UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

AUDIT

OF

UNDP'S COMPLIANCE WITH ISO 27001

Report No. 2645

Issue Date: 19 January 2024

(REDACTED)

Table of Contents

Report on the Audit of UNDP's compliance with ISO 27001
Executive Summary

The UNDP Office of Audit and Investigations (OAI) conducted an audit of UNDP's compliance with ISO 27001 from 6 to 10 November 2023. The audit aimed to assess compliance of the UNDP established Information Security Management System (ISMS)[1] against ISO 27001:2022[2] standard (the standard) and the adequacy and effectiveness of the controls relating to the following sub-areas of the standard:

(a) Organizational controls
(b) Technological controls
(c) Physical controls
(d) People controls

The audit covered the activities regarding the standard as of 6 November 2023. The last audit of the standard was conducted in 2022 by the United Nations International Computing Center (UNICC), engaged by the Bureau for Management Services/Information and Technology Management (ITM) team.

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* of The Institute of Internal Auditors (The IIA).

ISO audit findings

The International Organization for Standardization (ISO) stipulates that findings from audits be graded/rated into four different categories: (1) major non-conformance, (2) minor non-conformance, (3) observations, and (4) opportunities for improvement (see definitions and equivalence to OAI's audit ratings and priorities in 'Definitions of audit terms - ratings and priorities'). Any non-conformance requires an audited entity to devise an action plan to address the non-conformity against requirements, while observations and opportunities for improvement are suggestions and do not require action plans.

Overall audit rating

OAI issued an audit rating for the compliance of ISO 27001 of **fully satisfactory**, which means "The assessed governance arrangements, risk management practices and controls were adequately established and functioning well. Issues identified by the audit, if any, are unlikely to affect the achievement of the objectives of the audited entity/area." This rating was mainly due to the fact that no major non-conformities (high/critical priority findings) were noted during the audit.

Key recommendations: Total = **2**, rated as minor non-conformity (medium/important)

The audit did not result in any major non-conformity (high/critical) recommendations. There are two minor non-conformity medium/important) recommendations.

The two minor non-conformity (medium/important) recommendations aim to ensure compliance with legislative mandates, regulations and rules, policies, and procedures.

[1] An information security management system (ISMS) is a framework of policies and procedures for systematically managing an organization's sensitive data.
[2] The International Organization for Standardization (ISO) is an independent, non-governmental international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market relevant international standards that support innovation and provide solutions to global challenges. Among the standards that it has issued is ISO 27001, which applies to Information Security. ISO 27001:2022 is the most updated version of the standard.

There were five observations and four opportunities for improvement (both low priority) findings that have been raised as well (refer to Annex 1 for details).

Management comments and action plan

The Director, ITM, of the Bureau for Management Services accepted the two recommendations and is in the process of implementing them. Comments and/or additional information provided have been incorporated in the report, where appropriate.

Observations and opportunities-for-improvement (low risk) issues (Annex 1) have been discussed directly with management and actions have been initiated to address them where possible.

Guillermo Munoz
Deputy Director (Audit) a.i.
Office of Audit and Investigations

I. About ISO 27001

The International Organization for Standardization (ISO) is an independent, non-governmental international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market relevant international standards that support innovation and provide solutions to global challenges. Among the standards that it has issued is ISO 27001 ,which applies to information security. The UNDP Information and Technology Management (ITM) team achieved ISO 27001 Information Security Management System certification in 2012.

ISO 27001 defines benchmarks through a set of controls that should be implemented for the management and security of assets, such as financial information, intellectual property, employee details or information entrusted by third parties. This set of controls includes policies, processes, procedures, organizational structures, rules and supporting tools used for information security. The standard does not require implementation of all controls specified; each organization selects controls that it deems to be necessary for mitigating information security risks applicable to its environment. As part of the certification requirements, these controls are documented into a Statement of Applicability (SoA). Further, the SoA references the policies, procedures or other documentation or systems through which the selected control would be evident.

To meet its specific security objectives, the organization should define, implement, monitor, review and improve applicable controls specified in the SoA. As a requirement for continued certification, organizations are required to conduct internal audits at planned intervals to provide information on whether the organization's ISMS conforms to the requirements set out in the standard as well as assess the organization's ability to meet its own information security requirements.

ITM has held the ISO 27001 certification for 11 consecutive years and was last re-certified on ISO 27001:2013 in 2021. The re-certification takes place every three years after the external auditors review the ISMS for compliance with the standard. ITM is in the process of transitioning to the ISO 27001:2022 version and will be audited against the updated standard in June 2024. Therefore, this internal audit served as a pre-assessment to evaluate compliance to the new standard in preparation for the external audit. The scope of the ISMS was defined by ITM, and it is managed and maintained by ITM's information security team whose overall responsibility is to manage information security risks for UNDP.

II. Audit results

Effective controls were established and functioning in the following areas:

(a) People Controls. People-related controls were found to be adequate with no non-conformances identified.
(b) Physical Controls. There were no non-conformances identified in the review of physical controls.
(c) Technological Controls. Technological controls were found to be adequate with no non-conformances identified.

OAI made two recommendations ranked as minor non-conformity (medium/important priority).

Observations and opportunities for improvement (low risk) findings were discussed directly and agreed with ITM and are included as Annex 1 of this report.

Minor non-conformity (medium priority) recommendations, arranged according to significance:
(a) Implement an appropriate risk treatment option for Risk ID 52 (Recommendation 1).
(b) Develop a cloud exit process that can be followed (Recommendation 2).

A. Organization controls

1. Information security risk treatment

Issue 1 No risk treatment applied to a long outstanding risk

ISO 27001:2022 standard control 6.1.3 requires organizations to define and apply an information risk treatment process to implement appropriate information security risk treatments in response to findings in risk assessments and/or audits. The information security risk treatment process is documented in the annual information security risk assessment and the risk treatment plan is a part of it.

[redacted]

Risks that are left untreated could lead to the exposure of personally identifiable information and can also adversely affect the future outlook of the overall information security management system.

Priority	Minor non-conformity
Recommendation 1: [redacted]	
Management action plan: [redacted] **Estimated completion date:** March 2024	

2. Information security for use of cloud services

Issue 2 No cloud exit process in place

ISO 27001:2022 standard control 5.23 requires that processes for acquisition, use, management and exit from cloud services be established in accordance with the organization's information security requirements. A cloud exit process, while not used on a day-to-day basis, is critical in the event an organization decides to exit from the cloud to some other arrangement.

At the time of this audit, UNDP did not have a cloud exit process documented and approved.

The lack of a cloud exit strategy can lead to negative consequences such as prolonged system downtime, decreased productivity, and even data loss if there is a need to alter the cloud strategy or provider.

Priority	Minor non-conformity
Recommendation 2: ITM should develop a cloud exit process that can be followed should there be a need to change from a cloud environment or transition to a different service provider.	
Management action plan: ITM will create a new standard called "Cybersecurity for cloud services" acquisition, governance and termination. The standard will address the process to be followed to terminate a cloud service. **Estimated completion date:** June 2024	

Annex 1: Observations and Opportunities for Improvement

Observations			
#	ISO 27001 Clause	Description	Recommendation
1	Annex A 5.22 **Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	[redacted]	[redacted]
2	Annex A 8.15 **Control** Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected and analyzed.	[redacted]	[redacted]
3	Annex A 8.12 **Control** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	[redacted]	[redacted]
4	Annex A 5.23 **Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	[redacted]	[redacted]

[3] RACI Matrix is a responsibility assignment matrix.

5	Annex A 8.9 **Control** Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored and reviewed.	There is no evidence of a documented configuration standards for the software and network services. Although Centre for Internet Security (CIS) benchmark is being followed, there is no evidence of a documented configuration standards for the software and network services	It might be beneficial to document configuration standards for software and network services using the guidance from CIS Benchmarks that are already being used.
Opportunities for improvements			
#	IS) 27001 Clause	Description	Recommendation
1	6.1.2 **Control** The organization shall define and apply an information security risk assessment process that establishes and maintains information security risk criteria that include: - the risk acceptance criteria.	Agreeing and documenting the management level of who will be authorized to make decision on risks, e.g., accepting untreated risks	It might be beneficial to document the minimum management level for the person taking decisions on risks such as risk acceptance. This will mitigate the risk of entry level management accepting risks which have high impact on UNDP or their stakeholders.
2	6.1.3 **Control** The organization shall define and apply an information security risk treatment process to select appropriate information security risk treatment options, taking account of the risk assessment results and determine all controls that are necessary to implement the information security risk treatment options chosen.	During the management review meetings, it was noted that there were no deadlines for executing risk mitigation actions plans related	It might be beneficial to include deadline for executing those action plans.
3	Annex A 5.13 **Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	There are no examples of different types of classification of data included in the Information classification and handling policy to guide users in application of the policy	It might be beneficial to include examples for different types of document classifications to help staff accurately apply the most appropriate data classification label.
4	Annex A 8.15 **Control**	Log collection policy does not mention the minimum log data retention period, and this should	It might be beneficial to include the minimum log data retention, and this

	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	be reflected in contracts where applicable	should be reflected in the contracts where applicable

Definitions of audit terms - ratings and priorities

A. AUDIT RATINGS

▪ **Fully Satisfactory**	The assessed governance arrangements, risk management practices and controls were adequately established and functioning well. Issues identified by the audit, if any, are unlikely to affect the achievement of the objectives of the audited entity/area.
▪ **Satisfactory / Some Improvement Needed**	The assessed governance arrangements, risk management practices and controls were generally established and functioning, but need some improvement. Issues identified by the audit do not significantly affect the achievement of the objectives of the audited entity/area.
▪ **Partially Satisfactory / Major Improvement Needed**	The assessed governance arrangements, risk management practices and controls were established and functioning, but need major improvement. Issues identified by the audit could significantly affect the achievement of the objectives of the audited entity/area.
▪ **Unsatisfactory**	The assessed governance arrangements, risk management practices and controls were either not adequately established or not functioning well. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area.

B. PRIORITIES OF AUDIT RECOMMENDATIONS

▪ **High (Critical)**	Prompt action is required to ensure that UNDP is not exposed to high risks. Failure to take action could result in major negative consequences for UNDP.
▪ **Medium (Important)**	Action is required to ensure that UNDP is not exposed to risks. Failure to take action could result in negative consequences for UNDP.
▪ **Low**	Action is desirable and should result in enhanced control or better value for money. Low priority recommendations, if any, are dealt with by the audit team directly with the Office management, either during the exit meeting or through a separate memo subsequent to the fieldwork. Therefore, low priority recommendations are not included in this report.

ISO Audit Ratings for Findings[4]

▪ **Major non-conformity**	Major non-conformity is defined as a nonconformity that affects the capability of the ISMS to achieve the intended results (equivalent to high rated recommendation as per OAI's priorities of audit recommendations).
▪ **Minor non-conformity**	Minor non-conformity is a nonconformity that does not affect the capability of the ISMS to achieve the intended results (equivalent to medium rated recommendation as per OAI's priorities of audit recommendations).
▪ **Observations**	Observations are items that may turn into non-conformities if not addressed (equivalent to low recommendation as per OAI's priorities of audit recommendations).
▪ **Opportunities for Improvement**	Opportunities for improvement are suggestions that can help improve the ITSM or prevent a possible non-conformance in the future (equivalent to low recommendation as per OAI's priorities of audit recommendations).

[4] https://auvacertification.com/