WORLD HEALTH ORGANIZATION

FIFTY-SIXTH WORLD HEALTH ASSEMBLY A56/29
Provisional agenda item 16.1 10 April 2003

Interim report of the External Auditor

The Director-General has the honour to transmit herewith to the Fifty-sixth World Health Assembly the interim report of the External Auditor on the World Health Organization for the financial period 2002-2003 (Annex).

ANNEX

INTERIM REPORT OF THE INDEPENDENT EXTERNAL AUDITOR TO THE FIFTY-SIXTH WORLD HEALTH ASSEMBLY: AUDIT OF THE WORLD HEALTH ORGANIZATION: 2002-2003 FINANCIAL PERIOD

INTRODUCTION

1. The audit of the World Health Organization (WHO) was assigned to the Auditor-General of the Republic of South Africa for the 2000-2001 and 2002-2003 financial periods, in terms of resolution WHA 52.8 of the fifty-second meeting of the World Health Assembly.

2. The purpose of this report is to inform the World Health Assembly of the salient matters arising from the external audit on a timely basis.

TERMS OF REFERENCE

3. The audit is performed in accordance with Regulation XIV of the Financial Regulations and the Additional Terms of Reference Governing the External Audit appended thereto. In accordance with these terms of reference, the auditor shall express an opinion on the financial statements for the financial period and report on the financial operations and various other matters set out therein.

4. The audit is conducted in accordance with the Common Auditing Standards of the Panel of External Auditors of the United Nations, the specialized agencies and the International Atomic Energy Agency.

5. The audit procedures that were carried out to date were not performed with the intention of expressing an audit opinion on the interim financial statements that are included in the Unaudited Interim Financial Report for the year 2002 (document A56/28).

OVERALL AUDIT APPROACH

6. A comprehensive audit approach which integrates financial, compliance and value-added aspects has been followed in performing the audit, with a view to providing WHO with an independent external audit service with an emphasis on promoting accountability, good governance and the effective, economic and efficient attainment of WHO's goals.

7. In this regard, continued emphasis has been placed on supporting existing governance structures through open and regular communication with the World Health Assembly and its organs on issues relating to the external audit process, as well as constructive interaction with the Secretariat. Related governance issues such as the internal audit function, delegations of authority and risk management have also been identified as key aspects of the governance structure and accordingly have been subjected to further external audit review.

8. In addressing the financial and compliance aspects of the audit, a risk-based approach has been adopted to ensure that audit resources are clearly focused. In this interim period, emphasis has been placed on performing these risk assessments and determining the related audit strategy for the remainder of the financial period. Interim substantive and analytical tests of transactions and account balances and procedures to test compliance with the Financial Regulations and legislative authority have also been performed at headquarters.

This work will be taken through to all of the regional offices during 2003 and then consolidated with the final audit at the financial period end.

9. The Director-General, the Regional Directors and the Secretariat are commended for the wide-ranging reforms implemented over the past years to ensure WHO rises to meet the number of challenges facing it, as it moves into the 21st century. The implementation of a strategic budgeting approach and results-based management has marked a significant shift from a focus on inputs, to an emphasis on outcomes and accountability for performance. The significant increase in extrabudgetary contributions introduces a number of new challenges, from ensuring that these resources are appropriately used to achieve WHO's strategic goals, through to ensuring that donor agreements are efficiently administered. Considerable cash balances and operations throughout the world mean that it is essential for WHO to actively manage its treasury function. WHO faces increasing pressure to modernise its approach to information and communication systems to ensure that the systems support the business objectives while related risks are actively managed. These are some of the issues considered during the interim period and commented on in this interim report.

10. The external audit strategic plan of work for the financial period 2002-2003 was presented to the seventh meeting of the Audit Committee (document EBAC7/3) and sets out in more detail the planned audit approach, activities and focus areas for this financial period. In this regard, it is envisaged that an organisation-wide evaluation of the fellowship programme, a review of the progress in implementing the country focus initiative as well as continued work in respect of issues pertaining to the governance of extrabudgetary funds will be performed in the coming year.

11. The implementation of external audit recommendations is tracked and the status reported to the Audit Committee. To date I am pleased to be able to report that a high level of co-operation has been received from the Secretariat and in general, I am satisfied with the progress achieved.

12. The matters arising from the current audit, as set out in the following paragraphs, have been thoroughly discussed with the Secretariat. I am pleased to note that the Secretariat has indicated that they welcome the recommendations made and will be taking steps to implement improvements.

GOVERNANCE

13. In recent years, increasing emphasis has been placed on issues relating to governance and the extent to which organisations are directed and controlled in a manner which supports openness, integrity and accountability. Issues relating to organisational structures, reporting to stakeholders, the systems of internal controls, and the values and standards of behaviour defined for the organisation are all important considerations.

14. WHO's commitment to supporting effective governance is well recognised. The revision of the Financial Regulations and Financial Rules together with improved financial reporting are some prior initiatives that I have welcomed. Issues previously raised relating to, *inter alia*, the implementation of a fraud prevention and contingency policy, a revised code of ethics and conduct and environmental policies, are all receiving the Secretariat's attention. In this interim period, attention has been paid to risk management, the internal audit function, delegations of authority and the WHO Manual as integral aspects of the governance framework.

Risk management

15. While risk assessment and management processes do exist in various forms throughout WHO, there is currently a lack of formalised risk management policy and strategy in place for WHO as a whole. WHO should review its risk assessment activity and implement an appropriate risk management architecture in which the significant exposures are identified and an appropriate strategy to manage these risks determined.

16. As part of the ongoing enhancement of the overall governance and risk management framework, the Secretariat has indicated that an overall risk management approach will be developed in close collaboration with Internal Audit and Oversight.

Internal audit function

17. In my interim report for 2000-2001, I reported the findings arising from a specialist review performed on the internal audit function. The purpose of the review was to provide an objective assessment of the Office of Internal Audit and Oversight (IAO) against the Standards for the Professional Practice of Internal Auditing promulgated by the Institute of Internal Auditors (IIA).

Initiatives introduced by the IAO

18. A progress review performed in February 2003 revealed that the IAO has introduced, amongst others, the following initiatives to improve its effectiveness:

a) In line with the decision of the Representatives of Internal Audit Services of United Nations Organizations and Multilateral Financial Institutions in June 2002, the IAO has adopted the IIA's Professional Practices Framework. Changes in the IAO charter to align it with the IIA standards are currently being considered by the Director-General. The IAO's policies and procedures have been reviewed and changes have been implemented to ensure compliance with the standards.

b) Staff development has been strengthened by the designation of an existing staff member as a training officer. The training needs of staff are being assessed and appropriate training interventions scheduled.

c) A risk assessment approach has been implemented, whilst various improvements to the planning, execution and reporting processes have been introduced. Certain audit programmes and documentation have been standardised and a follow-up tracking system has been implemented.

d) Key performance indicators have been elaborated. Supervisory processes have been introduced on larger audits and a quality review procedure has been adopted.

e) The IAO regularly communicates with senior management. Senior management is formally consulted on an annual basis during the preparation of the annual work plan. Discussions are held at the inception of each audit and during the reporting process. Management feedback is an integral part of the quality assurance process.

Areas for further improvement

19. The following areas for further improvement are highlighted:

a) The IAO should consider contributing to the implementation of an organisation-wide risk assessment process mentioned in paragraph 14 above. Once in place, the IAO could use management's risk assessment to prioritise its own activities as well as to determine its skills and resource requirements.

b) The annual operation plan is concise and does not describe the link between the high-level risks and the activities to be audited. The IAO should review the format and contents of the current internal audit plans and it should align the planned audit activities with the significant risks.

Delegations of authority

20. A consolidated and comprehensive framework setting out the delegations of authority for WHO has not been clearly set out and communicated. This is important to ensure accountability relationships are well understood. In addition, uniform practices for the method and retention of further delegations and temporary delegations are not in place. The Secretariat acknowledges that the delegations of authority require an organisation-wide review and is currently considering alternative approaches to addressing this issue.

WHO Manual

21. The WHO Manual aims to serve as the single unified source of WHO's policies and administrative instructions, yet it has become increasingly outdated over past years. A comprehensive review of the WHO Manual and an improvement in the manner in which such instructions are communicated to staff are urgently required. While the Secretariat has acknowledged this and some work has commenced on revising certain sections, I am concerned that there have been no significant improvements effected to the WHO Manual to date and consider it important to raise this issue again. As mentioned in my final report for 2000-2001, the responsibility for the review of the WHO Manual should be clarified and a timetable agreed to ensure that this matter is addressed.

22. The Secretariat has advised me that they too view this issue as a priority and a new, more structured approach will be taken to delegations of authority and the WHO Manual, which will introduce a clear distinction between delegation of authority and the related operational guidance. It is expected that the introduction of a new comprehensive framework of delegations of authority and related changes to the WHO Manual will be completed by March 2004.

STRATEGIC BUDGETING AND PERFORMANCE MEASUREMENT

23. Since the 2000-2001 financial period, WHO has been moving to a revised strategic budgeting process with the implementation of results-based management. In this regard, the programme budget for 2002-2003 clearly sets out WHO's strategic directions, its organisation-wide priorities and the thirty-five areas of work through which the programme budget will be implemented. It is a challenge for the organisation to operationalise the strategic budget through an integrated planning process, with effective monitoring and performance reporting. The considerable progress made in this regard over the past two financial periods is commended. As part of my continuing review of these important matters, attention was devoted to the issues of strategic budgeting, planning, monitoring and evaluation, with an emphasis on issues relating to resources from other sources. In the paragraphs that follow, matters where further improvements could fruitfully be implemented are highlighted.

Integrated planning for all sources of funds

24. The proposed programme budget is integrated in that it defines a common set of objectives and expected results for WHO, irrespective of the source of funding. The expenditure plan for 2002-2003, as reflected in the budget, provides details of the expenditure plan, broken down between regular budget and other sources of funds. While the breakdown at the organisational level and by regional office was reflected for the regular budget, similar information was not provided for that part of the budget funded by other sources.

25. The proposed programme budget serves as the basis for the detailed operational planning which should also follow an integrated approach. In order to ensure effective operational planning, it is necessary for indicative budget allocations, for both regular and other sources, to be communicated timeously.

26. Regular budget allocations for the 2002-2003 financial period were communicated in November 2001 and there was no formal communication detailing the planning allocation for other sources. The late communication of regular budget allocations and the absence of extrabudgetary estimates have complicated the operational planning process.

27. It is therefore pleasing to note that the proposed programme budget for 2004-2005 sets out, in percentage terms, the breakdown of budgeted expenditure for global, regional and country activities, for both regular budget and other sources. This not only provides for more complete and transparent information for stakeholders, but also provides planning officers at the different levels of WHO with an early indication of the expected resources they can use in following an integrated operational planning approach.

28. WHO should ensure that for 2004-2005, indicative planning figures for all sources of funds are communicated to clusters and regions in a timely manner, to ensure that comprehensive integrated operational planning can take place before the commencement of the biennium.

Allocation of funds from extrabudgetary resources

29. A review of the process of resource allocations at the operational level revealed that the allocations were mainly based on the priorities understood within each cluster and that different methods for determining the allocation were used. It is recognised that the allocation of extrabudgetary funds is a complex issue and the different requirements of donors as well as many organisational aspects need to be considered in this process. It is noted, however, that a more structured and transparent framework for the allocation of extrabudgetary funds would be desirable. This framework should provide for a clear link between the strategic budgetary process and the operational allocation of resources.

Resource mobilisation framework

30. Staff at the cluster level involved in interacting with potential donors to mobilise resources expressed the need for a common resource mobilisation framework, which encompasses practical and basic guidelines and principles to be adhered to in resource mobilisation activities. It is agreed that WHO should develop such a framework to clarify the roles and responsibilities and promote communication between the various role-players to ensure that a common vision is attained in resource mobilisation.

Use of Special Account for Servicing Cost funds

31. The implementation of any extrabudgetary financed programme activity requires technical, administrative and operational support and services. These programme support costs contribute to the expenditures WHO has to incur in order to provide the necessary technical and non-technical support and services to implement technical co-operation programmes. The Special Account for Servicing Costs was established in order to provide for the budgeting and accounting of these funds.

32. The funds earned in each biennium are allocated to the clusters and the regions for use in the next biennium. It was noted that clear criteria for the use of the funds allocated from the Special Account for Servicing Costs had not been elaborated and communicated throughout WHO.

Programme monitoring

33. The purpose of monitoring is to determine the level of progress made toward the delivery of planned products and services. Monitoring is performed on a six-monthly basis while at the end of the first year of the biennium, a mid-term review is performed. The mid-term review examines for each area of work the contribution achieved towards the expected results.

34. A review of technical progress and workplan review reports prepared after the first six months of 2002 revealed that insufficient information was recorded to effectively monitor progress. In this regard, information was not always provided on the status of delivery toward achieving the milestones, reasons for the delays in achieving certain milestones were not recorded and for those milestones that had not been achieved within the target dates, rescheduling was not indicated. Workplan review reports also did not contain comments on the status of delivery of products, whilst information on expected timeframes could also be improved.

35. A review of the mid-term reports revealed similar shortcomings in that targets or baselines had not been elaborated in most instances.

36. Comprehensive and relevant information should be provided in monitoring and reviewing reports to allow for an effective measurement of progress made, which will serve as the basis for corrective action.

Planning for evaluations

37. The purpose of programmatic or thematic evaluations is to measure WHO's contribution to international development efforts, as well as the achievements against stated commitments.

38. In order to coordinate the planned evaluations for the 2002-2003 financial period and ensure that appropriate funding was available, headquarters and each of the regional offices were required to submit proposals for evaluations to be undertaken, including information on proposed terms of reference, the proposed evaluation team, cost estimates as well as the suggested evaluation timetable. Two of the six regional offices did not submit their proposals while in some of the other cases, not all the required information was presented. A timely and complete sharing of information on proposed evaluations will facilitate the process of co-ordinating these efforts to the best advantage of WHO.

TREASURY AND INVESTMENTS

39. I have previously reported on the findings arising from a review of the more significant treasury and cash management functions, which was performed in February 2000. The timing of the initial review was planned to coincide with the Secretariat's planned re-engineering of the treasury function.

40. The current status of this important function was reviewed in early 2003. The treasury operations have improved significantly, a qualified treasurer has been appointed and a greater emphasis is being placed on the investment function, the liaison with and monitoring of fund managers, as well as the in-house management of funds.

41. The implementation of an integrated treasury information system together with changes to the segregation of duties between front and back office finance officers are the only significant aspects that still need to be implemented. The Secretariat has taken steps to address these issues and implementation is expected to be partially completed by the end of 2003.

Actions taken on initial recommendations

42. The actions taken on the salient recommendations arising from the initial review are summarised below:

a) The mandate of the Advisory Investment Committee has been revised.

b) The investment policies for WHO and the Staff Health Insurance Fund have been reviewed and approved by the Director-General.

c) New exposure limits based on independent credit ratings and maximum balances have been established. A monthly risk-management report has been implemented and reporting from fund managers has been improved to include meaningful risk analysis. Standardised reporting for the fund managers is expected to be completed with the appointment of a single global custodian in the near future.

d) A revised staff ethics framework is being developed by Human Resources for the whole of WHO and will be implemented in due course.

e) Performance measures have been implemented both for funds managed by WHO and funds managed by external managers. Benchmarks and targets are set and performance is closely monitored.

f) Cash flow management has been improved through the introduction of new short-term cash management procedures and the use of electronic bank balance reporting to carry out short-term forecasts.

g) The number of bank accounts has been rationalised and the bank account reconciliations were up to date as at December 2002.

Areas for further improvement

43. A comparison of the treasury function with the charter of best practice in treasury management of the International Group of Treasury Associations revealed the following areas for further improvement:

a) The monthly risk-management summary report could be improved to facilitate comparison with the approved investment policy.

b) Whilst the proposed new structure now provides for a more effective segregation of duties, the process needs to be completed.

c) The forecasted cash flows together with management review could be used to assist in identifying reasons for deviations and corresponding corrective action.

d) Limits on the deal size and maturity periods could be established.

e) Within the context of the overall business continuation plan, a business continuation plan for treasury could be established and tested to address any disruption of normal business.

FINANCIAL AND COMPLIANCE MATTERS

44. The interim audit once again confirmed that, in general, the financial records are reliable and well maintained and that adequate internal controls have been implemented by WHO. There are, however, areas where I believe there is scope to further improve the systems and procedures currently in place and these are highlighted in the following paragraphs with a view to providing constructive comments to WHO.

System for the administration of voluntary contributions

45. In the interim report for the 2000-2001 financial period, it was recommended that an integrated information system to record the details of voluntary contributions which can be accessed by the various technical units, management support units, resource mobilisation and financial services be considered. The Secretariat advised that such a system would form part of the new global management system, which would be implemented by 2007.

46. In evaluating the interim systems that had been implemented, it was noted that the management support units and departments have individually developed methods and systems for the monitoring and administration of donor contributions. The Protrack system, which was originally considered would address the interim need, has not proved viable. Due to the importance of the effective and efficient administration of voluntary contributions and the significant amount of time spent on this function, the need for an integrated system is a priority. Since the implementation of the global management system is a longer-term project, it is recommended that the individual efforts of the management support units be consolidated to find a uniform system to meet this need in the interim.

Recording of voluntary contributions

47. In order to facilitate the prompt and correct recording of voluntary contributions, it is necessary for the accounts department to have information on donor agreements and contributions that are expected. While all voluntary contributions had been identified and recorded as at 31 December 2002, it was noted during a review of the donor files maintained

in the accounts department that in many instances the clusters or regional offices had not provided the accounts department with contribution advisory notes and copies of the donor agreements. Without this information, the accounts department has to make additional enquiries resulting in delays in the recording of contributions received. Clusters and regional offices should comply with the existing financial procedures established to streamline the recording of voluntary contributions.

Accounts payable and accounts receivable

48. A number of long outstanding transactions in the headquarters accounts payable and accounts receivable were brought to management's attention at the end of the 2000-2001 financial period. Interim procedures revealed that significant follow-up action had been instituted, with the majority of the transactions identified having been cleared. It was recommended to management that the responsibility and process for the monitoring of these accounts should be clearly defined to ensure that transactions are followed up and cleared in a timely manner. It was further recommended that the remaining transactions that have been outstanding for a long period be investigated and cleared.

Personal accounts

49. The progress in clearing long outstanding transactions in the personal accounts at headquarters was reviewed and it was noted with satisfaction that considerable progress had been made in this regard, as the Secretariat had devoted additional resources to deal with these accounts. The level of personal accounts is, however, still high. It is believed that the task of clearing these accounts will be facilitated through increased co-operation and communication between the persons responsible for the various elements of the personal accounts.

Allotment control and review of unliquidated obligations

50. Instances were noted where obligations incurred exceed the amount available in the allotment. This is contrary to the Financial Regulations and Financial Rules, which state that obligations may be raised only for the purpose indicated on the allotment and may not exceed the amount available in the allotment.

51. As mentioned in my last report, a considerable improvement has been noted in the overall management of unliquidated obligations. An analysis of the savings on regular budget unliquidated obligations processed in the first year of the current biennium confirms that changes in the Financial Regulations together with more specific criteria have resulted in the increased validity of unliquidated obligations brought forward from the previous biennium.

52. It was noted, however, that in certain cases, the responsibility for the review of unliquidated obligations was not well understood. Instances were also noted where the unliquidated obligations no longer appeared to be valid legal liabilities of WHO.

53. Allotment and obligation holders should ensure that they fully comply with the established procedures for the thorough and timely review of allotments and unliquidated obligations.

INFORMATION AND COMMUNICATIONS TECHNOLOGY

54. In my 2000-2001 final audit report, I highlighted certain key organisation-wide strategic issues in respect of information technology (IT) and communication that required the Secretariat's urgent attention. The issues of a comprehensive IT strategy, a well-defined IT governance structure and appropriate staffing of the IT function are being addressed by the Secretariat and the progress made will continue to be monitored.

55. An information systems audit of the general controls surrounding the Administration and Finance Information System and related systems was carried out in the headquarters environment in 1998 and followed up in 1999. The results of the audit were included in my report for the 1998-1999 financial period. During the last biennium, the specialist review work was extended to a regional office. The most significant findings from this review were highlighted in my interim report for the 2000-2001 financial period.

56. The Secretariat has been addressing the issues highlighted in these audits and has regularly informed me of the progress made. In this regard, we have been informed that a strategic plan has been developed to improve the general control environment and network security in a coherent and planned manner that will provide WHO with lasting benefits. Due to the significance of the work being undertaken, which includes migration to a new multi-environment configuration, this process will take time, although it is noted that considerable milestones have already been achieved. All of the recommendations made in the initial reviews have been accepted by the Secretariat and wherever possible, changes have already been introduced to address these, while others will only be completely addressed on the completion of, *inter alia*, the environment project and major computing infrastructure projects to be commenced in 2003.

57. To contribute to this comprehensive exercise, reviews were performed at both headquarters and the region to determine what progress had been made in rectifying previously identified weaknesses within the IT environment and to focus on the corrective steps taken to this effect, in order to highlight any remaining concerns.

58. Furthermore, due to the importance of IT to WHO as a whole, my staff extended their added-value work in this area by performing a detailed audit of the network and security controls at the WHO headquarters.

Progress reviews of the information systems audits of the general control environments at headquarters and at a regional office

59. General controls establish a framework of overall control over the IT activities and provide reasonable assurance that the overall objectives of internal control are achieved. They serve as the foundation for the controls of all application systems and ensure the effective operation of programmed procedures including controls over the design, implementation, security, use and amendment of programs and files. If general controls are inadequate or ineffective, there is a material risk that application controls will be compromised.

60. Overall, the two progress reviews revealed that considerable progress had been made in addressing the previous audit findings. However, as a number of aspects were still in the process of being addressed or formalised, significant weaknesses still existed in the respective control environments as a whole.

General control environment at headquarters

Improvements implemented by the Secretariat

61. The following key actions have been taken by the Secretariat:

a) Aspects of an IT security policy have been drafted for the WHO headquarters and the network policy is being updated.

b) Approved change control procedures have been implemented.

c) An information security officer has been appointed and steps have been taken to address WHO's dependence on short-term staff.

d) Test documentation is now kept and a formal change control committee has been established. Program changes are logged and reviewed by management.

e) Some actions have been taken to improve logical access controls. Various physical security control measures have been implemented to prevent and detect unauthorised access to sensitive computer resources.

Areas for further improvement

62. The Secretariat is in the process of addressing the following remaining issues:

a) IT security and network policies and procedures should be completed and approved.

b) The formal service level agreement between the WHO and the International Computing Centre should be finalised.

c) System, user and program documentation should be brought up to date and maintained.

d) Quality assurance should be included in the program change process.

e) Programmers should not have access to production programs and data. Consideration should be given to implementing library management and change management software.

f) Formal system development life cycle (SDLC) methodologies should be documented and approved.

g) Certain remaining weaknesses relating to logical access controls should be addressed.

h) An authorised and tested disaster recovery plan should be implemented.

General control environment at a regional office

Improvements implemented by the Secretariat

63. The following are significant actions taken to address the weaknesses identified in the initial audit:

a) Elements of a security policy, disaster recovery plan, business continuity plan, information technology strategic plan, program change control procedures, operating procedures and data dictionary development and maintenance policies and procedures have been drafted and related procedures implemented.

b) The SDLC methodologies and standards have been developed and drafted, but have not been formally approved by management.

c) Physical access and environment controls have been improved to ensure that access to the computer room and other related equipment is restricted to authorised personnel only.

d) The reports generated by the network monitoring packages to monitor network performance and faults on the system are presented to management for review.

e) Alternative controls have been implemented to reduce the risk of unauthorised access via the modem.

f) Draft backup and restore procedures and incident reporting procedures now exist but are still to be approved by management. A backup register and operator run books are being maintained. Backup tapes are now being stored in two off-site backup locations. Backups are now periodically restored and tested.

g) Logical access controls have been improved.

h) Regular reviews are now performed to ensure that only legal software is being used. Termination and user registration procedures have been implemented. Anti-virus programs have been installed on all servers.

i) Controls have been implemented to ensure that programmers have read-only access to the production environment. Contracts and terms of reference exist for all IT staff.

j) Test plan standards have been introduced but not formalised. Procedures are being implemented for program changes to be logged and reviewed.

Areas for further improvement

64. The following significant issues, which are currently being addressed by the Secretariat, are noted as areas for further improvement:

a) The various IT policies and procedures drafted should be formally approved and fully implemented.

b) The remaining weaknesses relating to logical access controls should be addressed.

c) Consideration should be given to implementing an archiving policy. The issue of improving the controls to ensure that the data dump created in the region is accurate and complete when headquarters updates the financial system should be pursued. The Secretariat has already indicated that they will be taking steps to address this.

d) Segregation of duties has not been implemented between the critical job functions of the database administrator and the application programmers. Due to the limited staff available, the regional office is not able to segregate these functions. Compensating controls and processes should, however, be implemented to reduce the associated risk. A high level of dependency on some key IT staff members continues to be a concern.

e) Management-level IT steering committee meetings should be formalised.

f) A change control committee should be created and quality assurance should form part of the program change process.

Network and security controls

Scope and approach

65. Information and its supporting processes, systems and networks are essential for the effective functioning of WHO as it becomes more dependent on the availability of its IT resources in all of its areas of work and the integrity of not only financial, but also technical and other management information residing in these resources. With increasing connectivity between WHO's internal and external networks, it is necessary for WHO to ensure that adequate measures have been put in place to reduce the vulnerability to security threats, accidental damage and hardware or software failure.

66. The Secretariat has developed an Information Security and Assurance Plan based upon a risk assessment of the network and desktop security environment at headquarters carried out late in 2001. A strategic approach has been taken to implement a well-architected, secure environment which will require sustained effort and considerable resources over a period of time.

67. Due to the importance of these issues, a specialist information systems audit of the network and security controls at WHO headquarters was performed in October 2002 in accordance with the standards of the Information Systems and Control Association with a view to providing WHO with an evaluation of the current status of its network and security controls.

Focus areas

68. The following aspects of the local area network (LAN) and the wide area network (WAN) were identified as focus areas:

a) Controlled external network penetration testing directed at perimeter security measures, including routers, Internet firewalls, web and mail servers, dial-up connections and other externally accessible devices.

b) Controlled internal network penetration testing directed at critical components within the networks. Key communication devices, security devices and other devices that could be analysed from the internal network to determine the existence of exploitable vulnerabilities.

c) Host security diagnostic reviews that could be performed on a representative sample of key security, application or communication devices on the internal network.

Findings

69. The findings of the audit indicated that although some measures were in place to minimise network security risks, significant security-related weaknesses were present in the network environment as a whole.

70. In this regard, it was noted that the "WHO policy on the acceptable use of information systems" was utilised as the network policy. Although this policy was not comprehensive as a network policy, it was in the process of being updated at the time of the audit. Management had also not yet formally approved it.

71. It was also noted that network security controls at WHO were not optimally utilised and were seriously hampered by considerations of legacy systems and other organisations' systems that were hosted on the WHO network. Access controls between the internal network and Intranet were not optimally utilised to ensure effective network security and access control. Best practices for securing servers were not implemented in certain cases and various servers were running services that were vulnerable to certain exploits due to the software versions of these services that were not updated with the latest patches or releases.

72. The detailed findings and recommendations on how to reduce or eliminate the weaknesses and risks have been set out in a comprehensive report to the Secretariat.

ACKNOWLEDGEMENT

73. I wish to record my appreciation for the co-operation and assistance extended by the Director-General, the Regional Directors and the staff of the World Health Organization during my audit.

S.A. Fakie
External Auditor
Auditor-General of the Republic of South Africa

Pretoria, South Africa
20 March 2003

= = =