



United Nations
Educational, Scientific and
Cultural Organization

Organisation
des Nations Unies
pour l'éducation,
la science et la culture

Organización
de las Naciones Unidas
para la Educación,
la Ciencia y la Cultura

Организация
Объединенных Наций по
вопросам образования,
науки и культуры

منظمة الأمم المتحدة
للتربية والعلم والثقافة

联合国教育、
科学及文化组织

Internal Oversight Service

IOS/AUD/2010/09

Original: English

Audit of the UNESCO Data Center

June 2010

Contributors:
Sameer Pise
Prashant Sharma

Executive Summary

Introduction

The objective of the audit was to determine how UNESCO's Data centre operation is managed vis-à-vis comparable industry norms in the following areas:

- Integrity of data and protection of IT assets from unauthorized access, damage, theft and failures.
- Services levels based on documented definition and agreement on IT requirements.
- Established mechanisms for periodic review of data center performance and capacity levels.
- Service continuity to ensure minimal business impact in the event of an IT failure.
- Cost effectiveness when compared to similar public institutions including consideration of outsourcing opportunities such as ICC.

Accordingly, we have assessed the existence of following risks relevant to the audit objectives.

- Insufficient process for defining service levels.
- Insufficient capacity planning for key business processes and overall business need for IT services may exceed capacity.
- Insufficient planning for: risk, vulnerabilities and threats for IT operations; or the impact and recovery of loss IT services.
- Responsibilities and accountabilities not assigned for ensuring security
- Insufficient process to report and manage the IT infrastructure.
- Absence of process to ensure transparency and understanding of IT costs and improving cost-efficiency through well informed use of IT services.

The methodology used for the audit assignment is presented in Appendix V.

The key findings, risks, and recommendations relevant to the audit objectives set forth in the TOR are given below.

Key findings

- UNESCO's datacenter operation falls below industry norms:

Audit objective	Industry Average*	UNESCO
Integrity of data and protection of assets	3.12	2.14
Services levels	3.22	1.59
Performance review	3.62	1.24
Service continuity	3.40	2.11

*CobiT Maturity level rating on a scale of 1 to 5

- Current data center budget is insufficient to manage risks of IT service disruption and recovery
- UNESCO's IT operations as a whole are under-resourced with comparable institutions:

Metric	2010 industry average range*	UNESCO**
IT spending per employee	\$11,474 – \$ 7,430	\$3,100
IT employees % of total employees	5.6% - 3.8%	2.9%

*Source: Gartner IT Key Metrics Data 2010 (Government Analysis)

**UNESCO figures are preliminary and work is ongoing

- Effective IT governance is needed for proper resource planning

Principal Recommendation

Recommendation 5.1: We recommended that ADM/DIT conducts a cost-benefit analysis to ascertain whether UNESCO outsources the data center operations or continues to maintain it in-house. The analysis should be completed before the end of September 2010 to facilitate timely deliberations for eventual submission of budget proposal to 36 C/5.

Recommendations

Upon implementation of the principal recommendation, the recommendations listed in Table 1 and conditional recommendations in Table 2 should be implemented.

Table 1

The following recommendations apply irrespective of the decision to outsource or continued hosting of data centre in-house.

Recommendation 1.2	We recommend that ADM/DIT fully develops policies and procedures governing facilities maintenance, physical security and environmental
Recommendation 1.3	We recommend that ADM/DIT define mission, goals, and objectives of the Unit of System Security and Operations
Recommendation 1.4	We recommend ADM/DIT to establish scope of responsibilities of the IT Security officer(s) as well as define the appropriate job descriptions
Recommendation 1.5	We recommend ADM/DIT to ensure that IT Security officer(s) has appropriate knowledge and experience to carry out IT security operations
Recommendation 2.1	We recommend that CISS formulate and communicate the required IT service levels to ADM/DIT ; Required service levels should reflect strategic goals of the Organization and are evaluated against industry norms.
Recommendation 2.2	We recommend that ADM/DIT develop a formal SLA and establish an effective process for managing and monitoring the service levels expected by its customers.
Recommendation 3.1	We recommend that ADM/DIT establishes a comprehensive reporting system. Reporting of monitoring results should be formalized and standardized. There should be integration of metrics across major IT processes.

Recommendation 4.1	We recommend that CISS formulates and communicates the disaster recovery objectives to ADM/DIT.
---------------------------	---

Table 2

Recommendations apply (1.1, 2.3, 4.2 and 5.2) in the event UNESCO decides to continue hosting data center in-house.

Recommendation 1.1	If the Datacenter is not substantially outsourced, we recommend that ADM/DIT acquire and install additional equipment to Fontenoy and Miollis sites for ensuring integrity of data and protection of IT assets from disruption, failures, and damage
Recommendation 2.3	If the Datacenter is not substantially outsourced, we recommend ADM/DIT to consider establishment of a new unit or sub-unit within ADM/DIT for Data Center Operations
Recommendation 4.2	If the data center is not substantially outsourced, ADM/DIT should develop and test the formulated disaster recovery plans.
Recommendation 5.2	If the Datacenter is not substantially outsourced, we recommend that ADM/DIT and senior management consider the possibility of hiring additional permanent staff in ADM/DIT/SOA to meet the growing needs of the Organization in IT services.