



## **INTERNAL AUDIT DIVISION**

# **AUDIT REPORT**

---

### **Information security management certification in the Office of Information and Communications Technology**

**The information security management system  
established by OICT is compliant with the  
certification standard ISO-27001**

**30 June 2010  
Assignment No. AT2010/517/01**

---

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

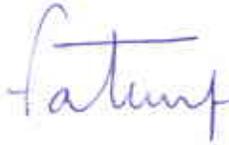
MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES - BUREAU DES SERVICES DE CONTRÔLE INTERNE  
INTERNAL AUDIT DIVISION - DIVISION DE L'AUDIT INTERNE

TO: Mr. Choi Soon-hong, Assistant Secretary-General,  
A Chief Information Technology Officer  
Office of Information and Communications Technology

DATE: 30 June 2010

FROM: Fatoumata Ndiaye, Director  
DE: Internal Audit Division, OIOS



REFERENCE IAD: 10- **00546**

SUBJECT: **Assignment No. AT2010/517/01 – Audit of the information security management certification in the Office of Information and Communications Technology**  
OBJET: **Assignment No. AT2010/517/01 – Audit of the information security management certification in the Office of Information and Communications Technology**

1. I am pleased to present the report on the above-mentioned audit.
2. Based on your comments, we are pleased to inform you that we will close recommendations 1 and 2 in the OIOS recommendations database as indicated in Annex 1. In order for us to close the remaining recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
3. Your response indicated that you did not accept recommendations 2 and 5. In OIOS' opinion however, these recommendations seek to address significant risk areas. We are therefore reiterating them and requesting that you reconsider your initial response based on the additional information provided in the report.
4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendation 5) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors  
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit  
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management  
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS  
Mr. Gurbur Kumar, Acting Deputy Director, Internal Audit Division, OIOS

---

## INTERNAL AUDIT DIVISION

---

### **FUNCTION**

*“The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization” (General Assembly Resolution 48/218 B).*

---

### **CONTACT INFORMATION**

#### **DIRECTOR:**

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,  
e-mail: [ndiaye@un.org](mailto:ndiaye@un.org)

#### **ACTING DEPUTY DIRECTOR:**

Gurpur Kumar: Tel: +1.212.963.5920, Fax: +1.212.963.3388,  
e-mail: [kumarg@un.org](mailto:kumarg@un.org)

---

## **EXECUTIVE SUMMARY**

### **Audit of the information security management certification in OICT**

OIOS conducted an audit of the information security management certification in the Office of Information and Communications Technology (OICT). The overall objective of the audit was to determine whether OICT had adequate controls and mechanisms in place to govern its information security management system in conformance with the control requirements of the certification standard ISO-27001. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

In general, OIOS found that OICT has adequately documented and implemented the information security management systems related to the local and metropolitan area networks in accordance with the requirements of the international certification standard ISO-27001. However, the system could be improved with the implementation of the following additional controls:

- (a) Document the linkage between controls and their supporting evidence;
- (b) Develop a policy requiring the systematic identification and documentation of preventive and corrective actions taken to address cases of nonconformity;
- (c) Develop a policy defining requirements for data restoration procedure; and
- (d) Requirements for a proactive analysis and alerting system of potential exceptions detected in the administrators' logs.

## TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-7
II. AUDIT OBJECTIVES	8
III. AUDIT SCOPE AND METHODOLOGY	9-11
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Documents and records controls	12-15
B. Governance	16-22
C. Risk management	23-28
D. Statement of applicability	29-31
E. Corrective and preventive actions	32-34
F. Asset management	35-38
G. Physical and environmental security	39-41
H. Change management	42-45
I. Capacity management	46-50
J. Backup	51-55
K. Media handling	56-59
L. Access controls	60-71
M. Information security incident management	72-76
N. Business continuity	77-82
V. ACKNOWLEDGEMENT	83
ANNEX 1 – Status of Audit Recommendations	

---

## I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the information security management certification in the Office of Information and Communications Technology (OICT). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. OICT is responsible for providing overall computing, telecommunications, office automation, software, and hardware and infrastructure support at United Nations Headquarters in New York and, in cooperation with the Department of Peacekeeping Operations (DPKO) as appropriate, for lease lines and satellite communications to the overseas duty stations. The previous Information Technology Services Division (ITSD) is now fully integrated into OICT.

3. OICT also provides infrastructure support for enterprise-wide applications such as the Integrated Management Information System (IMIS), Galaxy, email and the Official Document System (ODS), as well as consulting and advisory services to all offices of the Secretariat, as well as research and development of new technologies.

4. Within OICT, the Strategic Management Service (SMS) is responsible for coordinating activities that affect all ICT units in the Secretariat; measuring progress on an ongoing basis to ensure strategic alignment, information technology resource and quality controls, and compliance of Secretariat-wide policies; as well as providing ICT-related business consulting and project management services, including portfolio management, process re-engineering, support for project methodologies, business case development and project reviews.

5. The six functional areas that comprise the work of SMS are:

(a) Business Relationship Management, further distinct in:

- i) Client Services;
- ii) Project Management Office; and
- iii) Work Practices.

(b) Technology Policy and Standards, further distinct in:

- i) Architecture and Standards;
  - ii) Quality Assurance and Audit; and
  - iii) Security.
-

---

6. In March 2006, OICT (formerly known as ITSD) certified its information security management system for the local and metropolitan area networks (LAN and MAN) in accordance with the international standard for security management systems ISO-27001 (previously known as BS-7799 and ISO-17799). The certification process included an external audit conducted by the British Standard Institution of the following domains and activities:

- (a) Security Policies;
- (b) Organization of Assets and Resources;
- (c) Asset Classification and Control;
- (d) Personnel Security;
- (e) Physical and Environmental Security;
- (f) Communications and Operations Management;
- (g) Access Control;
- (h) Systems Development and Maintenance;
- (i) Business Continuity Management; and
- (j) Compliance with international standards and UN rules & regulations.

7. Comments made by OICT are shown in *italics*.

## **II. AUDIT OBJECTIVES**

8. The main objectives of the audit were to:

- (a) Determine whether the OICT has adequate controls and mechanisms in place to ensure continuous sustainability and governance of its information security management system (ISMS) in conformance with the requirements of the certification standard ISO-27001; and
- (b) Assess whether adequate risk assessment and management procedures have been put in place for the management of the information management system.

## **III. AUDIT SCOPE AND METHODOLOGY**

9. The audit was conducted at the United Nations Secretariat in New York, in accordance with the control requirements established by the certification standard for information security management systems (ISMS) ISO-27001.

---

10. The review included interviews with officers in charge of the relevant functions, analysis of the documentation supporting the controls established, and site inspections of the primary data centre located in the 19<sup>th</sup> floor of the United Nations Headquarters in New York, and the secondary data centre in Piscataway, New Jersey.

11. In accordance with the requirements of the certification standard ISO-27001, the audit referenced the "Statement of Applicability" prepared by the United Nations Secretariat for its information security management system established at Headquarters in New York.

## **IV. AUDIT FINDINGS AND RECOMMENDATIONS**

### **A. Documents and record controls**

12. The documentation supporting the ISMS should include records demonstrating that any actions taken with regard to the security of the information systems are traceable to management decisions and policies, and ensure that the recorded results are reproducible.

13. OICT developed an automated system to monitor and maintain all the documents and referenced records related to the ISMS. This system is based on a web interface and is called the "UN Rosetta Stone". However, this system did not indicate which control(s) were supported by each document, to ensure that there were no dependencies on obsolete documents. In addition, there was no indication of which version – paper based or electronic - of the documentation related to the ISMS was the official controlled version.

#### **Recommendations 1 and 2**

**(1) OICT should ensure that the documents stored in the "UN Rosetta Stone" are current and aligned with the controls listed in the statement of applicability.**

**(2) OICT should clearly state that the documentation supporting the information security management system of the United Nations Secretariat in New York is maintained electronically and footnote each electronic document that "All printed documents are considered uncontrolled".**

14. *OICT accepted recommendation 1, and stated that it had already been implemented. Based on the action taken by OICT, recommendation 1 has been closed.*

15. *OICT did not accept recommendation 2 stating that its description does not reflect the existing situation in OICT since there is no automated tool to maintain the documents supporting the ISMS. Some of the documents supporting*

---

*ISMS are paper based because of process requirements. Samples or templates of these documents are stored in ISMS tool.* OIOS acknowledges the clarifications provided by OICT with regard to the documentation supporting the ISMS. However, since the requirement for controlling the documentation is still applicable, regardless of the means (manual or electronic) utilized for its support, it is still necessary for OICT to implement adequate mechanisms to demonstrate that documents are controlled. In particular, these controls pertain to the date, version, and ownership of each document supporting the ISMS. Recommendation 2 remains open pending receipt from OICT of evidence demonstrating that adequate controls mechanisms have been implemented to control all the manual documents supporting the ISMS.

## **B. Governance**

### Management controls

16. The certification standard ISO-27001 requires evidence of management's commitment for the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS. This commitment is usually supported by evidence of the following controls:

- (a) Issuing an ISMS policy;
- (b) Defining ISMS objectives and plans;
- (c) Allocating roles and responsibilities for information security;
- (d) Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy;
- (e) Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
- (f) Deciding the criteria for accepting risks and the acceptable levels of risk;
- (g) Ensuring that internal ISMS audits are conducted; and
- (h) Conducting management reviews of the ISMS.

17. OIOS' interviews with relevant staff confirmed that management is dedicated to ensuring continued improvement of the ISMS. Information security policy is documented, reviewed and approved and is communicated to all staff. Management reviews and responsibilities are outlined in "Policy for the Management Review of the Information Security Management System" (ISMS dated 9-4-2009 V. 3.0).

18. Management's commitment to information security is formalized by the policy requirements to establish a formal ISMS. This commitment is further

---

demonstrated by the funding of costs associated with all security projects ensuring their continual improvement. Other security-related initiatives (i.e. Identity management programme) are also being implemented to complement and strengthen the ISMS.

19. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

Information security management scope

20. The ISMS should be based on clearly defined elements, including its scope and boundaries in terms of the characteristics of the organization, location, assets and technology, and details of and justification for any exclusion from the scope.

21. The “UN scope of work”, dated 24 February 2010, provided evidence that the Organization has defined the scope and boundaries of the ISMS in terms of the characteristics of the organization, its departments, their location, assets and technology. The scope included a framework for setting objectives and establishing an overall sense of direction and principles for action with regard to information security. The scope also aligned with the Organization’s strategic risk management context in which the establishment and maintenance of the ISMS took place.

22. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

**C. Risk management**

23. Documentation shall demonstrate the relationship between security controls and mitigating measures implemented to address the risks identified, their corresponding treatment plans, and the ISMS policy.

24. The “ICT security, business continuity and emergency preparedness policy” defined the criteria against which information security risks have been evaluated.

25. OICT has adopted the methodology called “Octave” (Operational Controls, Threats, and Vulnerability Evaluation) to ensure that risk assessments produce comparable and reproducible results. Also, documented evidence showed that risks were assessed on the basis of identified threats, vulnerabilities, and their impact. Management approved any residual risk that was applicable.

26. A total of 80 threats were used to evaluate risks and cross-functional teams were involved to triage threats and evaluate risks. Three types of vulnerability scans were run to provide data about the likelihood of each threat. The three main security requirements for confidentiality, integrity, and availability were evaluated for each threat. Any initial risk without a mitigating control was ranked on a scale 0 – 5 and accepted as is. All risks ranking “High” required an action documented with a remediation plan.

---

27. The risk evaluation was sent to the "ICT Security Board" where only medium and high risks were discussed. The ICT Security Board reviewed and decided on mitigating controls, ordering technical investigation on specific items even when the risk had been accepted.

28. Since there was documented evidence showing that the Organization defined and implemented an adequate risk assessment approach and methodology, with criteria for accepting risks, OIOS is not issuing any recommendation in this area.

#### **D. Statement of applicability**

29. The certification standard requires the preparation of a "Statement of Applicability" describing which of the controls listed in the standard have been implemented and why. In this regard, the statement should include:

- (a) The objectives of the controls currently implemented, with the reason for their selection; and
- (b) The justification for exclusion of any of the controls listed in the standard.

30. The "Statement of applicability" of the United Nations Secretariat was documented and it included the list of standard controls selected and the reason for their selection. While the statement included the controls currently implemented, it did not contain adequate details justifying why two controls were excluded from the ISMS implementation.

#### **Recommendation 3**

**(3) OICT should complete the "Statement of applicability" with additional details regarding the exclusion of certain standard controls.**

31. *OICT accepted and already implemented recommendation 3 with the definition of the out of scope controls.* Based on the action taken by OICT, recommendation 3 has been closed.

#### **E. Corrective and preventive actions**

32. Adequate actions should be taken to both prevent and correct the causes of nonconformities with the ISMS control requirements. In support of these actions, a documented procedure should define requirements for:

- (a) Identifying nonconformities;
- (b) Determining the causes of nonconformities;

- 
- (c) Evaluating the need for actions to ensure that nonconformities do not recur;
  - (d) Determining and implementing the preventive or corrective actions needed;
  - (e) Recording results of actions taken; and
  - (f) Reviewing of actions taken.

33. OICT had a set of recorded instances where it took actions for eliminating the causes of nonconformities and preventing their recurrence. The Change Management Unit had a process in place for recording actions taken with regard to nonconformities, and the management review policy required a review of the corrective and preventive actions implemented. However, many of the target dates had passed with no updates, and interviews with process owners indicated that updates were reviewed only at subsequent management reviews. Therefore, OICT lacked a formal documented procedure or policy outlining guidelines for corrective and preventive actions as required by the certification standard.

#### **Recommendation 4**

**(4) OICT should develop and implement a policy requiring the systematic identification and documentation of nonconformities with control requirements and their causes, evaluation of the need for corrective actions, and recording the results of their implementation.**

34. *OICT accepted recommendation 4 and stated that based on the input provided during the audit, OICT Security Board, in its first quarter meeting on March 2010, decided to develop a separate procedure for outlining the guidelines for corrective and preventive actions.* Recommendation 4 remains open pending receipt from OICT of the procedure for the systematic identification and documentation of nonconformities with control requirements.

#### **F. Asset management**

35. The certification standard requires controls for protecting organizational assets. These controls include: i) Inventory of assets; ii) Definition of their ownership; iii) Acceptable use policies; iv) Classifications; and v) Labeling.

36. The United Nations Secretariat has an acceptable use policy (ST/SGB/2004/15), and uses two tools for managing and monitoring assets: i) E-Comp; and ii) Procure Plus. These two applications were cross-referenced, and a formal process was in place for approving additions, changes, and disposal of assets. An administrator reviews all requests prior to their approval.

37. OIOS reviewed a sample of random assets and found that:

- 
- (a) Virtual assets were linked to the physical assets that they served;
  - (b) A team (VMWARE team) was responsible for all virtual assets;
  - (c) All asset approvals were routed through the E-Comp tool and approval signatures were noted; and
  - (d) Assets were categorized in the risk assessment process.

38. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

### **G. Physical and environmental security**

39. The standard control requirements for physical and environmental security include the definition of the following:

- i) Physical security perimeter;
- ii) Physical entry controls;
- iii) Securing offices, rooms and facilities;
- iv) Protecting against external and environmental threats;
- v) Working in secure areas;
- vi) Public access, delivery and loading areas;
- vii) Equipment siting and protection;
- viii) Supporting utilities;
- ix) Cabling security;
- x) Equipment maintenance;
- xi) Security of equipment off-premises;
- xii) Secure disposal or re-use of equipment; and
- xiii) Removal of property.

40. OIOS reviewed the physical protective measures put in place for the primary data centre located in the 19<sup>th</sup> floor of the United Nations Secretariat building, and the secondary data centre in Piscataway, New Jersey. The review highlighted the following:

- i) Access to the data centres is regulated with a policy dated 1-27-10, version. 1.0;

- 
- ii) Data centres are locked down and require a limited/approved number of access cards. All entries must pass through a gate keeper;
  - iii) Security desk at entrance is manned 24X7;
  - iv) The Director of Operations approves all access for all operators. As some operators are contract workers, access is reviewed for those resources on a regular basis;
  - v) Access granted to the data centres is reviewed every 6 months and it is subject to automatic expiration;
  - vi) Every person with access to the data centres receives an e-mail to confirm their need and justification for continued access. If there is no response, access is deleted;
  - vii) The most recent access list, labeled "OICT-17", appeared to be up-to-date;
  - viii) Cabling was generally under the floor and unstructured locally; and
  - ix) The New Jersey data centre is compliant with the latest construction standard (TIA-942), and environmental controls. The data centre has redundant power feeds and runs on two separate power grids.

41. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

## **H. Change management**

42. Changes to information processing facilities and systems should be controlled and documented.

43. OICT has a change management procedure and a technical group is responsible for reviewing and approving changes. Emergency and backup plans exist and used as applicable. All change requests are managed and monitored by the Chief Information Technology Officer (CITO). In addition, when applicable, there is a process for notifying users of a service interruption.

44. In addition, a testing environment is used for testing changes before their release into production. Control mechanisms were in place to detect and address instances of deployed changes with adverse impact on the local and metropolitan area network (LAN and WAN). Regular reports were issued to review and monitor metrics and indicators of performance of the network.

45. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

---

## **I. Capacity management**

46. The use of network resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

47. OICT implemented a system for measuring network capacity on a real-time, monthly and yearly basis. Thresholds are set and administrators are alerted when the system exceeds the thresholds. Current thresholds measured are based on bandwidths (MB/S). Only daytime data is used to evaluate usage history as to avoid skewing results by injecting evening data where there is typically less usage.

48. The introduction of new systems is supported by a testing process performed in a lab environment (sandbox). A controlled set of users are issued access to evaluate the new system in a segregated testing environment. Evaluation and feedback is analyzed and decisions made concerning acceptance or additional actions.

49. While server capacity is not directly part of the network environment, it has interrelationships with their scope and therefore it is necessary that the network process owners monitor and review data on a regular basis. OIOS reviewed servers and network capacity reports and found that these services were being monitored.

50. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

## **J. Backup**

51. Backup procedures should be defined, implemented, and regularly tested to ensure availability of data.

52. OICT has a backup procedure based on the following architecture and control mechanisms:

- i) Control server initiates the backup with storage nodes that talk to the servers;
- ii) Nodes backup locally, but indexes are sent to the central repository;
- iii) Failures are re-run during the weekend;
- iv) Backups are sent to virtual libraries and data is then moved to physical tapes for off-site storage. Both full and incremental backups are scheduled; and

- 
- v) Retention schedule is documented and based on a backup retention policy.

53. OIOS noted that there is no formal restore procedure and there are daily restore requests that are tested at the time of processing. This seems to be an informal and optional practice that has not been formally reviewed and approved by management in accordance with the "Enterprise backup system policy" dated 1 January 2009, stating that it is a good practice for both user offices and ITSD to test periodically the restoration procedures based on some fictional scenarios.

54. In addition, restores done for investigative purposes were not subject to a special classification and documentation to ensure confidentiality.

#### **Recommendation 5**

**(5) OICT should update its enterprise backup system policy with specific requirements for restore procedures, including the need to document and classify the restoration tasks performed in the context of investigations.**

55. *OICT did not accept recommendation 5, stating that restores for investigative purposes are not in the scope of the ISO-27001 certification and performed according to the requirements of ST/SGB/2004/15. According to section 9.2.d of this SGB, these requests and all the activities to support investigations are treated as confidential and no records for such access shall be retained by OICT. In OIOS' opinion, OICT did not address the substance of recommendation 5, related primarily to the need of updating the enterprise backup system policy with specific requirements for restore procedures. Furthermore, the fact that restores for investigative procedures are conducted in accordance with the requirements established by ST/SGB/2004/15 is an additional element that should be simply referenced in the policy when the recommended update is completed. Recommendation 5 remains open pending receipt from OICT of the updated enterprise backup system policy, including the reference to the restores conducted for investigative purposes in accordance with ST/SGB/2004/15.*

#### **K. Media handling**

56. Media should be protected to prevent unauthorized access, disclosure, modification, removal or destruction. In this regard, a policy should regulate the following aspects related to media handling:

- i) Management of removable media;
- ii) Disposal of media;
- iii) Information handling procedures; and
- iv) Security of system documentation.

---

57. Media handling in the United Nations Secretariat is regulated by ST/AI/2001/4, "Disposal of computer equipment at the United Nations Headquarters". In addition, procedures for handling and storing information are defined in the "ITSD Divisional ICT Security, Business Continuity and Emergency Preparedness Policy"(Version 3.0). System documentation is currently on a file share accessible only by OICT.

58. The physical management of media storage is outsourced to an external company (Iron Mountain). Media that is no longer required are disposed of on the basis of ST/AI/2001/4. However, at the time of the audit, media was not being disposed of and stored in a secure locked environment. Smaller media such as CDs were shredded.

59. OICT has started a procurement process to identify an external entity to handle disposal, and confirmed that after the issuance of the audit draft report adequate space for the disposal of media is available. Therefore, OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place on the basis of the

#### **L. Access controls**

60. Access to information resources should be controlled and monitored on the basis of the following requirements and functions:

- i) Organizational requirements for access control;
- ii) User access management;
- iii) User responsibilities;
- iv) Network access control;
- v) Operating system access control;
- vi) Application and information access control; and
- vii) Remote access and teleworking.

#### Requirements for access control and user management

61. OICT has implemented a user registration procedure requiring that each request for access must be routed through a service team for approval based on access requirements. Notifications are sent to the users and/or service teams. The "User Registration Group" conducts reviews at regular intervals to confirm and validate user's access rights.

62. The logs of the administrators are reviewed on a random basis to prevent the establishment of patterns. However rules and alerting mechanisms for

---

monitoring the logs do not exist. Logs are stored on a backup media, creating an audit trail.

#### **Recommendation 6**

**(6) OICT should define rules and develop mechanisms for a proactive monitoring of exceptions that could be detected in the administrator's logs, with the generation of automated alerts.**

63. *OICT accepted recommendation 6 and stated that the need for effective management of logs has been already recognized and efforts have been started to evaluate alternative solutions for centrally managing and monitoring of logs. Recommendation 6 remains open pending receipt from OICT of the rules and mechanisms for proactive monitoring of exceptions in the administrator's logs, with the generation of automated alerts.*

#### User responsibilities

64. Users' responsibilities with regard to accessing information technology resources are regulated by the ST/SGB/2004/15, "Use of information and communications technology resources and data".

#### Application access control

65. OICT procedures require that any application accessed through a user login process must be protected with secure connections (Secure Socket Layer, SSL). There is a process for the approval of the SSL registrations.

66. Connection timeouts are monitored by each application and timed out on predefined rules. Networks and firewalls use standard Cisco timeout sessions.

#### Network access control

67. Network access control is segregated into network segments. Each segment is used for a different purpose. Procedures are in place to require a request for an internet protocol (IP) address. OICT employs a tool for registering IP addresses (i.e. IMIS User Application System). Some network segments are processed manually because they are externally facing processes.

68. Shared networks require a separate password for each segment. Each access is authorized separately. Sensitive networks are completely isolated from other networks.

69. All network devices are monitored 24x7 by the "Network Operations Center" (NOC). Issues are re-analyzed on a regular basis to detect consistency correlations with other events. Formal incidents are analyzed using root cause analysis and reported to management on a regular basis.

#### Remote access and teleworking

---

70. Remote access requests are processed based on the "Secure remote network operations – user registration" procedure. Telecommuters use secure connections (either SSL or Virtual Private Network, VPN). Mobile access requires two factor authentications with a password and token authentication. (using RSA servers). A different token is generated each minute to ensure the highest level of security (token and RSA server then communicate to authenticate the user).

71. OIOS is not issuing any recommendations in this area since the requirements of the certification standard appear to be in place.

### **M. Information security incident management**

72. Procedures should be in place to ensure that information security incidents are timely reported and managed, including requirements for follow-up and lessons learned.

73. OICT established a procedure for reporting and tracking incidents by e-mail or phone. Incidents are categorized and e-mail notifications are sent to the responsible group, and subsequently escalated on the basis of their priority. Information security events are documented and reported through appropriate management channels.

74. The incident management procedure is supported by an automated system ("iNeed") for documenting and tracking events. The resolution of incidents is updated in the system and closed by the service group.

75. Corrective actions are based on the analysis of metrics that are reported on a monthly basis for all incidents.

76. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

### **N. Business continuity**

77. The Organization should have adequate procedures in place to ensure the continuity of its critical processes in case of failure of information systems or disasters.

78. The United Nations Secretariat started a business continuity management (BCM) initiative in 2007. A dedicated unit was created for supporting BCM with the mandate to document the necessary information about critical processes and requirements of each office in the Secretariat.

79. A risk management and business impact analysis was conducted on all relevant processes and organizational entities. A cost benefit analysis was completed and funding obtained for the BCM initiative in 2008.

80. A specific disaster recovery and continuity plan for information and communications technology operations has been developed in conjunction with

---

the BCM initiative. In this regard, OICT has adopted the framework based on an international standard (ISO 24762 IT Disaster Recovery), that included the definition of standard recovery time and point objectives (RTOs and RPOs).

81. All critical systems have been tested to ensure adequate fail-over in case of interruption. Since OICT is currently migrating the primary data centre to a new location, all current systems are being tested as they are migrated.

82. OIOS is not issuing any recommendations in this control area since the requirements of the certification standard appear to be in place.

## **V. ACKNOWLEDGEMENT**

83. We wish to express our appreciation to the Management and staff of OICT for the assistance and cooperation extended to the auditors during this assignment.

## STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date <sup>2</sup>
1	OICT should ensure that the documents stored in the "UN Rosetta Stone" are current and aligned with the controls listed in the statement of applicability.	Information Resources	Medium	C	Recommendation closed.	Implemented
2	OICT should clearly state that the documentation supporting the information security management system of the UN Secretariat in New York is maintained electronically and footnote each electronic documents that "All printed document are considered uncontrolled".	Information Resources	Medium	O	Implement mechanisms to control the date, version, and ownership of all manual documents supporting the ISMS.	Not provided
3	OICT should complete the "Statement of applicability" with additional details regarding the exclusion of certain standard controls.	Information Resources	Medium	C	Recommendation closed.	Implemented
4	OICT should develop and implement a policy requiring the systematic identification and documentation of nonconformities with control requirements and their causes, evaluation of the need for corrective actions, and recording the results of their implementation.	Governance	Medium	O	Implement procedures for the systematic identification and documentation of nonconformities with control requirements.	Q3-2010
5	OICT should update its enterprise backup system policy with specific requirements for restore procedures, including the need to document and classify the restoration tasks performed in the context of investigations.	Governance	High	O	Update the enterprise backup system policy, and include a reference to the restores conducted for investigative purpose in accordance with SI/SGB/2004/15.	Not provided

6	OICT should define rules and develop mechanisms for a proactive monitoring of exceptions that could be detected in the administrator's logs, with the generation of automated alerts.	Operational	Medium	O	Defines and implement rules and mechanisms for the proactive monitoring of exceptions in the administrator's logs, with the generation of automated alerts	Q4-2011
---	---	-------------	--------	---	--	---------

1. C = closed, O = open
2. Date provided by OICT in response to recommendations.