provides administrative and logistical support services to the Departments of Peacekeeping Operations and Political Affairs, through the delivery of support to United Nations peacekeeping operations, special political missions and other field operations. This includes services in the areas of human resources, finance and budget, conduct and discipline, logistics, and ICT.

3. The Information and Communications Technology Division (ICTD) within DFS is primarily responsible for: (i) providing ICT operational, logistics and administrative support to field operations; and (ii) managing the Secretariat's global telecommunications infrastructure that underpins field operations, covering the wide area network and the DFS teleport located at the United Nations Logistics Base in Brindisi, Italy, and the communications facility in Valencia, Spain. In accordance with the global field support strategy, the logistics base has been re-profiled as the United Nations Global Service Centre (UNGSC).

4. The Service for Geospatial, Information and Telecommunication Technologies (SGITT) at UNGSC is the service within DFS that provides connectivity and hosting services to field missions and staff, including email services and related infrastructure. UNGSC is based in two locations (Brindisi and Valencia) to mitigate the risks of disaster recovery and business continuity.

5. Email messaging is regarded as a business critical application. Field offices and DFS use email extensively for operational communication to send both general information as well as sensitive and important data within and outside the Organization. The email system of DFS and field offices is hosted in Brindisi and Valencia data centres. Given their "active-active" configuration, both locations function as primary sites. Either data centre can be the disaster recovery site when the other one is unavailable.

6. DFS migrated its email services in 2014, following a pilot initiative conducted at the United Nations Interim Force in Lebanon in 2013. The migration included 45,000 email users. However, approximately 800 users located in field offices still remained on the old system to ensure encrypted communication with Headquarters, New York. It is expected that the new system will also be adopted by the United Nations Secretariat as the corporate standard for email system across the Organization by the end of 2016.

7. The SGITT Mail Engineering Group (MEG) had a dedicated functional team of 12 staff members managing a total of 50,620 mailboxes located across the various field missions, UNGSC (Valencia and Brindisi), and Headquarters, New York. In addition, the team provided email services to the Department of Safety and Security and the Special Tribunal for Lebanon. All email servers were virtualized. Virtual machines run on dedicated clusters of physical servers.

8. The number of staff approved for SGITT for 2015/16 was 116. In addition, SGITT engaged 375 individual contractors from the United Nations International Computing Centre, the United Nations Office for Project Services, and a third party service provider. The approved UNGSC budget for ICT support for the year 2015/16 was $32.5 million.

9. According to the Secretary-General's bulletin ST/SGB/2007/5, the United Nations Archives and Records Management Section (UNARMS) is responsible for establishing the policy and standards for the structure, content and context of electronic records to ensure that they are accurately created, captured, preserved, and remain accessible for as long as the electronic record is retained.

10. Comments provided by DFS and UNARMS are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

11. The objective of the audit was to assess the adequacy and effectiveness of controls over the management of email and ICT security in DFS.

12. This audit was included in the 2016 risk-based work plan of OIOS due to the risks (including information security risks) associated with the high dependency of DFS and field offices on email systems.

13. OIOS conducted this audit from March to June 2016. The audit covered the period from January 2014 to June 2016. Based on an activity-level risk assessment, the audit covered higher and medium risks in DFS, which included risk management, ICT support systems, and security policies.

14. The audit methodology included: (i) analyzing ICT policies, standard operating procedures, controls and guidelines; (ii) interviewing key personnel; (iii) reviewing data; (iv) testing the effectiveness of governance, operations and security arrangements; (v) conducting walkthroughs of email processes and procedures; (vi) conducting vulnerability assessments and network port mapping; (vii) performing tests to detect open relays; (viii) running security scripts on the email server against best practice guidelines; (ix) conducting physical verification tests of the data centre in Valencia; and (x) reviewing the relationships between SGITT and other third party service providers.

III. OVERALL CONCLUSION

15. DFS had implemented some good controls and practices such as network segmentation, multiple layers of security built into the ICT infrastructure, best practice certifications, and active-active disaster recovery infrastructure. However, some control weaknesses were identified in the management of email and ICT security, including: (i) inadequate log management procedures; (ii) weak configuration management procedures; (iii) limited guidelines for the management of email records; (iv) gaps in the security configuration of the email server; (vi) lack of security policies for managing email clients and mobile devices; (vii) weak network access control procedures and active directory configuration; (viii) weak role-based access controls; and (ix) lack of a formalized vulnerability assessment plan.

IV. AUDIT RESULTS

A. Risk management

Need to formalize and implement log management procedures

16. The Office of Information and Communications Technology (OICT) had established a technical procedure defining the requirements for monitoring and managing the logs of United Nations ICT systems to detect malfunctions, performance degradation, anomalous events, or unauthorized activities.

This procedure defined, *inter alia*, the details related to: (i) monitoring of system activities; (ii) logging, activating logging, and list of activities that should be logged; (iii) log storage, retention and disposal and protecting sensitive data; (iv) log review, analysis, escalation procedures, and tools; and (v) log protection and security controls for access and modification of logs.

17. In January 2016, DFS issued a centralized log management and audit architecture document (MIS-DCSS-2001). However, this document was not formalized and implemented. Also, there was no evidence that a risk assessment had been performed to identify the critical activities requiring logging, monitoring and reviewing. The following control weaknesses were noted in this area:

(i) In most cases, logs were enabled by default but the schedule for their periodic review was not established (i.e., the firewall security logs were not periodically reviewed). OIOS reviewed the firewall logs and identified failed attempts to access the checkpoint firewall. Similarly, although the creation and deletion of all virtual machines[1] and the creation and deletion of system level objects were logged, these logs were not periodically reviewed.

(ii) The role of discovery management[2] should be granted on a need-to-know basis and restricted to very few users with their activity regularly monitored. OIOS analysis of the use of this role within the email environment identified nine super user accounts with discovery management role. There were no compensating controls in place to ensure that this privilege was correctly used, since these logs were not monitored.

(iii) Although, mailbox auditing was enabled on a few email boxes, there were no defined criteria for using the "mailbox audit logging" feature[3].

18. Inadequate implementation of log management procedures could prevent DFS from detecting malicious attempts to gain unauthorized access and potentially compromise the integrity of the email system.

(1) DFS should formalize and implement its centralized log management and audit architecture procedures to ensure systematic review of system logs.

DFS accepted recommendation 1 and stated that it is currently preparing an implementation plan to address this recommendation. Recommendation 1 remains open pending receipt of evidence of the formalization and implementation of a centralized log management and audit architecture procedures for the systematic review of system logs.

Need to document and implement policies and procedures for the management of email records

19. The Secretary-General's bulletin on record-keeping and management of United Nations archives (ST/SGB/2007/5) states that email messages created and received by the Organization constitute records because they provide evidence of and information about its business transactions. The bulletin mandates UNARMS to establish a policy and standards for the structure, content and context of electronic records to ensure that they are accurately created and captured in their integrity, preserved without alteration, and remain accessible for as long as the electronic record is retained. The bulletin further requires departments and offices to: (i) ensure that email records are identified, managed and stored in accordance with the

[1] A virtual machine is an operating system or application environment installed on software which imitates dedicated hardware.
[2] Discovery management is a role within the email server that allows users to perform searches of email boxes.
[3] The email server system logs the access to email boxes of owners, delegates, and administrators, using a feature called mailbox audit logging.

requirements for record-keeping set forth in the bulletin; and (ii) develop and disseminate guidelines, in keeping with business processes and practice, to prescribe appropriate use of email systems as a means of official communication.

20. The Secretary-General's bulletin ST/SGB/2007/6 defined the classification principles and levels for determining what information should be considered sensitive with particular reference to the electronic transmission of classified information, which must be performed only through the use of protected means of communication.

21. UNARMS provided some guidance on managing emails as records. However, this guidance had not been established as a standard for the Organization. Also, DFS had not defined: (i) data classification procedures for emails based on data sensitivity, content and user groups; (ii) tools to ensure secure communication of sensitive emails; and (iii) email retention procedures in compliance with the requirements of ST/SGB/2007/5.

[redacted]

23. This condition was caused by the absence of defined procedures for email collection, retention and classification which may lead to loss or misuse of official communication. Furthermore, the lack of journaling may limit the ability to retrieve emails for investigation/audit purposes.

(2) UNARMS should document policies/standards to ensure that email records are identified, managed and stored in accordance with the requirements for record-keeping set forth in the Secretary-General's bulletin ST/SGB/2007/5.

UNARMS accepted recommendation 2 and stated that it is currently revising ST/SGB/2007/5 in response to the audit of records management (AH2015/513/04), which will provide clearer guidance on the management of electronic records, including email. The first draft of this revision will be ready for the review of the Office of Legal Affairs (OLA) by 31 December 2016. UNARMS also stated that issuance of the revised Secretary-General's Bulletin will be contingent on various stakeholders, including OICT and OLA. Recommendation 2 remains open pending the receipt of evidence of the policies/standards issued to ensure that email records are managed and stored in accordance with established requirements for record-keeping.

(3) DFS should implement the journaling feature in the email server to enhance controls for the retention and retrieval of email communications.

DFS accepted recommendation 3 and stated it is in consultation with OICT to determine the best way to implement enhanced controls for the retention and retrieval of email. Recommendation 3 remains open pending receipt of evidence demonstrating the implementation of a technical solution to enhance controls over the retention and retrieval of email communications.

Need to update monitoring and incident management procedures

24. The Control Objectives for Information and Related Technology (COBIT) recommend regular monitoring and reporting of emails, based on the criticality and sensitivity of the data contained therein. DFS had established a preventive maintenance schedule and an incident management process to fulfil these requirements.

25. The preventive maintenance schedule and incident management process established by DFS did not include a process to monitor and review email security anomalies. OIOS identified: (i) 8,000 mailboxes which had not been used for six months; and (ii) nine super user accounts enabled for mailbox search. These anomalies were not reviewed by the SGITT ICT Security Team. Furthermore, incident management procedures were not updated to require such anomalies to be reported as an incident for review and remediation.

26. This condition was due to inadequacy of monitoring procedures which prevented DFS from identifying and reporting instances of unused and obsolete email boxes, which could further lead to the misuse of the email system and loss of confidential information.

(4) DFS should update: (i) the preventive maintenance schedule to include the review and clean-up of unused/obsolete email boxes; and (ii) the incident management procedure to identify security anomalies for implementing timely management actions.

DFS accepted recommendation 4 and stated that it is currently preparing an implementation plan to address the various elements of this recommendation. Recommendation 4 remains open pending receipt of updated procedures relating to: (i) the preventive maintenance schedule to include the review and clean-up of unused/obsolete email boxes; and (ii) incident management procedure to identify security anomalies for implementing timely management actions.

B. ICT support systems

Need to strengthen the configuration and implementation of procedures for managing email operations

27. COBIT recommends: (i) the use of configuration management procedures and an automated central repository to capture and maintain a baseline of configuration items for every system and service. The baseline should also serve as a checkpoint to which to return after changes are made; and (ii) the configuration of application software in accordance with the best practices suggested by vendors and in conformance with internal architecture standards and policies.

28. SGITT had deployed a configuration management database to capture all configuration items. However, configuration management was not centrally owned to ensure completeness and consistency of configuration items in the configuration database. Each service area was responsible for documenting its own service assets. This weakness caused the following:

(i) The database was not complete with a record of all configuration items across all service areas. Therefore, reliance could not be placed on the system for the identification of Internet protocol (IP) addresses of network hosts, network devices and a complete network diagram for SGITT; and

(ii) There was inadequate visibility of the processes and relations between parts, subsystems, and systems for effective control of the entire ICT infrastructure (e.g., no visibility of security vulnerabilities across the virtual and physical ICT infrastructure).

29. DFS had not formalized and implemented a policy for ensuring standardized and secure configuration of the email server.

30. OIOS conducted tests of the email server using standard security scenarios and noted deviations from industry best practices, as follows:

[redacted]

(ii) Mobile devices and other appliances were not adequately configured because the parameter "Do not permanently delete items until database has been backed up" was set to 'False' instead of 'True'; and

[redacted]

31. This condition was caused by inadequate configuration and implementation of procedures and policies for managing email operations which could lead to loss of critical data assets and security breaches, and the provision of outdated information about the entire ICT infrastructure.

(5) DFS should: (i) define responsibility for configuration management; (ii) update the configuration management database with all service assets; (iii) establish procedures to update the comprehensive network diagram; and (iv) formalize and implement policies and standards to manage the security configuration of the email server.

DFS accepted recommendation 5 and stated that: (i) it is reviewing the current configuration management definition plan which will address roles and responsibilities, and address identified gaps for configuration management; (ii) it understands that this recommendation relates to the absence of SAN (Storage Area Network) devices (as 'service assets') from the database and it has now updated the database to include SAN devices; (iii) it is currently preparing an implementation plan to address this recommendation; and (iv) in coordination with OICT, it is in the process of developing standards on security configuration of the email server. Recommendation 5 remains open pending receipt of evidence demonstrating that: (i) the responsibility for configuration management is defined; (ii) the configuration management database has been updated with all service assets; (iii) procedures are established to update the comprehensive network diagram; and (iv) policies and standards are formalized to manage the security configuration of the email server.

[4] A protocol for sending email messages between servers. Most email systems that use the Internet use the "simple mail transfer protocol" to send messages from one server to another.

C. Security policies

Need to define and implement policies and procedures for the management of email clients and mobile devices

32. COBIT recommends the protection of email clients to prevent unauthorised access and malware. Accordingly, email clients should be configured to disable automatic opening of messages and downloading and processing of active content that may compromise the security of the email infrastructure.

33. Furthermore, in accordance with COBIT, mobile device management policies and procedures should be implemented to manage and safeguard data stored and processed on mobile devices (smartphones, laptops, tablets) that access the email infrastructure to protect from unauthorized access, loss of data, and malware infections.

34. DFS users accessed email boxes on the email server using various client applications, including Outlook, Outlook Anywhere, Outlook Web App, mobile devices and other appliances. However, DFS did not define a policy regulating the configuration and management of the security settings of these email clients and mobile devices accessing the email infrastructure.

[redacted]

36. DFS had approximately 800 mail boxes on the previous email system to maintain secure communication with the United Nations Secretariat which was still using the old system. Therefore, DFS was currently managing two email infrastructures which impacted its ability to adequately maintain both infrastructures. [redacted]

37. The absence of adequate policies and procedures regulating the management of email clients and mobile devices may result in the loss of critical data.

(6) DFS should: (i) define a policy for regulating the configuration and management of security settings for email clients; (ii) implement and configure email in accordance with a mobile device management policy; and (iii) assess and mitigate ICT security threats posed by the use of unlicensed email boxes.

DFS accepted recommendation 6 and stated that ICTD is the lead for issuing the policy and it will comply with centrally issued policy in relation to this recommendation. Recommendation 6 remains open pending receipt of evidence demonstrating the: (i) documentation of a policy for regulating the configuration and management of security settings for email clients; (ii) implementation and configuration of emails in accordance with a mobile device management policy; and (iii) assessment and mitigation of ICT security threats posed by the use of unlicensed email boxes.

Need to document and implement periodic vulnerability assessment

38. According to the information security management standard (i.e., ISO 27001) adopted by the United Nations Secretariat, organizations should assess the technical vulnerabilities of their information systems, and implement controls for their mitigation. Periodic testing of ICT systems should be conducted and adequate controls implemented to prevent and reduce the negative impact of the potential exploitation of technical network vulnerabilities (i.e., Out-of-date software versions; missing patches or system upgrades; deviations from the organization's security policy; etc.).

39. SGITT did not document a comprehensive vulnerability assessment plan to cover the entire infrastructure and applications (i.e., scans were not performed on firewalls and the active directory). Additionally, in cases where vulnerability scans were performed, SGITT did not document a remediation plan to address the vulnerabilities identified.

40. During the audit, OIOS, in collaboration with the SGITT ICT Security Team, conducted vulnerability scans on the DFS network. The results of these scans showed some weaknesses with patch management and the lack of a standard security baseline. The scans also identified several exposures to un-authorized access to the email infrastructure.

41. The lack of periodic ICT vulnerability testing could lead to breaches of data security, potential losses of information assets, and unavailability of ICT systems and applications.

(7) DFS should document a schedule for the conduct of periodic vulnerability assessment of its entire ICT infrastructure to proactively identify and address ICT security vulnerabilities in a timely manner.

DFS accepted recommendation 7 and stated that it is preparing a schedule for the conduct of periodic vulnerability assessment of its entire ICT infrastructure. Recommendation 7 remains open pending receipt of evidence demonstrating the conduct of periodic vulnerability assessment of the DFS ICT infrastructure.

Need to improve the security elements of the Windows Active Directory

42. Active Directory is a directory service developed for supporting user logon processes and authentication. DFS established procedures for the governance of the Active Directory infrastructure, its security and design. These procedures specified the policies to be applied to the Active Directory, along with compliance and reporting processes and the definition of roles and responsibilities of the relevant technical teams.

43. OIOS reviewed the policies implemented for the Active Directory infrastructure and noted deficiencies related to backup, security and audit policy configuration.

44. An in-house tool was used to audit the Active Directory. This tool could be modified by the SGITT Active Directory Team. However, the SGITT ICT Security Team did not analyse reports generated using this tool nor did they exercise oversight over the development and deployment of the tool. In addition, the tools used were not specified in the Active Directory design/enterprise security policy documents.

45. This condition was due to the inadequate management of the security elements of the Windows Active Directory and may lead to security breaches and loss of confidential information.

(8) DFS should: (i) assess the ICT security policy settings for the Active Directory and periodically monitor their implementation status; (ii) document the backup policy for the Active Directory; and (iii) establish control over the audit tool for monitoring the Active Directory.

DFS accepted recommendation 8 and stated that it is developing: (i) an assessment plan for ICT security policy settings for the Active Directory which will address periodic monitoring; (ii) the backup policy for the Active Directory; and (iii) processes to formalize control over the audit tool. Recommendation 8 remains open pending receipt of evidence demonstrating the: (i) assessment of ICT security policy setting for the Active Directory and the periodical monitoring of their implementation status; (ii) documentation of a backup policy for the Active Directory: and (iii) establishment of controls over the audit tool for monitoring the Active Directory.

Need to define criteria and implement procedures for access controls

46. User access to systems and applications should be controlled with procedures and mechanisms for requesting, granting, suspending, modifying and terminating access and related privileges. These procedures should apply to all users, for both standard and emergency cases.

47. The organization management role group is one of several built-in role groups that compose the role based access control permissions model in the email server. This role allows administrators that are members of the group to access the entire email organization and perform any task on the email object (with a few exceptions).

48. In SGITT, access to the organization management role group was not adequately managed. Therefore, the administrators had access to their own logs and could delete system mailboxes. In addition, there was a potential conflict in the segregation of duties related to the management of the checkpoint firewall and the Active Directory. OIOS noted the following weaknesses:

(i) Some of the access rights were not mapped in line with best practices for the firewall. For instance, members of the SGITT ICT Security Team were configured as "Domain Super Users;

(ii) The firewall administrator's activities were not reviewed;

(iii) The antivirus software could be disabled by the administrators on the domain controllers on the active directory;

(iv) Administrators had access to the log of their own activities; and

(v) Administrators on the main domain controller could also act as Active Directory schema administrators. None of the activities were independently reviewed.

49. This condition was due to the absence of established criteria for user access, which may lead to unauthorized access and loss of confidential information.

(9) DFS should establish criteria and implement procedures for: (i) granting privileged access rights; (ii) conducting regular reviews of privileged access; and (iii) reviewing and establishing controls over conflicting roles.

DFS accepted recommendation 9 and stated that it is developing a process for granting and reviewing privileged access rights, as well as control procedures related to conflicting roles, to address all aspects

of this recommendation. Recommendation 9 remains open pending receipt of evidence demonstrating the establishment of criteria and implementation of procedures for: (i) granting privileged access rights; (ii) conducting regular reviews of privileged access; and (iii) reviewing and establishing controls over conflicting roles.

V. ACKNOWLEDGEMENT

50. OIOS wishes to express its appreciation to the management and staff of DFS and UNARMS for the assistance and cooperation extended to the auditors during this assignment.

(*Signed*) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of electronic mail and information and communications technology security in the Department of Field Support

Rec. no.	Recommendation	Critical[5]/ Important[6]	C/ O[7]	Actions needed to close recommendation	Implementation date[8]
1	DFS should formalize and implement its centralized log management and audit architecture procedures to ensure systematic review of system logs.	Important	O	Formalize and implement a centralized log management and audit architecture procedures for the systematic review of system logs.	31 March 2017
2	UNARMS should document policies/standards to ensure that email records are identified, managed and stored in accordance with the requirements for record-keeping set forth in the Secretary-General's bulletin ST/SGB/2007/5.	Important	O	Issue policies/standards to ensure that email records are managed and stored in accordance with established requirements for record-keeping.	31 December 2017
3	DFS should implement the journaling feature in the email server to enhance controls for the retention and retrieval of email communications.	Important	O	Implement a technical solution to enhance controls over the retention and retrieval of email communications.	31 December 2018
4	DFS should update: (i) the preventive maintenance schedule to include the review and clean-up of unused/obsolete email boxes; and (ii) the incident management procedure to identify security anomalies for implementing timely management actions.	Important	O	Update procedures relating to: (i) the preventive maintenance schedule to include the review and clean-up of unused/obsolete email boxes; and (ii) incident management procedure to identify security anomalies for implementing timely management actions.	31 March 2017
5	DFS should: (i) define responsibility for configuration management; (ii) update the configuration management database with all service assets; (iii) establish procedures to update the comprehensive network diagram; and (iv) formalize and implement policies and standards to manage the security configuration of the email server.	Important	O	(i) Define responsibilities for configuration management; (ii) Update the configuration management database with all service assets; (iii) Establish procedures to update the comprehensive network diagram; and (iv) Formalize policies and standards to manage the security configuration of the email server.	31 March 2017
6	DFS should: (i) define a policy for regulating the	Important	O	(i) Document a policy for regulating the	30 June 2017

[5] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.
[6] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[7] C = closed, O = open
[8] Date provided by DFS and UNARMS in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of electronic mail and information and communications technology security in the Department of Field Support

Rec. no.	Recommendation	Critical[5]/ Important[6]	C/ O[7]	Actions needed to close recommendation	Implementation date[8]
	configuration and management of security settings for email clients; (ii) implement and configure email in accordance with a mobile device management policy; and (iii) assess and mitigate ICT security threats posed by the use of unlicensed email boxes.			configuration and management of security settings for email clients; (ii) Configure emails in accordance with a mobile device management policy; and (iii) Assess and mitigate ICT security threats posed by the use of unlicensed email boxes.	
7	DFS should document a schedule for the conduct of periodic vulnerability assessment of its entire ICT infrastructure to proactively identify and address ICT security vulnerabilities in a timely manner.	Important	O	Conduct periodic vulnerability assessments of the DFS ICT infrastructure.	31 March 2017
8	DFS should: (i) assess the ICT security policy settings for the Active Directory and periodically monitor their implementation status; (ii) document the backup policy for the Active Directory; and (iii) establish control over the audit tool for monitoring the Active Directory.	Important	O	(i) Assess the ICT security policy settings for the Active Directory and the periodic monitoring of their implementation status; (ii) Document a backup policy for the Active Directory: and (iii) Establish controls over the audit tool for monitoring the Active Directory.	31 March 2017
9	DFS should establish criteria and implement procedures for: (i) granting privileged access rights; (ii) conducting regular reviews of privileged access; and (iii) reviewing and establishing controls over conflicting roles.	Important	O	Establish criteria and implement procedures for: (i) Granting privileged access rights; (ii) Conduct regular reviews of privileged access; and (iii) Review and establish controls over conflicting roles.	31 March 2017

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of electronic mail and information and communications technology security in the Department of Field Support

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	DFS should formalize and implement its centralized log management and audit architecture procedures to ensure systematic review of system logs.	Important	Yes	Director GSC	First quarter of 2017	DFS' comments are reflected in the report.
2	UNARMS should document policies/ standards to ensure that email records are identified, managed and stored in accordance with the requirements for record-keeping set forth in the Secretary-General's bulletin ST/SGB/2007/5.	Important	Yes	Chief, OCSS/ARMS	31 December 2017	ARMS is currently revising ST/SGB/2007/5, in response to the OIOS audit of records management (AH2015/513/04), which will provide clearer guidance on the management of electronic records, including e-mail. The first draft of this revision will be ready for OLA's review by 31 December 2016. Issuance of the revised Secretary-General's Bulletin will be contingent on various stakeholders, including OICT and OLA.
3	DFS should implement the journaling feature in the email server to enhance controls for the retention and retrieval of email communications.	Important	Yes	Directors GSC, ICTD and OICT	Fourth quarter of 2018	DFS requests that our comments reflected in the report be reworded to read; "*DFS accepted recommendation 3 and stated that it is in consultation with OICT to determine the best way to implement enhanced controls for the retention and retrieval of email.*"
4	DFS should update: (i) the preventive maintenance schedule to include the review and clean-up of unused/obsolete	Important	Yes	Director GSC	First quarter of 2017	DFS' comments are reflected in the report.

[1] "Critical" denotes a recommendation which, if not implemented, would most likely lead to the occurrence or recurrence of an identified high risk event with a serious impact on the Organization's mandate, operations or reputation.

[2] "Important" denotes a recommendation which, if not implemented, may lead to the occurrence or recurrence of an identified risk event with an unfavorable or adverse impact on the Organization's mandate, operations or reputation.

APPENDIX I

Management Response

Audit of electronic mail and information and communications technology security in the Department of Field Support

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	email boxes; and (ii) the incident management procedure to identify security anomalies for implementing timely management actions.					
5	DFS should: (i) define responsibility for configuration management; (ii) update the configuration management database with all service assets; (iii) establish procedures to update the comprehensive network diagram; and (iv) formalize and implement policies and standards to manage the security configuration of the email server.	Important	Yes	Director GSC	First quarter of 2017	DFS' comments are reflected in the report.
6	DFS should: (i) define a policy for regulating the configuration and management of security settings for email clients; (ii) implement and configure email in accordance with a mobile device management policy; and (iii) assess and mitigate ICT security threats posed by the use of unlicensed email boxes.	Important	Yes	Director ICTD	Second quarter of 2017	DFS' comments are reflected in the report.
7	DFS should document a schedule for the conduct of periodic vulnerability assessment of its entire ICT infrastructure to proactively identify and address ICT security vulnerabilities in a timely manner.	Important	Yes	Director GSC	First quarter of 2017	DFS' comments are reflected in the report.
8	DFS should: (i) assess the ICT security policy settings for the Active Directory and periodically monitor their implementation status; (ii) document the backup policy for the Active Directory; and (iii) establish control over the audit tool for monitoring the Active Directory.	Important	Yes	Director GSC	First quarter of 2017	DFS' comments are reflected in the report.

APPENDIX I

Management Response

Audit of electronic mail and information and communications technology security in the Department of Field Support

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
9	DFS should establish criteria and implement procedures for: (i) granting privileged access rights; (ii) conducting regular reviews of privileged access; and (iii) reviewing and establishing controls over conflicting roles.	Important	Yes	Director GSC	First quarter of 2017	DFS' comments are reflected in the report.