



# **INTERNAL AUDIT DIVISION**

## **REPORT 2023/009**

---

**Audit of the issuance of identity cards  
and physical access controls in the  
United Nations Mission in the Republic  
of South Sudan**

**The Mission needed to strengthen procedures  
for the authorization and deactivation of the  
United Nations identity cards and controls  
over access to the Mission's premises**

**6 April 2023  
Assignment No. AP2022-633-05**

# **Audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan**

## **EXECUTIVE SUMMARY**

The Office of Internal Oversight Services (OIOS) conducted an audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan (UNMISS). The objective of the audit was to assess the adequacy and effectiveness of procedures to safeguard the United Nations personnel and property by preventing unauthorized access to UNMISS premises. The audit covered the period from 1 July 2021 to 30 June 2022 and included authorization and deactivation of identity cards, information systems control and physical access control.

UNMISS needed to strengthen controls over the process of issuing United Nations identity cards, timely deactivate the identity cards of separated staff, enhance the protection and integrity of data on portable handheld electronic card readers, and implement measures to effectively record and manage access of individuals into the Mission's premises, and improve the supervision of armed guards.

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

- Establish procedures to verify the authenticity of authorized signatories on the request forms to issue United Nations identity cards;
- Issue instructions clarifying the roles of offices and sections to timely inform the Pass and ID Unit about the separation of staff and promptly deactivate United Nations identity cards for separated staff;
- Optimize the synchronization of data between portable handheld electronic card readers and the web-based security application, configure the portable handheld electronic card readers to erase data if the devices are lost, and manually record the entry and exit of personnel with low-cost United Nations identity cards that are not integrated with the system; and
- Improve the monitoring and reporting on the key performance indicators related to the performance of unarmed guards and strengthen the supervision of their work.

UNMISS accepted all recommendations, of which one is implemented, and it has initiated actions to implement the remaining recommendations.

# CONTENTS

I. BACKGROUND	1
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	1-2
III. AUDIT RESULTS	2-7
A. Authorization and deactivation of identity cards	2-3
B. Information systems control	3-5
C. Physical access control	5-6
IV. ACKNOWLEDGEMENT	7
ANNEX I      Status of audit recommendations	
APPENDIX I   Management response	

# **Audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan**

## **I. BACKGROUND**

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan (UNMISS).
2. The Security and Safety Section is responsible for developing and monitoring the implementation of security policies and procedures to maintain the security and safety of the United Nations personnel, premises and assets at the Mission headquarters in Juba and ten field offices. UNMISS had established two contracts with a cumulative not-to-exceed amount of \$38.6 million to provide unarmed security guard services to ensure that access to all its premises is restricted to authorized individuals only. The Guard Force Unit within the Security and Safety Section supervised the unarmed security guards.
3. UNMISS issued three types of security passes to staff and other individuals entering its premises, namely: (a) United Nations identity cards (UNIDs) that are issued by the Security and Safety Section's Pass and ID Unit in Juba to individuals who are authorized to access UNMISS premises, (b) low-cost UNIDs that were introduced in December 2020 to provide access to large numbers of contractors who are authorized to enter the Malakal premises recurrently, and (c) visitor passes that are issued to visitors including short-term contractors at the entry points of UNMISS premises in exchange for identity documents such as valid national identification documents, passport, United Nations Laissez Passer and identity cards issued by other United Nations entities.
4. The contracted unarmed security guards posted at the entry points of UNMISS premises allowed the entry of individuals after checking the validity of their UNIDs using handheld electronic card readers. These devices were integrated with a web-based security application called ONPASS<sup>1</sup> to process and report on the movement of cardholders in and out of UNMISS premises. Visitor passes cannot be scanned by handheld electronic card readers; therefore, visitor entry and exit details are entered manually into logbooks/sheets by the contracted unarmed security guards.
5. UNMISS issued 23,648 UNIDs to its staff and affiliates<sup>2</sup> and 7,755 UNIDs to the staff of United Nations Agencies, Funds and Programmes (UNAFPs) from 1 July 2021 to 30 June 2022. In addition, the Field Security Office in Malakal issued 1,424 low-cost UNIDs to contractors.
6. Comments provided by UNMISS are incorporated in italics.

## **II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY**

7. The objective of the audit was to assess the adequacy and effectiveness of procedures to safeguard the United Nations personnel and property by preventing unauthorized access to UNMISS premises.

---

<sup>1</sup> ONPASS is a web-based reporting application which offers features such as blocking/unblocking UNIDs, tracking, recording, and reporting of entry and exit of all personnel to and from UNMISS compounds. ONPASS is integrated with the third-party software used by the Security and Safety Section to issue UNIDs that can be scanned by the handheld electronic card readers used at the gates.

<sup>2</sup> It includes other non-staff personnel such as contractors and consultants who are authorized to access UNMISS premises by virtue of their functions.

8. This audit was included in the 2022 risk-based work plan of OIOS due to the importance of physical access controls on the safety and security of UNMISS personnel, property and premises.

9. OIOS conducted this audit from September to November 2022. The audit covered the period from 1 July 2021 to 30 June 2022. Based on an activity-level risk assessment, the audit covered higher and medium-risk areas in implementing access control measures, which included: authorization and deactivation of identity cards, information systems control and physical access control.

10. The audit methodology included: (a) interviews of key personnel involved in access control, (b) a review of documents for a random sample of 93 out of 32,827 UNIDs issued during the audit period, (c) physical inspection of the entry points and the perimeter of UNMISS premises at five of the 10 field offices, and (d) analytical review of data from the ONPASS and UNIDs card production systems.

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

### III. AUDIT RESULTS

#### A. Authorization and deactivation of identity cards

##### UNMISS should strengthen controls over the process of issuing United Nations identity cards

12. The standard operating procedures to issue UNIDs require Pass and ID Unit to process the UNIDs only upon the completion and authorization of request forms by the UNMISS Human Resources Management Section (HRMS), UNAFPs or authorized officials from other requesting offices such as UNMISS Sections, Military and Police components.

13. A review of a random sample of 93 out of 32,827 UNIDs issued during the audit period indicated that UNIDs were issued after receipt of approved request forms from HRMS, UNAFPs or other requesting offices within an average of four days from the requested date. However, 30 UNIDs were issued based on request forms signed but not stamped by the requesting offices. Although OIOS did not identify cases where such requests were invalid, the absence of official stamps on request forms may lead to a risk to document integrity. Furthermore, the Pass and ID Unit had not established procedures to compare the signature on request forms with the specimen signatures of designated officials approved by HRMS, UNAFPs or other requesting offices to authorize the issuance of UNIDs.

14. The above occurred because the Pass and ID Unit did not implement standard procedures and establish more robust controls over issuing UNIDs. As a result, there was a risk of issuing UNIDs to unauthorized individuals.

**(1) UNMISS should establish procedures to verify the authenticity of authorized signatories on the request forms to issue United Nations identity cards and ensure that such forms bear the official stamp of requesting offices.**

*UNMISS accepted recommendation 1 and stated that the Pass and ID Unit is currently collecting scans of sample signatures and official stamps from authorized signatories. The scans are also being compiled in a binder.*

### Need to timely deactivate identity cards of separated staff

15. The Security and Safety Section needs to deactivate the UNIDs of separated staff from the date of their separation. The staff checkout process in the Mission is initiated through the Field Support Suite (FSS) application that allows the Pass and ID Unit to deactivate their UNIDs.

16. UNMISS did not timely deactivate the UNIDs of separated staff. A review of active UNIDs as of 19 August 2022 indicated that the UNIDs of 29 individuals who separated from UNMISS remained active after separation for an average of 165 days.

17. The above resulted because: (a) the responsible staff in Pass and ID Unit overlooked the need to deactivate 25 UNIDs in the system during the staff checkout processes; however, they were deactivated subsequently after this was pointed out in the audit; and (b) four staff members departed the Mission without concluding their checkout processes to enable the deactivation of their UNIDs. However, these cards have been automatically deactivated after their expiry dates.

18. Furthermore, a review of the ONPASS database and discussions with the responsible officials indicated that the notifications for staff checkout were not timely sent to the Pass and ID Unit for certain categories of personnel such as military contingents, Formed Police Units, personnel of UNAFPs, vendors, consultants and contractors. The checkout process for these personnel, accounting for 88 per cent (28,926) of the UNIDs issued during the audit period, was initiated outside the FSS application. This had prevented the Mission from timely deactivating the identity cards of separated personnel who initiated the checkout process outside FSS. For example, UNIDs for 126 contractor personnel remained active for an average of 198 days after they were separated from service.

19. The lack of controls to timely deactivate UNIDs of separated staff and other personnel had exposed the Mission to security risks arising from unauthorized access. For example, a review of ONPASS movement reports noted that one national staff accessed the Mission premises after his contract was terminated due to misconduct, and two contractor personnel also accessed the Mission's premises after they were separated from service.

**(2) UNMISS should issue instructions clarifying the roles of offices and sections to timely inform the Pass and ID Unit about the separation of staff and strengthen procedures for the Unit to promptly deactivate United Nations identity cards for separated staff.**

*UNMISS accepted recommendation 2 and stated that it would provide specific guidance on the process and accountability measures in relation to the deactivation of the identity cards upon separation of the authorized holders.*

## **B. Information systems control**

### UNMISS took action to strengthen user access controls over information systems

20. User accounts need to be periodically reviewed to ensure that access rights are commensurate with responsibilities and that such rights are disabled when no longer needed.

21. UNMISS did not regularly review and disable user access rights when they were no longer required. For example, a review of the user access list of the ONPASS system as of 28 September 2022 indicated that 14 individuals had active user accounts with rights to view and download reports such as entry and exit data of individuals and to block or unblock identity card holders' access to UNMISS compounds although

they were separated from UNMISS for periods ranging from one month to four years. However, a review of the ONPASS user access logs indicated that none of these users subsequently accessed ONPASS after their separation. Furthermore, an employee of a contractor had access to ONPASS system since 2019, although his functions did not require such access.

22. After this was pointed out during the audit, the Security and Safety Section disabled these user accounts on 6 October 2022 and introduced measures to monitor user accounts monthly. Since the Mission had already taken action to strengthen the user access control, OIOS did not make a recommendation.

#### Need to strengthen controls over portable handheld electronic card readers

23. The portable handheld electronic card readers need to be configured and integrated with the ONPASS system to ensure data integrity.

24. UNMISS did not optimize data synchronization between the ONPASS system and handheld electronic card readers to enable these devices to access the real-time data entered into the system. OIOS noted a time lag of 4 to 10 hours in data synchronization in 7 out of 34 devices in four field offices. As a result, there was a risk that important information, such as the blocking of UNIDs in ONPASS system, may not be timely captured by the handheld electronic card readers. Furthermore, while handheld electronic card readers can be configured to erase data automatically if they remain idle for eight hours, this was not done as OIOS random tests of 10 devices indicated that data did not erase after staying idle for 10 hours. Consequently, there was a risk of a data compromise if the devices were lost or stolen.

25. Additionally, while the security guards denied access to unauthorized individuals based on the detection by electronic card readers, the ONPASS system incorrectly recorded them as having entered the premises. Also, 1,424 low-cost UNIDs issued to the contractors at the field office in Malakal were not fully integrated with the ONPASS system. As a result, such individuals' entry into and exit from the premises were not recorded in the system. The above increased the risk of inaccurate headcount on the Mission's premises at a given time, especially at the onset of an emergency.

**(3) UNMISS should: (a) optimize the synchronization of data between portable handheld electronic card readers and ONPASS application to ensure data integrity; (b) configure the portable handheld electronic card readers to erase data after they remain idle for the defined period to protect data if the devices are lost; and (c) take measures to record the entry and exit of personnel with low-cost United Nations identity cards that are not integrated with the system.**

*UNMISS accepted recommendation 3 and stated that the Guard Force Unit instructed the unarmed guards to synchronize the handheld electronic card readers every hour. Discussions are being held with the Vendor to update the system to ensure that handheld electronic card readers erase data after they remain idle for a specified period. Furthermore, the Mission is revisiting the current technology to strengthen the recording of low-cost identity cards at entry and exit points.*

#### UNMISS was taking action to register electronic card readers with unique names in ONPASS

26. The handheld electronic card readers are required to be registered in the ONPASS system with unique names to ensure that the access data captured by an individual device is properly identified for ONPASS reporting purposes. However, a review of the registered names of 121 active handheld electronic card readers in the ONPASS system indicated that 23 handheld electronic card readers had duplicates, including 16 that had the generic name "Test". This happened because the Field Technology Section (FTS) did not establish a device naming protocol to identify them uniquely. As a result, individual devices could

not always be associated with the access data they generated making it difficult to manage the devices and the information they produce.

27. Based on preliminary audit results, the Security and Safety Section committed to coordinating with the FTS to ensure that each portable handheld electronic card reader is registered under a unique name. Therefore, OIOS did not make a recommendation.

### C. Physical access control

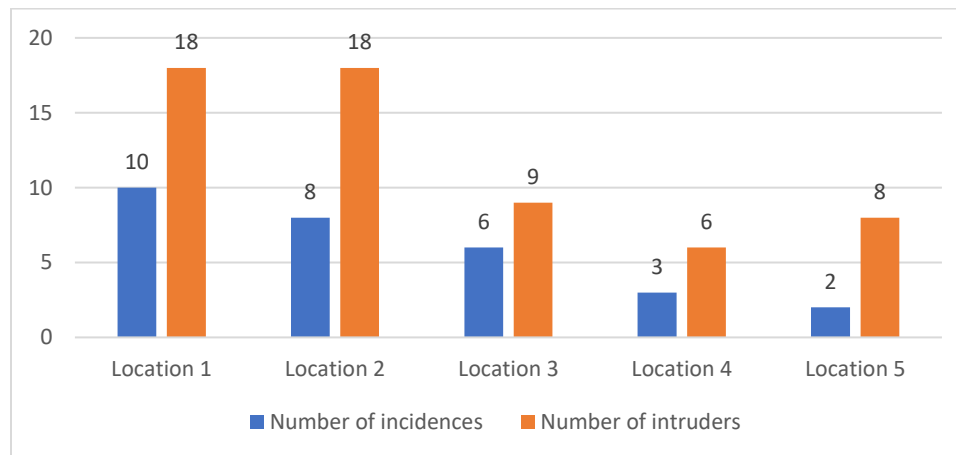
#### Need to strengthen physical access controls

28. An effective physical access control protects UNMISS personnel, property and premises.

a) The Mission has taken measures to strengthen perimeter security

29. A review of security incident logs of unauthorized entries at five field offices during the audit period indicated that 29 incidents involving 59 individuals were reported at these locations, as shown in figure 1 below.

**Figure 1: Unauthorized entries at five field offices during the period July 2021 to June 2022**



Source: Security and Safety Section

30. These intrusions occurred due to vulnerabilities in some sections of the boundary walls. A review of the September 2022 meeting minutes of the Integrated Project Team responsible for monitoring the prioritized Mission projects indicated that UNMISS had planned to reinforce the perimeter wall at Location 1 and was exploring ways to bolster the perimeter walls at the other locations. Furthermore, the Mission had implemented ongoing compensatory measures to enhance perimeter security including installing watch towers along perimeter walls and patrols by military and unarmed security guards. Since the Mission has implemented ongoing measures to strengthen perimeter security, OIOS did not make a recommendation.

b) Need to enhance performance monitoring of unarmed guards

31. The access of personnel and vehicles to UNMISS premises is controlled by contracted unarmed guards posted at the entry points of all premises. The guards perform physical security screening of personnel and vehicles using equipment such as X-ray machines, handheld electronic card readers, walk-through metal detectors and under-carriage mirrors.



32. A review of 115 monthly key performance indicators (KPIs) reports during the audit period indicated that the Security and Safety Section found acceptable performance levels of unarmed guards provided by two contracted vendors in all locations except one on primarily two KPIs: (a) prevention of unauthorized personnel or vehicle entry into UNMISS premises through access-controlled areas; and (b) knowledge to use security equipment such as X-ray machines, handheld electronic card readers and walk-through metal detectors. The Section took corrective actions to address the suboptimal performance of unarmed guards in one location by providing training and deducting performance credits totaling \$2,193 from the corresponding contractor who provided the guards. However, OIOS identified the following weaknesses in the contractor performance monitoring and reporting:

- The monthly review of KPIs of contracted unarmed guards was not done for four months in one location and one month in another.
  - The contractors did not countersign 6 KPIs reports, 5 reports had mandatory sections that were left blank, and an incorrect formula was applied in 22 KPI reports.
- c) Need to enhance controls over visitor access and record management

33. During field visits and discussions with the Security and Safety Section personnel, OIOS identified a need to improve the visitor access and record management system in some locations. For example:

- In one location, visitors were allowed to enter the premises based on authorization letters issued by UNMISS, but neither the copies of such letters were retained, nor the entry and exit details of such visitors were recorded on log sheets. As a result, there were no trails of such visits.
- In four locations, a total of 128 visitor passes were missing. The cases of these missing passes had not been reported to the Special Investigations Unit within the Security and Safety Section due to oversight by the Guard Force Unit.
- Visitor passes were not issued sequentially in three locations, and therefore, controls over the accountability of visitor passes were diminished.

34. Furthermore, the unarmed guards did not manually record the entry details of individuals in the logbook when: (a) staff and visitors from other United Nations entities entered the premises based on identity documents, such as United Nations Laissez Passer which cannot be scanned by handheld electronic card readers, and (b) card readers failed to read and scan the UNIDs for technical reasons.

35. The above occurred due to inadequate supervision by the Guard Force Unit of the performance of unarmed security guards. Consequently, it exposed the Mission to security risks arising from inadequate physical access control.

**(4) UNMISS should: (a) improve the monitoring and reporting on the key performance indicators related to the performance of unarmed guards in all locations; and (b) strengthen the supervision of unarmed guards to effectively record and manage access to the Mission's premises.**

*UNMISS accepted recommendation 4 and implemented it with improved monitoring and reporting of the key performance indicators to address the performance issues of unarmed guards. In addition, the Mission has established a stronger deployment monitoring, reporting and supervision system to enhance performance monitoring of unarmed guards.*

#### **IV. ACKNOWLEDGEMENT**

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

Internal Audit Division  
Office of Internal Oversight Services

## STATUS OF AUDIT RECOMMENDATIONS

## Audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical <sup>3</sup> / Important <sup>4</sup>	C/ O <sup>5</sup>	Actions needed to close recommendation	Implementation date <sup>6</sup>
1	UNMISS should establish procedures to verify the authenticity of authorized signatories on the request forms to issue United Nations identity cards and ensure that such forms bear the official stamp of requesting offices.	Important	O	Receipt of evidence that the binder containing specimen signatures has been developed, regularly updated and matched with the signatures on the request forms.	30 December 2023
2	UNMISS should issue instructions clarifying the roles of offices and sections to timely inform the Pass and ID Unit about the separation of staff and strengthen procedures for the Unit to promptly deactivate United Nations identity cards for separated staff.	Important	O	Receipt of evidence that suitable guidance has been issued and appropriate action is taken to timely deactivate identity cards for separated staff.	30 December 2023
3	UNMISS should: (a) optimize the synchronization of data between portable handheld electronic card readers and ONPASS application to ensure data integrity; (b) configure the portable handheld electronic card readers to erase data after they remain idle for the defined period to protect data if the devices are lost; and (c) take measures to record the entry and exit of personnel with low-cost United Nations identity cards that are not integrated with the system.	Important	O	Receipt of evidence that data is timely synchronized between the portable handheld electronic card readers and the ONPASS application, the devices are configured to erase data after they remained idle for a specified period, and the recording of the details of low-cost United Nations identity card holders are strengthened at the entry and exit points.	30 July 2023
4	UNMISS should: (a) improve the monitoring and reporting on the key performance indicators related to the performance of unarmed guards in all locations; and (b) strengthen the supervision of	Important	C		Implemented

<sup>3</sup> Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

<sup>4</sup> Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

<sup>5</sup> Please note the value C denotes closed recommendations whereas O refers to open recommendations.

<sup>6</sup> Date provided by UNMISS in response to recommendations.

## STATUS OF AUDIT RECOMMENDATIONS

## Audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical <sup>3</sup> / Important <sup>4</sup>	C/ O <sup>5</sup>	Actions needed to close recommendation	Implementation date <sup>6</sup>
	unarmed guards to effectively record and manage access to the Mission's premises.				

# **APPENDIX I**

## **Management Response**

**UNITED NATIONS**

United Nations Mission  
in South Sudan




**NATIONS UNIES**

Mission des Nations Unies  
en Soudan du Sud

Date: 29 March 2023

To: Mr. Kemal Karaseki  
Acting Chief, Peacekeeping Audit Service  
Internal Audit Division, OIOS

From: Guang Cong   
Officer-In-Charge  
United Nations Mission in the Republic of South  
Sudan

Subject: **Management Response to the draft report of the Audit of Issuance of ID Cards and Physical Access Controls in the United Nations Mission in the Republic of South Sudan (Assignment No. AP2022-633-05)**

1. UNMISS acknowledges receipt of the draft report from OIOS on the Audit of Issuance of ID Cards and Physical Access Controls dated 9 March 2023.
2. Please find attached the Management Response to the recommendations as indicated in Appendix I.
3. Thank you for your consideration and support.

cc: Ms. Victoria Browning, UNMISS  
Mr. Paul Egunsola, UNMISS  
Ms. Aminata Thiaw Kone, UNMISS  
Mr. Qazi Ullah, UNMISS  
Mr. Nikolay Kovalev, UNMISS  
Mr. Rabi Burathoki, UNMISS  
Ms. Ana Rodriguez, UNMISS  
Ms. Daniela Wuerz, UNMISS  
Mr. Jeffrey Lin, OIOS

Management Response

Audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical <sup>1</sup> / Important <sup>2</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNMISS should establish procedures to verify the authenticity of authorized signatories on the request forms to issue United Nations identity cards and ensure that such forms bear the official stamp of requesting offices.	Important	Yes	Chief, Pass & ID Unit	30 December 2023	The Pass & ID Unit is currently collecting scans of sample signatures and official stamps from UNSMS organizations and UNMISS focal points who are authorized to approve ID cards and extensions. A binder of all scans will be physically in place by 30 December 2023.
2	UNMISS should issue instructions clarifying the roles of offices and sections to timely inform the Pass and ID Unit about the separation of staff and strengthen procedures for the Unit to promptly deactivate United Nations identity cards for separated staff.	Important	Yes	Administrative Officer, Office of the DMS	30 December 2023	UNMISS will provide specific guidance on the process and accountability measures in relation to the deactivation of UNMISS-issued IDs upon separation of the authorized holders.
3	UNMISS should: (a) optimize the synchronization of data between portable handheld electronic card readers and ONPASS application to ensure data integrity; (b) configure the portable handheld electronic card readers to erase data after they remain idle for the defined period to protect data if the devices are lost; and (c) take measures to record the entry and exit of personnel with low-cost United Nations identity cards that are not integrated with the system.	Important	Yes	Chief, FTS  Chief, Integrated Security Solutions (ISS) Unit  Commander, Guard Force Unit (GFU)	30 July 2023	3(a) As an interim measure, the GFU Commander, after discussion with OIOS, has instructed all WS Insight guard supervisors to synchronize the handheld electronic card readers every hour.  3(b) FTS is discussing with UNDSS and Motorola to implement the OIOS recommendation as soon as possible. FSS is waiting for the cost and time estimates from Motorola for the system upgrade. The timeline will be provided once their inputs are received.  3(c) Currently, low-cost UN IDs are in operation only in Bentiu and Malakal. Any NGO requiring such ID cards must submit their request through OCHA or IOM which are the official agencies that can request ID cards. ISS and FTS are in the process of revisiting the current technology that supports low-

<sup>1</sup> Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

<sup>2</sup> Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

Management Response

Audit of the issuance of identity cards and physical access controls in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical <sup>1</sup> / Important <sup>2</sup>	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						cost ID cards and this will further strengthen the recording of low-cost ID cards at entry and exit points. It is estimated that implementation would occur by end of July 2023.
4	UNMISS should: (a) improve the monitoring and reporting on the key performance indicators related to the performance of unarmed guards in all locations; and (b) strengthen the supervision of unarmed guards to effectively record and manage access to the Mission’s premises.	Important	Yes	Area Security Advisers	Implemented	<p>Corrective actions have been taken according to the KPIs. In this regard, inputs are being provided to the Monthly Performance Management (MPM) exercise. Monthly Performance Management Meetings are held between GFU and the management of the private security company.</p> <p>An improved deployment monitoring system has been established. There is a system of three-layered reporting and supervision, which includes the Team Leader of the private security company, the International Security Officer of the private security company, and the GFU Duty Officer. This recommendation is considered implemented and the supporting documents have already been submitted to OIOS.</p>