INTERNAL AUDIT DIVISION

REPORT 2017/151

Audit of business continuity in the United Nations Interim Force in Lebanon

The Mission needed to develop and implement a mission-wide business continuity plan, ensuring cohesion with other emergency preparedness plans

20 December 2017
Assignment No. AP2017/672/05

Audit of business continuity in the United Nations Interim Force in Lebanon

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of business continuity in the United Nations Interim Force in Lebanon (UNIFIL). The objective of the audit was to determine whether UNIFIL implemented adequate and effective processes to ensure that an appropriate business continuity strategy and plan were developed, implemented and maintained. The audit covered the period from 1 July 2016 to 31 October 2017 and included a review of: (i) governance and strategy; (ii) development and implementation of emergency preparedness plans; (iii) maintenance, exercise and review of emergency preparedness plans, including training and awareness of staff; and (iv) management of data centres.

UNIFIL did not fully implement the Organization Resilience Management System (ORMS) Policy, and therefore it did not have an adequate mission-wide business continuity plan that had provisions to sustain and continue the conduct of business activities during crises and ultimate recovery of normal processes. Also, most of the emergency preparedness plans developed by different Mission components did not include the required risk assessment, identification of critical business processes and requirement to review them annually. The Mission had also not properly set up a mechanism to govern and make decisions on crisis management.

OIOS made six recommendations. To address issues identified in the audit, UNIFIL needed to:

- Develop and execute an action plan to implement ORMS;
- Clarify and establish an appropriate governance structure for crisis management in accordance with the United Nations Crisis Management Policy and update relevant guidance documents of the Mission;
- Develop a mission-wide, coherent business continuity plan;
- Include in its resilience management guidance documents, the requirement for annual updates of emergency preparedness plans and update outstanding plans;
- Establish a monitoring mechanism to ensure that all emergency preparedness plans include testing requirements, responsible mission components carry out the tests and report the lessons learned to senior management and the Policy and Best Practice Unit as well as update Mission personnel; and
- Conduct a full failover testing for the Mission's back-up data facility.

UNIFIL accepted the recommendations and has initiated action to implement them.

CONTENTS

Audit of business continuity in the United Nations Interim Force in Lebanon

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of business continuity in the United Nations Interim Force in Lebanon (UNIFIL).

2. Business continuity management is a holistic management process intended to strengthen an organization's ability to respond to risks and continue critical business processes following disruptive events. It is one of the core elements of the Organization Resilience Management System (ORMS) policy approved by the General Assembly in June 2013 (A/RES/67/254). The Policy aims to build the Organization's resilience and ability to deal with crises in a comprehensive, coherent and coordinated manner to better protect United Nations personnel and assets, and to enable it to continue delivering its mandates. The High-Level Committee on Management (HLCM) also requires the United Nations system organizations to develop business continuity policies/strategy and plans.

3. The UNIFIL Head of Mission intends to assign the responsibility to coordinate ORMS to the Office of the Mission Chief of Staff, pending the establishment of related post expected in July 2018. The Mission Support Centre under the Division of Mission Support was previously responsible for the coordination of ORMS. The Joint Operations Centre (JOC) and the military J5 Branch are responsible for developing policies and procedures on business continuity and crisis management. In addition, the military J7 Branch is responsible for coordinating relevant exercises and training activities and together with the Policy and Best Practices Unit, facilitating the implementation of the lessons learned.

4. Comments provided by UNIFIL are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

5. The objective of the audit was to determine whether UNIFIL implemented adequate and effective processes to ensure that appropriate business continuity strategy and plan were developed, implemented and maintained.

6. This audit was included in the 2017 risk-based work plan of OIOS due to operational and reputational risks related to inability to continue operations at defined levels and periods in cases of disruptive events affecting UNIFIL. During recent years, United Nations operations have become targets of increasing violence and malicious acts and have also suffered from natural disasters. Such events can cause serious disruptions in operations and impede the United Nations' ability to deliver time-critical services.

7. OIOS conducted this audit from July to September 2017. The audit covered the period from 1 July 2016 to 31 October 2017. Based on an activity-level risk assessment, the audit covered higher and medium risk areas in business continuity management, which included: (i) governance and strategy; (ii) development and implementation of emergency preparedness plans; (iii) maintenance, exercise and review of emergency preparedness plans, including training and awareness of staff; and (iv) management of data centres.

8. The audit methodology included interviews of key personnel and reviews of relevant documentation.

9. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

III. AUDIT RESULTS

A. Governance and strategy

Mission has not fully implemented the ORMS Policy

10. The ORMS Policy, promulgated in August 2015, requires field missions to fully implement the Policy by June 2016 and submit annual status reports to the Departments of Peacekeeping Operations and Field Support (DPKO/DFS). The Policy requires missions to develop seven plans[1], including a mission-wide business continuity plan. Missions should also define roles and responsibilities of individuals managing business continuity in their job description, evaluate their performance in the appraisal process, and appoint and train ORMS focal points on an ongoing basis.

11. UNIFIL had not fully implemented ORMS by June 2016 as required. The Mission submitted to DPKO/DFS the ORMS Status Report for the fiscal year 2016/17 in July 2017, which outlined measures undertaken by the Mission in implementing ORMS. However, UNIFIL had not adequately developed two of the seven plans, namely the Crisis Management Plan and the Escalation of Tension Business Continuity Plan. The Crisis Management Plan was still under development, while the Escalation of Tension Business Continuity Plan did not outline mission-wide business continuity activities but primarily focused on logistical support requirements (rations, fuel and water) by the Mission Support Centre for military operations. The Escalation of Tension Business Continuity Plan also did not include business continuity activities for the Division of Political and Civil Affairs and the Procurement, Finance and Budget Management, and Human Resources Management Sections. In addition to the five plans developed under the ORMS Policy, UNIFIL had seven other emergency preparedness plans[2], developed by various components of the Mission. These 12 plans provided useful guidance on incident management and logistical support activities such as evacuations, but they lacked proper provisions to sustain and continue the conduct of business activities during crises and ultimate recovery of normal processes. In addition, the emergency preparedness plans focused on man-made hazards such as war or hostilities but did not provide adequate guidance on management of natural calamities such as earthquakes, floods or pandemics.

12. This was because the Mission did not prioritize efforts for full implementation of the ORMS Policy. UNIFIL intends to assign the responsibilities to the Office of the Mission Chief of Staff, but the related post was only expected to be established from 1 July 2018. Other requirements for the implementation of ORMS were still not in place such as the development of an ORMS implementation plan with target implementation dates, appointment and training of ORMS focal points, and inclusion of ORMS related activities in the individual work plans of relevant staff members for performance appraisal. Therefore, risks of disruption of mandate implementation activities and loss of lives, assets or vital records during a crisis remained.

[1] Security Plan; Mass Casualty Incident Response Plan; Business Continuity Plan; Staff Support Plan; Crisis Management Plan; Crisis Communication Plan; and Information and Communications Technology (ICT) Disaster Recovery Plan.

[2] Ensuring Security and Freedom of Movement Contingency Plan; Escalation of Tension Contingency Plan; Protection of Civilians Implementation Plan; Military Support to the UNIFIL Security Plan – South Litani River; Sector West Headquarters Ration Warehouse Security Plan; Fuel Contingency Plan; and Catering Facility and Rations Contingency Plan.

(1) UNIFIL should: (i) develop and execute an action plan to implement the Organization Resilience Management System (ORMS), detailing the responsibilities of relevant mission components with target implementation dates; and (ii) appoint and train ORMS focal points from various mission components indicating their responsibilities in their individual annual performance work plans.

UNIFIL accepted recommendation 1 and stated that it would develop a plan to implement ORMS detailing responsibilities of mission components and target implementation dates, and appoint and train ORMS focal points. Recommendation 1 remains open pending receipt of the plan and evidence of appointment and training of ORMS focal points.

Crisis management decision-making bodies needed to be clarified

13. The United Nations Crisis Management Policy requires missions to establish proper governance mechanisms for handling crisis situations. The Policy further requires missions to leverage existing mechanisms such as security management teams and avoid introducing unnecessary layers of authority.

14. As UNIFIL did not fully implement ORMS, OIOS reviewed the 12 emergency preparedness plans developed by the Mission to assess their compliance with the main features of ORMS. OIOS noted that there was no clarity on the hierarchy, authority and relationship of the respective coordination bodies referred to in the plans to govern and make decisions in emergency situations. The plans mentioned five crisis coordination bodies, namely Crisis Management Team, Mission Leadership Team and Security Management Team at the strategic level and Crisis Coordination Board and JOC Enlarged at the operational level. Three of the plans stated that the Mission Leadership Team was the overall decision-making body for handling crises, two stated the Crisis Management Team, one mentioned the Security Management Team, two indicated the Head of Mission and the Director of Mission Support and the rest did not mention any. In interviews, the military J7 Branch stated that the Mission Leadership Team has the overall authority, while senior managers of the Mission mentioned the Crisis Management Team.

15. The lack of clarity of the governance mechanism for crisis management was caused by the Mission's inadequate implementation and coordination of ORMS as discussed above. In addition, the Mission misunderstood the Crisis Management Policy requirements and established Crisis Management Team and Crisis Coordination Body instead of leveraging existing structures in Mission. The two bodies were required only at United Nations Headquarters locations such as in New York and Geneva. This could lead to confusion and ineffectiveness in the Mission's response to crises.

(2) UNIFIL should clarify and establish an appropriate governance structure for crisis management in accordance with the United Nations Crisis Management Policy and update relevant guidance documents of the Mission.

UNIFIL accepted recommendation 2 and stated that it would align the Mission's crisis management governance structure with the United Nations Crisis Management policy and update related guidance documents accordingly. Recommendation 2 remains open pending receipt of evidence that an appropriate governance structure has been established and guidance documents updated.

B. Development of emergency preparedness plans

Required risk assessments were not adequately conducted

16. The United Nations HLCM guidelines on business continuity risk assessment require missions to identify and assess risks that could cause business interruptions within the broader framework of enterprise risk management (ERM), and take the risks into consideration when developing the missions' business continuity plans and mitigation strategies.

17. Risk assessments were not included in five of the plans and for the other seven, risks were identified but not ranked based on impact and likelihood. The risk assessments were generic and did not show how the identified risks impacted critical processes, activities and applications for purposes of developing mitigation strategies. Further, the risk assessments undertaken were not consistent with one another and the risk register under UNIFIL ERM. For instance, the Mass Casualty Plan rated the risks of armed conflict, terrorism and civil unrest as low, while the ERM risk register rated these risks as either very high or high. The rating of these risks was also different in the Ensuring Security and Freedom of Movement Plan, and Escalation of Tension Contingency Plan.

18. The above could reduce the effectiveness of the Mission's recovery and mitigation strategies for responding to the risks facing the Mission. This was attributed to the absence of business continuity plan and recommendation 3 indicates corrective actions.

Business impact analysis and identification of critical business processes, assets and staff were not done

19. The ORMS Policy requires missions to undertake business impact analyses with a view to identifying critical processes and applications where interruptions could have costly or otherwise damaging implications for the missions. Missions are required to develop appropriate strategies for the continuation of these critical processes when risk events take place, taking into consideration maximum tolerable length of disruption and target recovery time. Further, critical staff, records and assets necessary to perform critical activities should be identified and staff trained on an ongoing basis. ORMS and the Military Support to the Security Plan document require missions to regularly update names of critical staff; and distinguish critical assets between United Nations-owned assets and contingent-owned assets that require troop-contributing countries' approval for deployment outside UNIFIL's area of operations when necessary during crisis.

20. UNIFIL conducted business impact analysis and established target recovery time only for one of the plans, the ICT Disaster Recovery Plan; however, this Plan did not adequately identify critical applications. For instance, the Plan included telephone billing for staff, which was not critical for the Mission's operations, and the Progen Systems, which was no longer used, as critical applications with target recovery time within 24 and 4 hours, respectively.

21. The Mission established a list of critical staff and assets; however, the list of critical staff did not identify the specific individuals' names as it was based on generic job titles, while the list of critical assets did not distinguish between contingent-owned and United Nations-owned assets. The Mission Support Centre stated that it had instructed all sectors to distinguish between contingent-owned and United Nations-owned assets. UNIFIL also explained that it used job titles because of the constant and frequent rotation of military staff. However, without the names of identified personnel, there was no assurance that concerned staff had been appropriately informed about or trained on their responsibilities and provided with the resources they require to carry out the necessary functions in an emergency.

22. The above happened because the Mission did not dedicate sufficient attention to business continuity planning and did not properly assign a Unit responsible for overall coordination and management of business continuity activities in UNIFIL until recently. Inadequate business impact analysis may impede the Mission's ability to maintain and/or recover critical business processes in a timely manner when risk events take place.

(3) UNIFIL should: (i) conduct adequate risk assessments and business impact analyses to identify critical business processes, applications, staff and assets and develop appropriate business continuity strategies with target recovery times; and (ii) develop a mission-wide, coherent business continuity plan.

UNIFIL accepted recommendation 3 and stated that it would conduct risk assessments to identify critical processes and develop appropriate business continuity strategies. The Mission would also develop a mission-wide business continuity plan. Recommendation 3 remains open pending receipt of business continuity strategies and mission-wide business continuity plan.

C. Maintenance, exercise and review of emergency preparedness plans

Emergency preparedness plans should be regularly maintained

23. The ORMS Policy requires missions to update business continuity plans including other emergency preparedness plans annually, which should be approved by the Head of Mission to keep them up-to-date.

24. Seven of the 12 emergency preparedness plans were reviewed and approved by the Head of Mission within the past 12 months, but 5 of them were approved 2 to 6 years ago without recent update despite substantial changes in the operational environment. Seven plans reviewed had either outdated processes, risk assessment or contact details for staff and external stakeholders.

25. The above was because UNIFIL did not dedicate sufficient attention to maintain the plans adequately and was not aware of the ORMS Policy requirement for annual approval of the emergency preparedness plans by the Head of Mission. Eight of the plans either did not mention any review and approval cycle or indicated a cycle of two years. Inadequate and outdated emergency preparedness plans could inhibit the effectiveness of the Mission's resilience management, especially considering the high turnover rate of Mission personnel.

(4) UNIFIL should take steps to: (i) include in its resilience management guidance documents the requirement for annual updates of emergency preparedness plans, in line with the Organizational Resilience Management System Policy; and (ii) update its emergency preparedness plans accordingly.

UNIFIL accepted recommendation 4 and stated that it would include the requirement for annual updates to emergency preparedness plans in its ORMS guidance documents and update the plans accordingly. Recommendation 4 remains open pending receipt of the revised ORMS guidance documents and updated emergency preparedness plans.

Testing of emergency preparedness plans needed improvement

26. The United Nations Policy on Business Continuity Management requires UNIFIL to test its business continuity plans including other emergency preparedness plans, through periodic simulation exercises. Within UNIFIL, the Security Section, Division of Mission Support and military J-7 Branch are

required to coordinate and monitor simulation exercises on staff security and evacuation, logistical support and military component, respectively. UNIFIL's standard operating procedures on Recording and Reporting Lessons Learnt requires preparation of 'after action review' reports to identify lessons learned and submit them to the Policy and Best Practices Unit for consolidation and monitoring implementation of recommended actions, if any.

27. Three of the 12 emergency preparedness plans that were overseen by the Mission Support Centre did not include a requirement to test emergency arrangements; therefore, no simulation exercises were conducted. The Regional Information and Communication Technology Service (RCITS) undertook regular disaster recovery tests. Military J7 Branch that was responsible for testing the remaining eight plans tested six of them (including table top exercise for Mass Casualty Plan) but not the other two, namely the Ensuring Security and Freedom of Movement Plan and Ration Warehouse Security Plan. Further, during the audit period, no 'after action review' reports on the results of the tests were submitted to the Policy and Best Practices Unit.

28. The above was due to absence of an effective monitoring mechanism to ensure that all emergency preparedness plans include testing requirements and for the responsible mission components to carry out the testing and report the lessons learned. Also, 11 of the plans did not include the requirement to submit 'after action review' reports to the Policy and Best Practices Unit. As a result, the effectiveness of business continuity arrangements was not sufficiently validated, especially in view of frequent changes in the Mission personnel. Recommendation 5 below lays out corrective action.

Measures to raise awareness of Mission personnel on business continuity and crisis management needed enhancement

29. The HLCM requires all managers and staff to be aware of business continuity and crisis management plans. UNIFIL's standard operating procedures on Crisis Management require JOC and military J7 Branch to maintain the Crisis Management page and the J7 Branch Training page respectively on UNIFIL intranet to facilitate sharing of information on crisis management with the Mission personnel.

30. During the audit period, the Mission conducted campaigns related to business continuity and general emergency preparedness procedures to raise awareness in the Mission. For instance, UNIFIL conducted three evacuation exercises and regular radio checks for staff and their dependents, regularly issued security messages and broadcasts through text messages and email broadcasts and conducted induction trainings for the Mission personnel including sessions on emergency plans and procedures.

31. However, following the evacuation exercises, there was no formal feedback to staff on their performance although the Security Section reported to the Head of Mission on the identified areas of improvement with regards to staff attitude and behaviour. Further, the information on the intranet was not regularly updated. The JOC Crisis Management page was only updated once on 14 June 2017 during the audit period and contained outdated standard operating procedures. The J7 Branch Training Site could not be accessed.

32. The above happened because the Mission did not implement a feedback mechanism for sharing the results and lessons learned of various crisis management and business continuity exercises undertaken with staff. Also, the Mission did not monitor effective management of the intranet sites by JOC and military J7 Branch. As a result, awareness of the Mission personnel on emergency preparedness and business continuity may not be adequate.

(5)	**UNIFIL should: (i) establish a monitoring mechanism to ensure that all emergency preparedness plans include testing requirements and that the responsible mission**

components carry out the testing and report the lessons identified to senior management and the Policy and Best Practice Unit of the Mission; and (ii) implement a feedback mechanism to share test results and lessons learned with Mission personnel to promote awareness and appropriate behavioural changes. This should include effective management of the intranet sites of Joint Operations Centre and military J7 Branch.

UNIFIL accepted recommendation 5 and stated that it would ensure that all emergency preparedness plans include testing requirements, which would be carried out by mission components and report lessons learned to senior management and the Policy and Best Practices Office. The Mission would also ensure that a feedback mechanism is implemented to promote awareness, including effective management of JOC and military J7 Branch intranet sites. Recommendation 5 remains open pending receipt of evidence of requirements established for testing emergency plans, reporting and sharing of lessons identified and of functioning crisis management intranet sites.

D. Management of data centres

Mission was taking action to enhance fire and physical security at the data centres

33. The United Nations Data Centre Access Manual requires all data centres[3] to have appropriate physical access controls to prevent unauthorized physical access and measures against fire hazards. Minimum access controls required are door locks and security personnel or physical authentication devices, such as biometrics and/or smart cards. Logging of all entries into the data centres is required either electronically or via a manual access register. The Mission is also required to document a matrix of access privileges and approval requirements for different groups of visitors to data centres, which must be updated at least every six months.

34. The Mission did not document the access privilege matrix and approval requirements for entry into the data centres. The primary data centre was fitted with an electronic access system but the log was neither maintained nor reviewed. Instead, a manual access register was in place, which had only two records over 12 months, although several entries into the centre were observed. The back-up data centre was not fitted with an electronic access system and the manual access register in place was also rarely used. Further, surveillance cameras at the primary data centre were mounted in the passage and could therefore not capture activities in the server room. The primary data centre was only equipped with two small manual fire extinguishers, while the secondary data centre had an automated fire suppression system. The Mission assessed fire and physical security at the data centres in March 2017, which included adequate corrective measures to be taken. As the Mission started implementing those measures, OIOS did not make a recommendation on this issue.

Full failover testing of the back-up data centre needed be conducted

35. The UNIFIL ICT Disaster Recovery Plan requires disaster recovery exercises to be conducted on a regular basis. ORMS requires conducting full failover tests on an annual basis.

[3] The United Nations Data Access Manual defines a data centre as "physical or virtual infrastructure used by enterprises to house computer, server and networking systems and components for the company's information technology needs, which typically involve storing, processing and serving large amounts of mission-critical data to clients in a client/server architecture" and establishes technical procedures to be abode by. The UNIFIL RCITS, however, stated that the references to data centres in the Manual were outdated and some technical procedures required by the Manual would not be applicable at mission level. RCITS stated that it would remove such reference when updating its guidance documents.

36. RCITS conducted disaster recovery exercises in the form of simulation tests and structured walk-throughs twice a year, focusing on three aspects of the Plan: data, connectivity and power sources. However, RCITS did not conduct annual full failover testing of its secondary data centre to assess whether the centre would sustain UNIFIL's critical operations in the event of full failure of the primary data centre. According to the RCITS records, the last full interruption test was conducted in 2013.

37. RCITS stated that the above was because it tested selected aspects of the secondary data centre for in-depth assessments. As a result, there is a risk that critical ICT services may not be recovered in the event primary data centre becomes inoperable. The secondary data centre was the only back-up measure in UNIFIL.

(6) UNIFIL should conduct a full failover testing of its back-up data centre annually to assess its capacity and readiness in the event that the primary data centre becomes unavailable for use.

UNIFIL accepted recommendation 6 and stated that it regularly conducted failover tests of individual service components of the back-up equipment room to drill down into each specific technical area and cause minimal disruption to the client-base during such testing. The Mission would perform periodic full failover tests from the primary equipment room to the back-up equipment room. Recommendation 6 remains open pending receipt of appropriate reports confirming full failover testing of the Mission's back-up equipment room.

V. ACKNOWLEDGEMENT

38. OIOS wishes to express its appreciation to the management and staff in UNIFIL 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 business continuity in the United Nations Interim Force in Lebanon

Rec. no.	Recommendation	Critical[4]/ Important[5]	C/ O[6]	Actions needed to close recommendation	Implementation date[7]
1	UNIFIL should: (i) develop and execute an action plan to implement the Organization Resilience Management System (ORMS), detailing the responsibilities of relevant mission components with target implementation dates; and (ii) appoint and train ORMS focal points from various mission components indicating their responsibilities in their individual annual performance work plans.	Important	O	Receipt of a plan to implement ORMS and evidence of appointment and training of ORMS focal points.	30 September 2018
2	UNIFIL should clarify and establish an appropriate governance structure for crisis management in accordance with the United Nations Crisis Management Policy and update relevant guidance documents of the Mission.	Important	O	Receipt of evidence that an appropriate governance structure for crisis management has been established and guidance documents updated.	30 September 2018
3	UNIFIL should: (i) conduct adequate risk assessments and business impact analyses to identify critical business processes, applications, staff and assets and develop appropriate business continuity strategies with target recovery times; and (ii) develop a mission-wide, coherent business continuity plan.	Important	O	Receipt of business continuity strategies and mission-wide business continuity plan.	30 November 2018
4	UNIFIL should take steps to: (i) include in its resilience management guidance documents the requirement for annual updates of emergency preparedness plans, in line with the Organizational Resilience Management System Policy; and (ii)	Important	O	Receipt of revised ORMS guidance documents and updated emergency preparedness plans.	1 July 2018

[4] 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.
[5] 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.
[6] C = closed, O = open
[7] Date provided by UNIFIL in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of business continuity in the United Nations Interim Force in Lebanon

Rec. no.	Recommendation	Critical[4]/ Important[5]	C/ O[6]	Actions needed to close recommendation	Implementation date[7]
	update its emergency preparedness plans accordingly.				
5	UNIFIL should: (i) establish a monitoring mechanism to ensure that all emergency preparedness plans include testing requirements and that the responsible mission components carry out the testing and report the lessons identified to senior management and the Policy and Best Practice Unit of the Mission; and (ii) implement a feedback mechanism to share test results and lessons learned with Mission personnel to promote awareness and appropriate behavioural changes. This should include effective management of the intranet sites of Joint Operations Centre and military J7 Branch.	Important	O	Receipt of evidence of requirements established for testing emergency plans, reporting and sharing of lessons identified and of functioning crisis management intranet sites.	30 November 2018
6	UNIFIL should conduct a full failover testing of its back-up data centre annually to assess its capacity and readiness in the event that the primary data centre becomes unavailable for use.	Important	O	Receipt of appropriate reports confirming full failover testing of the Mission's back-up equipment room.	31 March 2018

APPENDIX I

Management Response

UNITED NATIONS
INTERIM FORCE IN LEBANON

NATIONS UNIES
FORCE INTERIMAIRE AU LIBAN

CONFIDENTIAL

18 December 2017

To: Ms. Muriette Lawrence-Hume, Chief, New York Audit Service
Internal Audit Division, OIOS

From: Major-General Michael Beary
Head of Mission and Force Commander, UNIFIL

UNIFIL
OFFICE OF THE FORCE COMMANDER

Subject: **Draft report on an audit of business continuity management in UNIFIL (Assignment No. AP2017/672/05)**

1. We refer to your memorandum on the above subject, reference No. IAD: 17-MO1203 dated 13 December 2017. Please find attached UNIFIL's response to the recommendations contained in the subject Draft Report.

2. In following the usual procedure, copies of any supporting documents will only be provided to MERAO based at UNIFIL HQ and will not be transmitted to you with this Mission's response.

Best regards.

Cc: Mr. Effendi Syukur, Audit Focal Point, UNIFIL
Mr. Daeyoung Park, Chief Resident Auditor, MERAO, Internal Audit Division, OIOS
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS

APPENDIX I

Management Response

Audit of business continuity in the United Nations Interim Force in Lebanon

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNIFIL should: (i) develop and execute an action plan to implement the Organization Resilience Management System (ORMS), detailing the responsibilities of relevant mission components with target implementation dates; and (ii) appoint and train ORMS focal points from various mission components indicating their responsibilities in their individual annual performance work plans.	Important	Yes	Mission Chief of Staff	30 Sept. 2018	UNIFIL will (i) develop and implement an ORMS System plan detailing responsibilities of the mission components and target dates for implementation and (ii) and appoint and train ORMS focal points.
2	UNIFIL should clarify and establish an appropriate governance structure for crisis management in accordance with the United Nations Crisis Management Policy and update relevant guidance documents of the Mission.	Important	Yes	Mission Chief of Staff	30 Sept. 2018	UNIFIL will align the mission's crisis management governance structure as per United Nations Crisis Management policy and update related guidance documents accordingly.
3	UNIFIL should: (i) conduct adequate risk assessments and business impact analyses to identify critical business processes, applications, staff and assets and develop appropriate business continuity strategies with target recovery times; and (ii) develop a mission-wide, coherent business continuity plan.	Important	Yes	Mission Chief of Staff	30 Nov. 2018	UNIFIL will (i) conduct risk assessments to identify critical processes and develop business continuity strategies accordingly and (ii) develop a mission wide business continuity plan

[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.

APPENDIX I

Management Response

Audit of business continuity in the United Nations Interim Force in Lebanon

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
4	UNIFIL should take steps to: (i) include in its resilience management guidance documents the requirement for annual updates of emergency preparedness plans, in line with the Organizational Resilience Management System Policy; and (ii) update its emergency preparedness plans accordingly.	Important	Yes	Mission Chief of Staff	1 July 2018	UNIFIL will include the requirement for annual updates to emergency preparedness plans in its ORMS guidance documents as per ORMS Policy and update its emergency preparedness plans accordingly.
5	UNIFIL should: (i) establish a monitoring mechanism to ensure that all emergency preparedness plans include testing requirements and that the responsible mission components carry out the testing and report the lessons identified to senior management and the Policy and Best Practice Unit of the Mission; and (ii) implement a feedback mechanism to share test results and lessons learned with Mission personnel to promote awareness and appropriate behavioural changes. This should include effective management of the intranet sites of Joint Operations Centre and military J7 Branch.	Important	Yes	Mission Chief of Staff	30 Nov. 2018	UNIFIL will (i) ensure that all emergency preparedness plans include testing requirements and that the responsible mission components ensure testing is carried out and that any lessons learned are reports to senior management and the Best Practice Office and (ii) ensure that feedback mechanism is implemented to promote awareness including effective management of the intranet sites of the JOC and J7 Branch.
6	UNIFIL should conduct a full failover testing of its back-up data centre annually to assess its capacity and readiness in the event that the primary data centre becomes unavailable for use.	Important	Yes	Chief RICTS	31 Mar. 2018	UNIFIL routinely and regularly tests fail-over of individual service components of the back-up equipment room in order to drill down deeply into each specific technical area and cause minimal disruption to the client-base during such testing.

APPENDIX I

Management Response

Audit of business continuity in the United Nations Interim Force in Lebanon

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						UNIFIL will perform a periodic full failover test from the primary equipment room to the back-up equipment room.