Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2023/030

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

There is need to establish a governance framework to guide information technology operations, cybersecurity and data management

8 August 2023
Assignment No. AT2022-590-01

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, operations and security at the Office for the Coordination of Humanitarian Affairs (OCHA). The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes for ICT operations and ICT security, including preparedness, resilience mechanisms and controls across people, process and technology to prevent, detect and respond to cybersecurity risks and threats in OCHA. The audit covered the period from 1 January 2020 to 30 November 2022 and included a review of: (a) governance and risk management; (b) training and awareness; (c) ICT operations and performance management; (d) data governance and management; (e) information and cybersecurity; and (f) operational resilience and recovery.

The audit indicated the need for OCHA to establish a governance framework to guide information technology operations, cybersecurity and data management.

OIOS made 12 recommendations. To address the issues identified in the audit, OCHA needed to:

- Establish a governance mechanism to guide and oversee its ICT operations and initiatives across its strategic and operational priorities by establishing an ICT committee and defining a roadmap for enabling its transformation and operational priorities;
- Formalize its entity-level risk register and ICT risk treatment plans;
- Implement a training and awareness programme for its staff on the handling of sensitive humanitarian information as well as cybersecurity specific to its operations and environment; and strengthen mechanisms to ensure that contractors complete the mandatory training on information security awareness;
- Define the ICT service delivery model, clarify catalogs of services to be provided by the Information Management Branch, and clarify the role and responsibilities for coordination and management of ICT initiatives at OCHA branches and field offices;
- Ensure that all service requests are recorded in iNeed to enable visibility of ICT support; provide guidance to users on how to submit and classify their requests in iNeed; and establish procedures to measure the effectiveness of ICT support across its branches and field offices;
- Ensure that all ICT systems are compliant with OICT's technical procedures and OCHA's policy on technology standards; and strengthen procedures for ensuring timely approval of the Architecture Review Board;
- Assess the risk of access to sensitive information by third parties and establish mechanisms to assure that service providers comply with the Secretariat's ICT policies;
- Ensure that all field offices conduct gap assessments with reference to the data responsibility guidelines and implement a standard operating procedure for performing regular data responsibility assessments in all field offices;
- Develop a roadmap for implementing multi-dimensional business intelligence capabilities, and assign responsibilities and define data architecture and organizational data visualization requirements to facilitate effective business intelligence for informed decision-making;
- Strengthen de-provisioning procedures to ensure that all staff separations are processed electronically to enable timely de-provisioning of access to ICT systems;

- Implement a cybersecurity review and vulnerability management process, including prioritization of assets and locations to be assessed, schedules for assessments, and remediation tracking for vulnerabilities pertaining to all its offices including field offices; and
- Define and implement recovery arrangements for the Grants Management System in line with the OICT technical procedure on disaster recovery planning.

OCHA accepted the recommendations and has initiated action to implement them. Actions required to close the recommendations are indicated in Annex I.

CONTENTS

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, operations and security at the Office for the Coordination of Humanitarian Affairs.

2. OCHA operates under the United Nations Secretariat's ICT policy framework and works in close cooperation with the Office of Information and Communications Technology (OICT), including on cybersecurity[1] requirements which are embedded within the ICT policies. OCHA is responsible for operationalizing the policies at the local level and implementing additional measures to mitigate the risks.

3. OCHA's Information Management Branch (IMB) provides ICT, data, and information management support services to OCHA's functions in Headquarters (New York and Geneva), five regional offices, and 30 country offices. IMB was headed by a Chief at D-1 Level, with 51 staff and 85 contractors. IMB staff were spread amongst New York, Geneva, The Hague, Istanbul, Bangkok and Nairobi, while contractors were dispersed all over the world. OCHA also had 30 ICT officers (ICTOs) stationed in country offices. The budget of IMB for 2022 was $13.9 million.

4. ICT systems are critical to the delivery of OCHA's mandated functions. Humanitarian financing was supported by the Grants Management System (GMS) for Country Based Pooled Funds (CBPF) and the Central Emergency Response Fund (CERF), which managed funds averaging $1 billion and $800 million per year, respectively. GMS had over 6,000 users, including implementing partners for over 1,800 projects. Additional systems included the core web and data sharing platforms – Reliefweb, Humanitarian Data Exchange (HDX) and Humanitarian Response, the OCHA Contribution Tracking System (OCTS) and the Virtual On-Site Operations Coordination Centre (VOSOCC). OCHA's ICT systems comprised of applications and services managed by its various branches.

5. Comments provided by OCHA 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 for ICT operations and ICT security, including preparedness, resilience mechanisms and controls across people, process and technology to prevent, detect and respond to cybersecurity risks and threats in OCHA.

7. This audit was included in the 2022 risk-based work plan of OIOS due to the high risks associated with ICT systems supporting OCHA's operations. Cybersecurity remains a high risk and a high priority for the Secretariat due to emerging threats in the cybersecurity landscape and persistent cyber-attacks.

[1] The Chief Executives' Board for Coordination has defined cybersecurity as the collection of tools, policies, laws, regulations best practices and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment.

8. OIOS conducted this audit from September to December 2022. The audit covered the period from 1 January 2020 to 30 November 2022. Based on an activity-level risk assessment, the audit covered risk areas relating to: (a) governance and risk management; (b) training and awareness; (c) ICT operations and performance management; (d) data governance and management; (e) information and cybersecurity; and (f) operational resilience and recovery.

9. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data and survey responses; (e) review of critical business applications; and (f) physical observation.

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

III. AUDIT RESULTS

A. Governance and risk management

Need to strengthen ICT governance mechanisms

11. ICT governance mechanisms should provide the framework for establishing an entity's priorities for ICT investments and management of ICT resources. The framework should define the respective roles and responsibilities across the organization and establish procedures for managing risks and ensuring that resources are used appropriately.

12. OCHA's strategic plan 2023-2026 identified 'Data, Analysis and Technology' as an enabler for OCHA's transformational priorities. However, OCHA was yet to define adequate ICT governance mechanisms to holistically enable the transformational priorities. As a result, there was no collective understanding of the desired future state of OCHA's ICT architecture for systems/applications, data and infrastructure to facilitate prioritization of ICT initiatives. For instance, ST/AI/2005/10 on ICT initiatives requires establishing an ICT committee to ensure that ICT initiatives are supported by a high-level business case, are updated in the ICT assets inventory, and comply with ICT standards while avoiding duplication of initiatives. OCHA did not have an ICT committee to provide the required oversight of its ICT initiatives and activities. For example, there was no visibility over ICT costs across OCHA because information for expenditures related to ICT projects and systems was not consolidated across branches and field offices. OIOS also noted the following:

(a) In 2022, OCHA undertook seven projects on systems such as ICT field networks, HDX, GMS, and Humanitarian Programme Cycle tools. These projects were implemented in silos by the respective branches, without the required oversight to ensure that the projects were required and were not duplicated.

(b) There was no defined mechanism to consider and allocate funds to important ICT projects. For example, applications such as OCTS delayed implementing security functionalities due to lack of funding, which exposed it to the risk of systems failure.

13. The lack of ICT governance mechanisms may expose OCHA to the risks of lack of accountability and direction, the inability to meet ICT needs for effective and timely mandate execution, and ICT resources not being used effectively.

(1)	**OCHA should establish a governance mechanism to guide and oversee its ICT operations and initiatives across its strategic and operational priorities by: (a) establishing an ICT**

committee; and (b) defining a roadmap for enabling its transformation and operational priorities.

OCHA accepted recommendation 1 and stated that IMB created a draft terms of reference (TOR). Also, OCHA would identify a core group of participants, agree on the TOR and establish the priorities. Further, OCHA stated that many of its critical applications have distributed ownership across different sections and creating a roadmap collectively would be critical to its success.

Need to establish mechanisms for ICT risk management across OCHA

14. Best practice requires visibility, awareness and management of significant risks to an entity. OCHA's organizational strategic plan 2023-2026 acknowledges that the humanitarian needs and response context will have higher levels of misinformation, distrust and increased cyber-attacks; technology will present new risks, dangers and opportunities for vulnerable populations; and the international humanitarian system would need to embrace new and emerging technology while guarding against risks.

15. Although OCHA's strategic plan identified digitization and ICT risks at a high level, OCHA had not undertaken an ICT risk assessment across all its branches and did not have an entity-level risk register which would highlight the criticality of ICT to OCHA and facilitate the management of ICT risks across its organization. Risk areas that OCHA branches need to consider include exposure of personal information, email and application security, data theft, among others, in the context of day-to-day operations. Risks of emerging technologies used by partners e.g., artificial intelligence and unmanned aerial vehicles, also need to be assessed.

(2) OCHA should formalize its entity-level risk register and ICT risk treatment plans.

OCHA accepted recommendation 2 and stated that Senior Leadership Group has individually endorsed the risks included in the Corporate Risk Register and has committed to complete its treatment plans by December 2023. IMB will support the Sustainability, Resilience and Risk Management Section in the implementation of this recommendation.

B. Training and awareness

Need to implement a training and awareness programme

16. To mitigate risks associated with people and behaviour, a workforce should be digital security-conscious and properly skilled. An organization should provide appropriate awareness, education and training, and regular updates on organizational policies and procedures, including to non-staff personnel to reduce risks to the entity.

17. During the audit period, OCHA's training and awareness activities comprised of: hands-on ICT operations and emergency-response training for field ICTOs; data responsibility training for information management officers in 19 countries; cybersecurity awareness campaign comprising webinars on pertinent topics (e.g., social engineering and remote working); and cybersecurity awareness information shared on the OCHA Hub and ICTOs' online collaboration platforms. OIOS noted the following:

(a) No training needs assessment was conducted for handling of sensitive information. There was no entity-level cybersecurity awareness programme specifying the target groups, type and frequency of awareness activities, resourcing and implementation schedules. Therefore, there was no training for staff on handling of sensitive information, and no tailored training for staff groups with a higher threat profile

(e.g., senior management, field staff operating in sensitive locations), business application administrators, software developers, and contractors who may be targeted because of their privileged access to OCHA's sensitive information.

(b) OCHA did not leverage the Secretariat campaigns (such as OICT's October cybersecurity month) by reminding its staff to participate in cybersecurity awareness activities.

(c) The completion rate for the mandatory course on information security awareness by staff was 93 per cent. However, completion of the course by contractors was poor – only 18 out of 85 (21 per cent) IMB contractors had completed the course.

(3) OCHA should: (a) implement a training and awareness programme for its staff on the handling of sensitive humanitarian information as well as cybersecurity, specific to its operations and environment; and (b) strengthen mechanisms to ensure that contractors complete the mandatory training on information security awareness.

OCHA accepted recommendation 3 and stated that this work will be a joint effort between IMB and the Learning Development Unit, who will collaborate to assess needs and design the training programme for delivery in 2024. It will target all staff as well as those functions working with data. The Human Resources Section will also support the implementation of this recommendation.

C. ICT operations and performance management

Need to improve the ICT service delivery approach

18. OCHA's ICT services are required by staff and business functions in geographically dispersed field offices, sub-offices, humanitarian disaster response locations, and Headquarters. The ICT service delivery approach should provide quality services in an efficient and effective manner, while complying with applicable policies, procedures, standards, and architecture. Best practices recommend defining an ICT service delivery model and describing the ICT services catalog, roles and responsibilities, service request processes, service level expectations, and performance monitoring mechanisms.

19. OCHA's geographically dispersed structure requires that its business model be enabled by an effective ICT service delivery model. OCHA had not defined a service delivery model on how ICT will support business processes, and how it will be implemented. This led to siloes in ICT service delivery, funding misalignments, and duplication of effort.

20. OCHA's ICT service delivery comprised of: catalogs of OICT-provided services; roles and responsibilities documented in IMB's TOR; and designated support teams at Headquarters and field offices. OIOS noted the following:

(a) IMB's TOR did not provide clarity on roles and responsibilities vis-a-vis OCHA branches and its ICT units at field locations. Further, the coordination mechanism between IMB and OCHA branches and ICT units in the field also required clarification. While field offices at times coordinated their country ICT projects with IMB, OCHA Headquarters branches did not. There were no criteria specifying the matters that IMB should be consulted on. For example, the Coordination Division adopted a software technology that was nearing obsolescence, while there was expertise within IMB that could have advised against it.

(b) OCHA did not have a catalog of the applications hosting, website hosting, and cybersecurity scanning services that IMB provided to other branches and country offices. These services were in place,

but OCHA did not document the service descriptions, hours of operation, customer responsibilities, service level expectations, procedures, and performance indicators. This led to unclear responsibilities and an inability to measure service performance.

(4) OCHA should strengthen ICT service delivery by: (a) defining its service delivery model; (b) clarifying catalogs of services to be provided by the Information Management Branch; and (c) clarifying the role and responsibilities of the Information Management Branch regarding coordination and management of ICT initiatives at OCHA branches and field offices.

OCHA accepted recommendation 4 and stated that this work will be accomplished through the recently formed ICT Governance Board as a forum to bring all sections of OCHA together and agree on standards for applications and services.

Need to measure the effectiveness of ICT support

21. OICT implemented the Unite self-service management system (iNeed) to enable staff to submit and track their ICT requests. The system comprises various modules including: (a) Service Requests module for browsing service catalogs, raising requests, and tracking the status of the request, while categorizing the request as a service request or an incident[2]; and (b) Work Orders module to assign tasks to technicians. Service requests were resolved by field ICTOs, the OCHA Product Support Team or the OICT Unite Service Desk. The system also gives ICT personnel the ability to measure and improve services.

22. OCHA did not use the iNeed system consistently to record service requests. For instance, field ICTOs received email, phone, or verbal requests and only recorded them on iNeed on behalf of the user when escalating the requests to Headquarters for advanced support. Consequently, there was no visibility over field-level service requests which were resolved without escalation. As such, the adequacy of support at the field level, where the majority of OCHA staff are located, was not measured. Consequently, there was no visibility as to: (i) whether the support services were adequate; and (ii) of common trends or patterns that may indicate systemic problems.

23. In the years 2020, 2021 and 2022, the OCHA Product Support Team processed 1817, 1261 and 2421 service requests and 151, 164 and 149 work orders, respectively. OCHA prepared monthly reports of these service requests and work orders, comprising the number of requests in a month, categorized in sub-areas (e.g., account management, network, applications support, printing, virtual meetings, and software). OIOS noted the following:

(a) Service requests (e.g., general queries, requests for laptops, requests for virtual meetings, and training) were frequently misclassified as incidents. The monthly average percentage of incidents versus service requests was 28 per cent in 2022. However, October and November 2022 had 54 per cent categorized as incidents. Although these months had similar volumes as other months, the incident numbers were nearly double due to incorrect classification, leading to suboptimal prioritization of responses.

(b) Monthly reports did not capture the service request locations, time taken to close the requests, and user satisfaction feedback. Although OIOS' analysis showed that requests were closed within the same month, it was not possible to determine the actual time taken (in days) to assess the timeliness of support. This was because OCHA did not define specific criteria for measuring the effectiveness of ICT support.

[2] While service requests are for pre-defined ICT services, incidents are unplanned interruptions to a service or reduction in the quality of services.

24. OCHA submitted 4,042 requests to Unite Service Desk from January to November 2022. Although 99 per cent of the requests were closed, it was not possible to measure timeliness. Moreover, 22 requests had been pending for over a month without clarification as to why they were still open.

(5) OCHA should: (a) ensure that all service requests are recorded in iNeed to enable visibility of ICT support; (b) provide guidance to users on how to submit and classify their requests in iNeed; and (c) establish procedures to measure the effectiveness of ICT support across its branches and field offices.

OCHA accepted recommendation 5 and stated that iNeed is used by its product support team and ICT officers to submit tickets but is not user friendly and intuitive. Staff primarily communicate through Microsoft Teams chat and would like to continue its use for service requests as it facilitates a faster response. OCHA further stated that there are a lot of support services that OCHA requires, and these services are not reflected in iNeed, so a full range of Request for Service or Incident Management are not captured. Also, the iNeed service level agreements are inadequate in a humanitarian response organization due to delayed response time. OIOS is of the view that OCHA needs to engage with OICT to address these limitations.

Need to strengthen software management procedures

25. OICT technical procedures on system installation, configuration, monitoring and maintenance require the implementation of mechanisms to ensure normal and secure operation of ICT systems.

26. OCHA had implemented mechanisms for managing and monitoring its applications and websites hosted in the Amazon Web Services (AWS) cloud platform. System administrators received automated alerts on anomalies. However, alerts for sensitive changes in AWS identity and access management policies were not activated. This was brought to OCHA's attention during the audit and was promptly addressed.

27. Further, OCHA's policy instruction on technology standards requires its personnel to use OICT-approved software and outlines the process to obtain approval from the OICT Architecture Review Board (ARB) to use technologies not previously approved. OCHA had established a process for identifying instances of unauthorized software in use and engaging the concerned focal points to seek ARB approval. However, in some instances ARB approval had not been obtained, or the durations approved by ARB had expired (see Table 1 below). OCHA needed to strengthen its procedures for ensuring ARB approval and use of authorized software.

Table 1: Examples of unauthorized software in use at OCHA

Software and focal points	Notes
Airtable (Inter Agency Standing Committee), Trello (Pooled Funds Management Branch (PFMB)	Not approved by ARB. PFMB commenced migration from Trello to an approved software
Pigeonhole (External Relations and Partnerships), Fleeq.io (Financing)	Not approved by ARB
Contentful, Beagle vulnerability scanner, Google account HID and Siteguru, (IMB); QR.io and Webflow (Donor Relations)	Duration approved by ARB had expired
Various remote access, virtual private network, and anonymous browsing tools (field offices)	These were flagged in network and security monitoring reports but were not investigated

Software and focal points	Notes
OCHA register of sensitive data disclosure incidents on Google drive (IMB)	This was discontinued during the audit

(6) OCHA should: (a) ensure that all ICT systems are compliant with OICT's technical procedures and OCHA's policy on technology standards; and (b) strengthen its procedures for ensuring timely approval of the Architecture Review Board, and for ensuring the use of authorized software.

OCHA accepted recommendation 6 and stated that this work will be accomplished through the recently formed ICT Governance Board as a forum to bring all sections of OCHA together and agree on standards for applications and services.

Need to strengthen mechanisms to manage operations associated with third-party service providers

28. Organizations need to assess and manage interdependency and risks with third-party service providers, including vendors and partners. Measures should be taken to monitor the adequacy of their performance, based on defined criteria, and implement corrective action where the services are inadequate.

29. OCHA relied on other United Nations entities and external vendors for ICT services and cybersecurity-related activities. The provision of these services was governed by contracts and memoranda of understanding. OCHA took some measures to manage third-party risks. For instance, it monitored the performance of the United Nations Global Services Centre (UNGSC) and took corrective action as required, and initiated the Field Secured Gateway (FSG) project after determining that UNGSC-provided network devices and services were not cost-effective and flexible to meet OCHA's field needs. However, in other cases, OCHA needed to strengthen its management of third-party risks as follows:

(a) OCHA did not conduct a review to determine whether service providers that had access to sensitive information were protecting it in accordance with ICT policies. The parties providing field network monitoring and security had access to sensitive information, intellectual property and software code. OCHA did not include data handling and cybersecurity provisions in the contracts and memorandum of understanding, which may expose it to ICT risks emanating from weaknesses in its service providers' environment.

(b) OCHA had no mechanism to obtain assurance from the United Nations entities providing ICT services that they adhered to the Secretariat's ICT policies because the requirements were not defined in the contract or memorandum of understanding. For example, OCHA did not require the entities providing cloud hosting services to assure that they had secured the cloud infrastructure to mitigate against cybersecurity-related threats, including availability of OCHA resources in the cloud environment.

(7) OCHA should: (a) assess the risk of access to sensitive information by third parties; and (b) establish mechanisms to assure that service providers comply with the Secretariat's ICT policies.

OCHA accepted recommendation 7 and stated that IMB will chair an ICT Governance Group in which different sections of OCHA that manage critical business applications will participate and some baseline standards on development, support and maintenance will be developed jointly, in accordance with the Secretariat's policies.

D. Data governance and management

Need to ensure compliance with data responsibility procedures across OCHA field offices

30. In October 2021, OCHA published data responsibility guidelines[3] in line with the Secretary General's Data Strategy and related policies. Although field offices had pre-existing data responsibility practices, all offices were to conduct a gap assessment and prioritize actions to adopt the guidelines fully. Nineteen out of 30 offices commenced adopting the guidelines. While some offices proactively adopted them, others were reacting to external pressure, e.g., to share sensitive information with donors and member states. The remaining 11 offices had not adopted the guidelines due to inadequate follow up by management. The use of the name 'guideline' implied that it was optional, thereby contributing to delayed adoption, which could impact OCHA's ability to manage data responsibly and securely.

(8) OCHA should: (a) ensure that all its field offices conduct gap assessments with reference to its data responsibility guidelines; and (b) implement a standard operating procedure for performing regular data responsibility assessments in all its field offices.

OCHA accepted recommendation 8 and stated that IMB is tracking the adoption of the data responsibility guidelines across OCHA country and regional offices. Also, the practical implementation of these guidelines needs to be reinforced by the Operations and Advocacy Division within their field offices. OCHA stated that its offices will conduct an annual data responsibility diagnostic ("gap assessment" / "assessment") with support from the Centre for Humanitarian Data, and this work will be tracked and reported on within the key performance indicators for OCHA's 2023-2026 strategic plan.

Need to strengthen data analytics capabilities to support decision making

31. The Secretary-General's Data Strategy prioritizes improving decision-making through self-service analytics, business intelligence and visualizations, and improving tool sets and policies for managing master data, data inventory and data integration in Secretariat entities, while complying with information sensitivity, classification and handling policies. Further, OCHA's 2023-2026 strategy indicates the need to leverage data and data analytics across its functions to enable the delivery of its transformational priorities.

32. OCHA established a Global Information Management Functional Team (GIFT) to bring together expertise for functional excellence in information management, including management of corporate and humanitarian community data. Also, in line with the Data Strategy, OCHA established anticipatory action frameworks for drought and disease outbreak use cases enabled by predictive analytics, enhanced data sharing on HDX, and data visualizations for the humanitarian community.

33. However, OCHA lacked a defined data architecture and requirements for data visualization. As a result, senior leaders' decision-making was delayed in some emergency situations. Data architecture that clearly identifies data sources across OCHA, defines data use cases, and articulates how the data will be transformed and distributed to support decision-making, are essential to realize full value from the data. OIOS noted the following:

(a) There was no roadmap to implement the data strategy, including data governance, master data management, data inventory, and data integration.

[3] These guidelines define data responsibility in humanitarian action as the safe, ethical and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection.

(b) OCHA lacked oversight and standards for development of visualization platforms. As a result, reporting functionalities and dashboards were implemented in silos by the respective branches. For example, CBPF GMS, CERF GMS, OCTS and FTS applications obtained contributions data from Umoja and other sources and presented it in dashboards for specific branch requirements that did not provide an entity-level view to inform senior leadership's decision-making. Over time, this approach may cause proliferation of dashboards that overlap in functionality, duplicate efforts and impede self-service capabilities.

(9) OCHA should: (a) develop a roadmap for implementing multi-dimensional business intelligence capabilities; and (b) assign responsibilities and define data architecture and organizational data visualization requirements to facilitate effective business intelligence for informed decision-making.

OCHA accepted recommendation 9 and stated that this work will be accomplished through the recently formed ICT Governance Board as a forum to bring all sections of OCHA together and agree on standards for applications and services.

E. Information and cybersecurity

Need to strengthen de-provisioning procedures for OCHA systems

34. The OICT technical procedure on access control requires that access to ICT systems be granted to authorized users only. Regular reviews should be undertaken to determine whether user access rights are commensurate to their job duties, and there should also be timely communication for removing access rights when users no longer require access to ICT systems.

35. OCHA took appropriate measures for timely de-provisioning of users of its systems. For example, VOSOCC privilege user rights were reviewed regularly, and the Sudan Humanitarian Fund timely de-provisioned CBPF GMS access for staff who checked out of the country office. Also, regular security assessments were conducted on the Humanitarian ID authentication service that enabled users to access a range of humanitarian websites. However, 6 out of 70 staff who separated from OCHA between January and November 2022 were not de-provisioned from the Active Directory by December 2022, due to offline separations. OCHA needs to address this issue.

(10) OCHA should strengthen its de-provisioning procedures to ensure that all staff separations are processed electronically to enable timely de-provisioning of access to its ICT systems.

OCHA accepted recommendation 10 and stated that the Human Resources Section will continue to process staff separations using iNeed Separations tool, which automatically notifies and assigns the service request/work order to the clearing office to take further action including de-provisioning of access to ICT systems. OCHA will continue to use the Global Separation Checklist to ensure that all necessary actions are taken before finalizing separation. IMB will support the Human Resources Section in the implementation of this recommendation.

Need to strengthen the vulnerability management process

36. It is best practice to establish procedures for regular vulnerability assessments of the ICT landscape to optimize threat detection and response, and mitigation of identified vulnerabilities.

37. [redacted]

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

(11) OCHA should implement a cybersecurity review and vulnerability management process, including prioritization of assets and locations to be assessed, schedules for assessments, and remediation tracking for vulnerabilities pertaining to all its offices including field offices.

OCHA accepted recommendation 11 and stated that implementation of a cybersecurity review and vulnerability management process is underway.

F. Operational resilience and recovery

Need to establish ICT operational resilience and recovery plans

38. OICT's technical procedure on disaster recovery planning requires all disaster recovery solutions for critical ICT services and applications to have a target recovery time objective of 24 hours and a target recovery point objective of four hours if possible.

39. [redacted]

(a) [redacted]

(b) [redacted]

(12) OCHA should define and implement recovery arrangements for the Grants Management System in line with the OICT technical procedure on disaster recovery planning.

OCHA accepted recommendation 12 and stated that the Information Management System Data Analytics Unit (IMSDAU) in the Guidance Learning and Reporting Section of the Humanitarian Financing and Resource Mobilization Division is implementing a disaster recovery model by developing a high availability environment. [redacted]

IV. ACKNOWLEDGEMENT

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

Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[4]/ Important[5]	C/ O[6]	Actions needed to close recommendation	Implementation date[7]
1	OCHA should establish a governance mechanism to guide and oversee its ICT operations and initiatives across its strategic and operational priorities by: (a) establishing an ICT committee; and (b) defining a roadmap for enabling its transformation and operational priorities.	Important	O	Receipt of evidence of the ICT steering committee guiding and overseeing ICT operations and initiatives across OCHA's strategic and operational priorities, and a roadmap for enabling the transformation and operational priorities.	31 December 2024
2	OCHA should formalize its entity-level risk register and ICT risk treatment plans.	Important	O	Receipt of the formalized entity-level risk register and ICT risk treatment plans.	31 December 2023
3	OCHA should: (a) implement a training and awareness programme for its staff on the handling of sensitive humanitarian information as well as cybersecurity specific to its operations and environment; and (b) strengthen mechanisms to ensure that contractors complete the mandatory training on information security awareness.	Important	O	Receipt of evidence that OCHA has implemented a training and awareness programme for its staff on handling of sensitive humanitarian information as well as cybersecurity, specific to its operations and environment, and strengthened mechanisms to ensure that contractors complete the mandatory training on information security awareness.	31 December 2024
4	OCHA should strengthen ICT service delivery by: (a) defining its service delivery model; (b) clarifying catalogs of services to be provided by the Information Management Branch; and (c) clarifying the role and responsibilities of the Information Management Branch regarding coordination and management of ICT initiatives at OCHA branches and field offices.	Important	O	Receipt of the defined ICT service delivery model, catalogs of services to be provided by the Information Management Branch; and clear roles and responsibilities of the Information Management Branch regarding coordination and management of ICT initiatives.	31 December 2024
5	OCHA should: (a) ensure that all service requests are recorded in iNeed to enable visibility of ICT support; (b) provide guidance to users on how to submit and classify their requests in iNeed; and (c) establish procedures to measure the effectiveness of ICT support across its branches and field offices.	Important	O	Receipt of evidence that all service requests are recorded in iNeed, users have been provided guidance on how to submit and classify their requests in iNeed; and procedures to measure the effectiveness of ICT support across the branches and field offices have been established.	31 December 2024
6	OCHA should: (a) ensure that all ICT systems are compliant with OICT's technical procedures and OCHA's policy on technology standards; and (b)	Important	O	Receipt of evidence that all ICT systems are compliant with OICT's technical procedures and OCHA's policy on technology standards, and	31 December 2024

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

	strengthen its procedures for ensuring timely approval of the Architecture Review Board, and for ensuring the use of authorized software.			procedures for ensuring timely approval of the Architecture Review Board, and use of authorized software have been strengthened.	
7	OCHA should: (a) assess the risk of access to sensitive information by third parties; and (b) establish mechanisms to assure that service providers comply with the Secretariat's ICT policies.	Important	O	Receipt of evidence that the risk of access to sensitive information by third parties is being assessed and a mechanism to assure that service providers comply with the Secretariat's ICT policies has been established.	31 December 2024
8	OCHA should: (a) ensure that all its field offices conduct gap assessments with reference to its data responsibility guidelines; and (b) implement a standard operating procedure for performing regular data responsibility assessments in all its field offices.	Important	O	Receipt of evidence of data responsibility gap assessments have been conducted in all field offices, and a standard operating procedure for regular data responsibility assessments in all field offices has been implemented.	31 December 2024
9	OCHA should: (a) develop a roadmap for implementing multi-dimensional business intelligence capabilities; and (b) assign responsibilities and define data architecture and organizational data visualization requirements to facilitate effective business intelligence for informed decision-making.	Important	O	Receipt of the roadmap for implementing multi-dimensional business intelligence capabilities, assigned responsibilities, defined data architecture and organizational data visualization requirements.	31 December 2024
10	OCHA should strengthen its de-provisioning procedures to ensure that all staff separations are processed electronically to enable timely de-provisioning of access to its ICT systems.	Important	O	Receipt of evidence that that all staff separations are processed electronically to enable timely de-provisioning of access to its ICT systems.	31 December 2023
11	OCHA should implement a cybersecurity review and vulnerability management process, including prioritization of assets and locations to be assessed, schedules for assessments, and remediation tracking	Important	O	Receipt of evidence of a cybersecurity review and vulnerability management process, including prioritization of assets and locations to be assessed, schedules for assessments, and	31 December 2024

[4] 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.
[5] 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.
[6] Please note the value C denotes closed recommendations whereas O refers to open recommendations.
[7] Date provided by OCHA in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

	for vulnerabilities pertaining to all its offices including field offices.			remediation tracking for vulnerabilities pertaining to all its offices including field offices.	
12	OCHA should define and implement recovery arrangements for the Grants Management System in line with the OICT technical procedure on disaster recovery planning.	Important	O	Receipt of evidence of recovery arrangements implemented for the Grants Management System in line with the OICT technical procedure on disaster recovery planning.	31 December 2023

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OCHA should establish a governance mechanism to guide and oversee its ICT operations and initiatives across its strategic and operational priorities by: (a) establishing an ICT committee; and (b) defining a roadmap for enabling its transformation and operational priorities.	Important	Y	Chief, Information Management Branch (IMB)	31 December 2024	OCHA's Information Management Branch (IMB) created a draft TOR which has been endorsed by OCHA's ASG, Joyce Msuya. Next steps include identifying a core group of participants, agreeing on the TORs and then establishing the priorities. Many of OCHA's critical applications have distributed ownership across different sections. Creating a roadmap collectively is critical to its success.
2	OCHA should formalize its entity-level risk register and ICT risk treatment plans.	Important	Y	Head of Sustainability, Resilience and Risk Management (SRRM), Executive Office (EO)	31 December 2023	OCHA's Senior Leadership Group has individually endorsed the risks included in the Corporate Risk Register and has committed to complete its treatment plans by December 2023. IMB will support SRRM in the implementation of this recommendation.
3	OCHA should: (a) implement a training and awareness programme for its staff on the handling of sensitive humanitarian information as well as cybersecurity specific to its operations and environment; and (b) strengthen mechanisms to ensure	Important	Y	Chief, Information Services Section, IMB and Head, Learning & Development	31 December 2024	This work will be a joint effort between IMB and the Learning Development Unit (LDU.) LDU will collaborate with IMB to assess needs and design the training programme for delivery in 2024. It will target all staff as well as those functions

[1] 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.

[2] 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.

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	that contractors complete the mandatory training on information security awareness.			Unit (LDU), EO		working with data. The Human Resources Section (HRS) will also support the implementation of this recommendation.
4	OCHA should strengthen ICT service delivery by: (a) defining its service delivery model; (b) clarifying catalogs of services to be provided by the Information Management Branch; and (c) clarifying the role and responsibilities of the Information Management Branch regarding coordination and management of ICT initiatives at OCHA branches and field offices.	Important	Y	Chief, IMB	31 December 2024	This work will be accomplished through the recently formed ICT Governance Board as a forum to bring all sections of OCHA together and agree on standards for applications and services.
5	OCHA should: (a) ensure that all service requests are recorded in iNeed to enable visibility of ICT support; (b) provide guidance to users on how to submit and classify their requests in iNeed; and (c) establish procedures to measure the effectiveness of ICT support across its branches and field offices.	Important	Y	Chief, Information Services Section (ISS), IMB	31 December 2024	OCHA's product support team and ICTOs use INeed to submit tickets. There has been a lot of outreach to colleagues to use INeed which hasn't worked. INeed is not user friendly and intuitive. Another issue is the only way to interact is through an email. OCHA staff have adopted MS Teams and primarily communicate via chat. They would like to continue this behavior for service requests as it facilitates a faster response. A general practice is OCHA staff contact their ICTO's in field offices as first line of support and product support as secondary support. In HQ locations colleagues contact product

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						support. Additionally, there are a lot of support services which OCHA requires, and these services (LOVs) are not reflected in INeed so a full range of Request for Service (RFS) or Incident Management (IM) are not captured. The tool is inadequate with challenging service level agreements in a humanitarian response organization. The SLA's outline the number of days a request may take but often times our field colleagues need resolution quickly and can't wait for multiple days.
6	OCHA should: (a) ensure that all ICT systems are compliant with OICT's technical procedures and OCHA's policy on technology standards; and (b) strengthen its procedures for ensuring timely approval of the Architecture Review Board, and for ensuring the use of authorized software.	Important	Y	Chief, ISS, IMB	31 December 2024	This work will be accomplished through the recently formed ICT Governance Board as a forum to bring all sections of OCHA together and agree on standards for applications and services.
7	OCHA should: (a) assess the risk of access to sensitive information by third parties; and (b) establish mechanisms to assure that service providers comply with the Secretariat's ICT policies.	Important	Y	Chief, ISS, IMB and Chief, Digital Services Section (DSS), IMB	31 December 2024	IMB will chair an ICT Governance Group in which different sections of OCHA who manage critical business applications will participate and some baseline standards on development, support and maintenance will be developed jointly in accordance with the Secretariat.
8	OCHA should: (a) ensure that all its field offices conduct gap assessments with	Important	Y	Chief, Centre for	31 December 2024	IMB is tracking the adoption of the data responsibility guidelines across OCHA

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	reference to its data responsibility guidelines; and (b) implement a standard operating procedure for performing regular data responsibility assessments in all its field offices.			Humanitarian Data, IMB		country and regional offices. The practical implementation of these guidelines needs to be reinforced by the Operations and Advocacy Division (OAD) within the field offices. Moving forward, OCHA offices will conduct an annual data responsibility diagnostic ("gap assessment" / "assessment") with support from the Centre for Humanitarian Data (CHD.) These diagnostics will help identify gaps and related priority actions for data responsibility. The CHD will continue to support adoption of data responsibility through advice, missions, training, templates and tools. This work will be tracked and reported on within the KPIs for OCHA's 2023-2026 Strategic Plan.
9	OCHA should: (a) develop a roadmap for implementing multi-dimensional business intelligence capabilities; and (b) assign responsibilities and define data architecture and organizational data visualization requirements to facilitate effective business intelligence for informed decision-making.	Important	Y	Chief, ISS, IMB	31 December 2024	This work will be accomplished through the recently formed ICT Governance Board as a forum to bring all sections of OCHA together and agree on standards for applications and services.
10	OCHA should strengthen its de-provisioning procedures to ensure that all staff separations are processed electronically to enable timely de-provisioning of access to its ICT systems.	Important	Y	Chief of Human Resources Section (HRS), EO	31 December 2023	HRS will continue to process staff separations through the online iNeed Separations tool for all staff clearances/separation process and ensure that the service requests for separation cases are submitted through the online iNeed Separations

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						tool. The online iNeed Separations tool automatically notifies and assigns the service request/work order to the clearing office to take further action including de-provisioning of access to its ICT systems. Follow up action will be undertaken for pending cases, as required. In addition, HRS will continue the use of the Global Separation Checklist, which serves as a guide for the HR Partners to ensure that all necessary separation actions are taken before finalizing separation and processing separation PA in Umoja. IMB will support HRS in the implementation of this recommendation.
11	OCHA should implement a cybersecurity review and vulnerability management process, including prioritization of assets and locations to be assessed, schedules for assessments, and remediation tracking for vulnerabilities pertaining to all its offices including field offices.	Important	Y	Chief, ISS, IMB	31 December 2024	This work is underway.
12	OCHA should define and implement recovery arrangements for the Grants Management System in line with the OICT technical procedure on disaster recovery planning.	Important	Y	Head of Information Management System Data Analytics Unit (IMSDAU),	31 December 2023	IMSDAU (Information Management System Data Analytics Unit) in GLRS (Guidance Learning and Reporting Section) has already begun implementing a disaster recovery model by developing a HIGH

APPENDIX I

Management Response

Audit of information and communications technology governance, operations and security at the Office for the Coordination of Humanitarian Affairs

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
				Guidance, Learning and Reporting Section (GLRS), Pooled Fund Management Branch (PFMB), Humanitarian Financing and Resource Mobilization Division (HFRMD)		AVAILABILITY environment. [redacted]