



INTERNAL AUDIT DIVISION

REPORT 2017/075

Audit of business continuity in the United Nations Assistance Mission in Somalia and United Nations Support Office in Somalia

There is a need to ensure that activities essential to the successful implementation of business continuity and recovery plans are conducted

7 August 2017
Assignment No. AP2017/638/02

Audit of business continuity in the United Nations Assistance Mission in Somalia and United Nations Support Office in Somalia

EXECUTIVE SUMMARY

The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over management of business continuity activities in the United Nations Assistance Mission in Somalia (UNSOM) and the United Nations Support Office in Somalia (UNSOS). The audit covered the period from January 2015 to December 2016 and included reviews of: (a) the governance structure for business continuity activities; (b) risk assessment and business impact analysis; (c) business continuity and recovery plans, and their maintenance, exercise and review; and (d) reporting and recordkeeping.

UNSOM and UNSOS had established business continuity plans in December 2014 and a governance structure to ensure the provision of critical and time-sensitive services in the event of a disruption. The business continuity plans were regularly tested to validate policies, procedures and systems against established standards. Time-critical processes were identified and classified, and adequate reporting and recordkeeping procedures were also established. However, there was a need to ensure that all activities essential to the successful implementation of business continuity and recovery plans were conducted.

OIOS made four recommendations. To address issues identified in the audit, UNSOM and UNSOS needed to:

- Establish maximum tolerable periods for the resumption of critical services following disruptive events;
- Periodically conduct and properly document risk assessment and impact analysis for the whole Mission area and develop appropriate mitigating strategies;
- Up-date its business continuity and recovery plan to ensure it includes current information and adequately reflect changes to operations; and
- Ensure all staff with business continuity responsibilities are trained.

UNSOM and UNSOS accepted the recommendations and had initiated action to implement them.

CONTENTS

	<i>Page</i>
I. BACKGROUND	1
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	1
III. OVERALL CONCLUSION	2
IV. AUDIT RESULTS	2-7
A. Governance structure for business continuity activities	2-3
B. Risk assessment and business impact analysis	3-4
C. Business continuity and recovery plan	4-5
D. Maintenance, exercise and review of business continuity and recovery plan	5-7
E. Reporting and recordkeeping	7
V. ACKNOWLEDGEMENT	7
ANNEX I Status of audit of audit recommendations	
APPENDIX I Management response	

Audit of business continuity in the United Nations Assistance Mission in Somalia and United Nations Support Office in Somalia

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of business continuity in the United Nations Assistance Mission in Somalia (UNSOM) and the United Nations Support Office in Somalia (UNSOS).
2. Business continuity management (BCM) is a holistic management process intended to strengthen an organization's ability to respond to risks and continue important and time-critical business processes following a disruptive event. The United Nations business continuity strategy is incorporated into its policy on Organizational Resilience Management System (ORMS) which came into effect on 1 December 2014. The ORMS policy requires UNSOM and UNSOS to continuously improve management of operational risks and coordinate policies, processes and procedures relevant to improving security, preparedness, response, business continuity and recovery in case of disruptive incidents.
3. UNSOM and UNSOS have an emergency preparedness plan to govern their business continuity activities. The core elements of the emergency plan are: crisis management framework, business continuity and recovery (BCR) plan; information technology disaster recovery plan; emergency medical mass casualty incident protocol; staff victim support plan; and country security plan.
4. The UNSOM Chief of Staff and UNSOS Director have overall responsibility for business continuity activities in UNSOM and UNSOS respectively. The Integrated Information Hub within the UNSOM Office of the Chief of Staff has the day-to-day coordination responsibility for business continuity for both UNSOM and UNSOS. At the time of the audit, the Hub had four staff.
5. Comments provided by UNSOM and UNSOS are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

6. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over management of business continuity activities in UNSOM and UNSOS.
7. This audit was included in the 2017 risk-based work plan of OIOS due to the operational and reputational risks related to the inability to continue operations.
8. OIOS conducted this audit in February and March 2017. The audit covered the period from January 2015 to December 2016. Based on an activity-level risk assessment, the audit covered higher and medium risks areas and included reviews of: (a) the governance structure for business continuity activities; (b) risk assessment and business impact analysis; (c) BCR plans, and their maintenance, exercise and review; and (d) reporting and recordkeeping.
9. The audit methodology included: (a) interview of key personnel involved in business continuity activities; (b) review of relevant documentation; (c) analytical review of data; and (d) physical inspection of communication facilities in Mogadishu.

III. OVERALL CONCLUSION

10. UNSOM and UNSOS had established a joint BCR plan in December 2014 and a two-tier governance structure to ensure the provision of critical and time-sensitive services in the event of a disruption. The plan was regularly tested to validate policies, procedures and systems against established standards, time-critical processes were identified and classified and there was adequate reporting and recordkeeping. However, UNSOM and UNSOS needed to ensure that activities essential to the successful implementation of its BCR plans were conducted.

IV. AUDIT RESULTS

A. Governance structure for business continuity activities

Two-tier governance structure for business continuity activities was established

11. The Secretary-General's report on ORMS (A/67/266) requires UNSOM and UNSOS to establish a two-tier governance structure comprising a high-level body to make business continuity policy decisions and an operational team to implement these policies and decisions. Additionally, the United Nations crisis management framework for Somalia requires the two-tier governance structure to be composed of core and non-core members.

12. OIOS review of after-action review reports, minutes of meetings and interviews with key staff showed that UNSOM and UNSOS had established a two-tier governance structure comprising: a crisis management team (CMT) responsible for making strategic decisions regarding business continuity planning and activation of the plan; and a crisis management centre working group responsible for coordinating United Nations response to crisis in Somalia. Both the CMT and the working group had core and non-core members that included representatives from UNSOM, UNSOS, the African Union Mission in Somalia and United Nations agencies, and funds and programmes operating in Somalia. There were clear roles and responsibilities between the CMT and the working group and they met regularly to deliberate on crisis management issues including business continuity and following any incident that had the potential to disrupt operations. Minutes of meetings were maintained and decisions and recommendations were implemented. There were also appropriate arrangements in place for information sharing between the management team and the working group.

13. OIOS concluded that an effective governance structure was established for the overall emergency management system in UNSOM and UNSOS.

Time-critical business processes were identified and classified

14. The Secretary-General's report on ORMS requires senior management of UNSOM and UNSOS to identify and endorse critical services that must be continued or quickly recovered following a disruptive event.

15. Senior management of UNSOM and UNSOS had delegated the identification and classification of time-critical services and related business processes to the respective heads of sections/units. These sections/units had identified their critical business functions and classified 49 of 68 related business processes and activities as critical and assigned a recovery time of up to four hours after a disruptive event. The critical functions, processes and activities were endorsed by senior management of UNSOM and UNSOS and incorporated into the BCR plan.

16. OIOS concluded that UNSOM and UNSOS had identified and classified all critical services and related business processes.

Need to establish maximum tolerable periods for the resumption of critical services

17. The Department of Management template for a business continuity plan introduced in 28 September 2016 requires the establishment of maximum tolerable period for resuming critical services following a disruptive event. UNSOM and UNSOS had not yet established maximum tolerable periods for the resumption of critical services had not been established. This is because UNSOM and UNSOS were not aware about the new requirement and was yet to use the Department of Management template.

(1) UNSOM and UNSOS should establish maximum tolerable periods for the resumption of critical services following disruptive events.

UNSOM and UNSOS accepted recommendation 1 and stated that following the ORMS workshop held in April 2017 and with guidance from the ORMS focal points, the UNSOM/UNSOS BCR plan would be updated to reflect the new format, which grouped the business processes by critical services and the maximum tolerable periods of disruption. Recommendation 1 remains open pending receipt of a copy of the updated BCR plan indicating the maximum tolerable periods for the resumption of critical services following disruptive events.

B. Risk assessment and business impact analysis

Need to strengthen risk assessment and business impact analysis

18. The United Nations BCM Policy (January 2008) requires UNSOM and UNSOS to conduct risk assessment and business impact analysis and prioritize identified risks. The Departments of Peacekeeping Operations and Field Support (DPKO/DFS) template require the risk assessment to be updated annually.

19. OIOS review of critical business processes and impact analysis showed that UNSOM and UNSOS, with the help of experts from the Department of Management, conducted a multi-dimensional risk assessment exercise and business impact analysis exercise in September 2014. The assessment and analysis: (a) covered environmental disaster, organized and/or deliberate disruptions, loss of utilities and service, serious information security incidents, information and telecommunication systems threats, and software vulnerabilities; (b) identified threats and associated risks that could disrupt operations in Mogadishu; and (c) categorized and prioritized identified risks as high, medium and low based on likelihood of occurrence and impact. However:

- UNSOM and UNSOS had not updated their risk assessment since September 2014 and were of the view that there would not be significant changes to their previous assessment; and
- The 2014 risk assessment and impact analysis only covered operations in Mogadishu and did not cover other Mission areas in Somalia, and those in Nairobi and Mombasa in Kenya. UNSOM explained that the focus on Mogadishu was intentional to gain experience with the aim of expanding the process over time to the rest of the Mission area and did not consider risks in the other areas to differ significantly. However, as no risk assessment and business impact analysis had been done of the entire Mission area, it was not clear how UNSOM determined that the risks in other areas of operations were similar to the risks identified in Mogadishu.

20. Additionally, UNSOM and UNSOS updated their BCR plans in 2015 and 2017 without formally conducting risk assessments and business impact analyses. Due to the lack of comprehensive risk

assessment and impact analysis and identification of suitable mitigating measures, there was a risk that UNSOM and UNSOS would not be adequately prepared to promptly resume critical services and related processes after a major disruptive event.

(2) UNSOM and UNSOS should periodically conduct and properly document risk assessment and impact analysis covering all Mission areas and develop appropriate mitigating strategies.

UNSOM and UNSOS accepted recommendation 2 and stated that the Mission was in the process of updating the risk assessment and impact analysis covering all Mission areas in Somalia and Kenya. Recommendation 2 remains open pending the receipt of a copy of the updated risk assessment and impact analysis covering all Mission areas and the corresponding mitigating strategies.

C. Business continuity and recovery plan

Need to update the BCR plan

21. The United Nations framework on ORMS (A/RES/67/254) requires UNSOM and UNSOS to develop, implement, exercise and maintain a BCR plan based on their risk assessment, business impact analysis and prioritization of identified risks. The plan should outline: (a) critical business processes, critical staff, risk mitigation strategies and recovery procedures for each unit; (b) overall roles and responsibility and accountability for business continuity, plan activation, decision-making and activation processes; and (c) information technology systems and applications, vital records, storage facilities and list of critical business partners.

22. UNSOM and UNSOS had developed a combined BCR plan for Mogadishu operations, which was approved by their senior management in December 2014. The plan was subsequently reviewed by the DPKO/DFS Organizational Resilience Programme Officer, and updated in December 2015 and January 2017 to include all Mission areas. However:

- While the sections of the BCR plan related to UNSOM contained all the required elements; the sections for UNSOS did not include details such as overall responsibility and accountability for business continuity, names of representatives on the CMT, description of responsibilities of CMT members, names of critical staff, description of information and technology systems, description of vital records, and key vendor/supplier information. This was because UNSOS did not have a business continuity focal person for 2015/16 and only appointed its focal person in March 2017 to oversee the process;
- The BCR plan did not contain a list of alternate operational locations in the event of a disruption as the necessary arrangements had not been completed;
- The assumptions in the BCR plan of 2015 and 2017 were the same as those in the 2014 BCR plan even though the 2017 BCR plan covered all Mission areas and the 2014 plan was for Mogadishu only. Also, the operational and security environment, which had changed since 2014 was not reflected;
- The 2014 and the updated 2015 and 2017 BCR plans identified Entebbe as the alternate devolution location following a disruption. However, UNSOM and UNSOS advised that the data centre in the Regional Service Centre in Entebbe had been discontinued since 2014 and was taken over by the Cloud which was hosted in the United Nations Global Service Centre in Brindisi and the United Nations Support Base in Valencia. UNSOM and UNSOS also advised that staff were

relocated to Nairobi and Mombasa in 2015 when the need arose and these locations would be used again if necessary. However, the updated BCR plan did not reflect these changes; and

- Some of the mitigating strategies derived and developed from the business impact analysis exercise were not adequate. For example, the mitigating strategy for staff of the Finance Unit of UNSOS to manage imprest cash following a disruptive event in the Office was to work from home. This strategy was not practicable in Mogadishu as their office and home were in the same vicinity. UNSOM and UNSOS explained that the essence of the work-from-home arrangement was to work from a location other than assigned offices and that staff were regularly required to undertake alternate working arrangements due to security lockdowns and network connectivity issues.

23. The above occurred because UNSOM and UNSOS did not adequately review their risk assessments and business impact analyses when updating the BCR plan. As a result, there was a risk that UNSOM and UNSOS may not be able to effectively and efficiently recover critical business processes and activities after a disruptive event.

(3) UNSOM and UNSOS should up-date its business continuity and recovery plan to ensure it includes current information and adequately reflect changes to operations.

UNSOM and UNSOS accepted recommendation 3 and stated that they were in the process of updating the BCR plan according to the new format provided during the ORMS workshop in April 2017. Recommendation 3 remains open pending receipt of evidence that, based on up-dated and comprehensive risk assessments and business impact analyses, the UNSOM/UNSOS BCR plan is revised to reflect current information and changes to operations.

D. Maintenance, exercise and review of BCR plan

Need to train staff responsible for business continuity activities

24. ORMS requires UNSOM and UNSOS to conduct an annual awareness campaign that includes a staff emergency day to ensure staff and management are aware of emergency management (including business continuity) plans and procedures and to continuously familiarize crisis managers on the decision-making process and identify gaps in emergency management plans. Also, the ORMS maintenance, exercise and review regime requires all staff with business continuity responsibilities to be trained, particularly staff responsible for time-critical functions.

25. An awareness exercise was conducted in April 2016 for UNSOM and UNSOS staff covering: planning, safety and security; situational awareness; crisis decision-making processes; coordination and communication; and resource management. The Mission explained that in coordination with counterparts at the United Nations Headquarters in New York, it was agreed to postpone the 2015 awareness exercise to 2016. A roadshow to sensitize the regional offices on business continuity was held in August 2016. A staff emergency day was not organized because on several occasions in 2015 and 2016 there were emergency situations due to terrorist attacks. The generic awareness materials on crisis management, developed by the UNSOM Office of the Chief of Staff/Coherence and Effectiveness Group, to create awareness among staff were only available to a limited number of staff.

26. However, due to lack of oversight, some UNSOM and UNSOS staff listed as critical in the 2015 and 2017 BCR plans had not received the necessary training on business continuity. This included, for example, the spokesperson of the Strategic Communication and Public Affairs Group, planning officers in the Rule of Law and Security Institution Group, the designated focal person for business continuity in the Political Affairs and Monitoring Group and the Human Resources Section of UNSOS.

27. Therefore, while UNSOM and UNSOS had implemented procedures to raise emergency and business continuity awareness, and efforts were underway to intensify staff awareness, there was a need to ensure all staff with critical business continuity responsibilities were adequately trained to perform their functions.

(4) UNSOM and UNSOS should take action to ensure all staff with business continuity responsibilities are trained.

UNSOM and UNSOS accepted recommendation 4 and stated that ORMS and business continuity focal points would continue to update the list of staff with business continuity responsibilities and provide the necessary awareness exercise training. Recommendation 4 remains open pending receipt of evidence that all staff with business continuity responsibilities have been trained.

Business continuity plans and activities were tested

28. The United Nations Policy on BCM/ORMS requires UNSOM and UNSOS to test the BCR plan to validate policies, procedures and systems against established standards and update the plan to reflect lessons learned. The testing should include: (a) annual simulation exercises; (b) quarterly test of emergency notification system; (c) bi-annual telecommuting exercise and staff meetings using peer-to-peer technology; (d) annual exercise of devolution arrangements; (e) annual fail-over tests; and (f) annual functional tests.

29. OIOS review showed that: (a) one test and one simulation exercise were conducted by the UNSOS Geospatial Information Technology and Telecommunications Section (GITTS) to validate the section's recovery time objectives in 2016; (b) real life devolution exercises were carried out by UNSOM and UNSOS in 2015 and 2016 following disruptions when staff were successfully devolved to Nairobi, Kenya where they were able to telecommute and the emergency notification system was activated; and (c) six fail-over tests/incidents were handled by the UNSOS GITTS in 2016 and after-action reports were produced. Lessons learned from the tests, simulations and actual events were used to improve the existing plans. A simulation exercise to demonstrate reliability, high availability and performance in the event of a major technological outage at one of the two data centres and a partial failure were planned for 2017 but had not been conducted at the time of the audit.

30. OIOS physical inspection of communication facilities in Mogadishu and tests of equipment in Mogadishu, Nairobi and Mombasa, review of critical business processes and related mitigating strategies, showed that, in general, critical staff were aware of their business continuity roles and responsibilities although they were not always formally included in the BCR plan as referred to above. Critical staff were also adequately equipped with access to functioning mobile phones, external faxes and radios and were aware of the types of backup files maintained, their locations and how to access them.

31. The alternate locations for business continuity for the various sections included Mombasa and Nairobi, which OIOS assessed were adequately equipped to serve as alternate locations for business continuity. The review also showed that the Human Resources Section of UNSOS was taking steps to prepare a recovery plan with a critical staff list while the Budget and Finance Section was in the process of updating the critical staff list as it included staff who had left the Mission.

32. OIOS concluded that adequate controls exist to test, validate and update the emergency preparedness and business continuity readiness of UNSOM and UNSOS.

E. Reporting and recordkeeping

Adequate reporting and recordkeeping procedures were established

33. DPKO/DFS Code Cable on the implementation of ORMS in peacekeeping operations require UNSOM and UNSOS: (a) to provide an annual business continuity status update to the Department of Management; and (b) ORMS focal points to prepare and maintain a crisis management quick reference guide. Additionally, the terms of reference of the focal points require them to maintain updated copies of relevant policies/plans/checklists on two flash memory drives - one held by the Head of Mission/Office of Chief of Staff and the other by the focal point.

34. The focal unit of UNSOM, under the leadership of the Chief of Staff, was given responsible for reporting and recordkeeping. The UNSOM focal point maintained relevant policies, plans and other documents regarding BCM/ORMS, but these were kept on the official computer instead of on a flash drive. Furthermore, the policies, plans and other documents were not duplicated for the Head of Mission. UNSOM explained that this was because of the constantly changing nature of policies and plans and the impracticality of the Head of Mission and/or Chief of Staff having a flash drive with them at all times. However, during the audit, the flash drives with relevant crisis management and business continuity documents were prepared and distributed to the Head of UNSOM and the two deputies as well as the Chief of Staff and Head of UNSOS. UNSOM and UNSOS also prepared a United Nations Somalia crisis management quick reference guide to act as a handy document during crisis. BCM/ORMS status updates were prepared and submitted to the Department of Management on 8 September 2015 and in July 2016.

35. OIOS concluded that adequate controls were established to ensure periodic reporting and recordkeeping on business continuity.

V. ACKNOWLEDGEMENT

36. OIOS wishes to express its appreciation to the management and staff of UNSOM and UNSOS 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

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity in the United Nations Assistance Mission in Somalia and United Nations Support Office in Somalia

Rec. no.	Recommendation	Critical ¹ / Important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
1	UNSOM and UNSOS should establish maximum tolerable periods for the resumption of critical services following disruptive events.	Important	O	Receipt of the updated BCR plan indicating the maximum tolerable periods for the resumption of critical services following disruptive events.	30 November 2017
2	UNSOM and UNSOS should periodically conduct and properly document risk assessment and impact analysis for all Mission areas, and develop appropriate mitigating strategies.	Important	O	Receipt of a copy of the updated risk assessment and impact analysis covering the whole mission area and the corresponding mitigating strategies.	31 January 2018
3	UNSOM and UNSOS should up-date its business continuity and recovery plan to ensure it includes current information and adequately reflect changes to operations.	Important	O	Receipt of evidence that, based on up-dated and comprehensive risk assessments and business impact analyses, the UNSOM/UNSOS BCR plan is revised to reflect current information and changes to operations.	31 December 2017
4	UNSOM and UNSOS should take action to ensure all staff with business continuity responsibilities are trained.	Important	O	Receipt of evidence that all staff with business continuity responsibilities have been trained.	31 October 2017

¹ 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.

² 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.

³ C = closed, O = open

⁴ Date provided by UNSOM and UNSOS in response to recommendations.

APPENDIX I

Management Response

Management Response

Audit of business continuity in the United Nations Assistance Mission in Somalia and United Nations Support Office in Somalia

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNSOM and UNSOS should establish maximum tolerable periods for the resumption of critical services following disruptive events	Important	Yes	- Chief Integrated and Information Hub UNSOM - Sr. Special Assistant to ASG UNSOS - Chief Mission Support Centre (MSC)	November 2017	Following the Organizational Resilience Management System Workshop (ORMS) held last April 2017, and with guidance from the ORMS focal points, the UNSOM / UNSOS Business Continuity Plan will be updated to reflect the new format which groups the business processes by critical services and the maximum tolerable period of disruption.
2	UNSOM and UNSOS should periodically conduct, properly document risk assessment and impact analysis for the whole mission area and develop mitigating strategies suited to risks faced in the mission area.	Important	Yes	- Chief Integrated and Information Hub UNSOM - Risk Management and Compliance Officer UNSOS	January 2018	UNSOM and UNSOS is in the process of updating the risk assessment (RA) and impact analysis (IA) which covers all Mission areas in Somalia and Kenya. The reviewed Risk Register is expected to be finalized by January 2018.

¹ 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.

² 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.

Management Response

Audit of business continuity in the United Nations Assistance Mission in Somalia and United Nations Support Office in Somalia

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
3	UNSOM and UNSOS should take adequate and effective review actions to ensure comprehensive and proper updating of their business continuity/recovery plan.	Important	Yes	- Chief Integrated and Information Hub UNSOM - Sr. Special Assistant to ASG UNSOS - Chief Mission Support Centre (MSC)	December 2017	As mentioned in the Draft Audit Report, UNSOM has complied with the required elements of the BC/R plans. For a more comprehensive BC/R plan, the other Mission areas in Somalia will also be incorporated, as well as reflect the alternate relocation sites in the event of disruption of operations. UNSOM and UNSOS are currently updating their BC/R plan according to the new format provided during the last ORMS Workshop in April 2017.
4	UNSOM and UNSOS should monitor and ensure all staff with business continuity responsibilities are trained.	Important	Yes	- Chief, Integrated Information Hub, UNSOM - Sr. Special Assistant to ASG UNSOS - Chief Mission Support Centre (MSC)	October 2017	Due to the fluidity of staff movement, ORMS and BC focal points will continue to update the list of all staff with business continuity responsibilities and provide the necessary awareness exercise training.