Public Health Agency of Canada | Agence de la santé publique du Canada

REVIEW REPORT

INFORMATION TECHNOLOGY SECURITY

Audit Services Division

November 2010

Approved by Chief Public Health Officer
on January 12, 2011

Canada

Table of Contents

Review Objectives and Scope **2**

Background **2**

Review Findings and Recommendations **3**

IT Security Governance.. ..... ……3

Network Operations ……. 5

IT Incident Management …….. ……..6

Conclusion ……...6

Appendix A: Review Criteria…….. 8

Appendix B: Management Action Plan ……..9

Appendix C: Description of Networks Used by PHAC…… 15

Appendix D: List of Acronyms.....17

Cat: HP5-104/2010E-PDF
ISBN: 978-1-100-17536-2

Review Objectives and Scope

1. The overall objective of this review was to inform the Public Health Agency of Canada (PHAC or the Agency) senior management on the extent to which the Agency's Information Technology (IT) Security Infrastructure is consistent with global best practices as outlined in the Control Objectives for Information and Related Technology (COBIT) Security Baseline guide and Treasury Board (TB) Operational Security Standards: Management of Information Technology Security (MITS). A review does not constitute an audit as it provides a lower (moderate) level of assurance than an audit. The review was conducted in accordance with TB Policy on Internal Audit.

2. The IT Security review was part of the Agency's 2010-15 Risk-based Audit Plan. The review was performed between April and November 2010.

3. The scope of the review included an examination of IT governance, network operations and IT incident management. This review did not look at the IT Security measures and safeguards dealing with business continuity planning, security in the system development life cycle environment, and contracting.

4. The review criteria presented in Appendix A were derived from the Information Systems Audit and Control Association COBIT Security Baseline guide and TB MITS standards.

Background

5. PHAC is critically dependent on the availability and soundness of its IT systems and technical infrastructure supporting all four network services (see description of the four networks currently used by PHAC in Appendix C). The management of security is most effective when it is systematically woven into the business, programs and culture of a department. As for all government departments and agencies, PHAC is facing a continuing challenge to maintain an up-to-date IT Security infrastructure to be able to detect new threats and respond quickly to all security incidents.

6. In PHAC, the Chief Information Officer (CIO), the Departmental Security Officer (DSO) and Information Technology Security Coordinator (ITSC) are involved in the management of the IT Security. Information Management and Information Technology (IM/IT) Security Services, a section of the IM/IT Directorate (IMITD), is responsible for the IM/IT Security Program of the Agency. The IM/IT Security Program aims to protect the information assets and the information systems of the Agency.

7. PHAC network perimeter services include numerous external players: Health Canada, Public Works and Government Services Canada (under contract with Health Canada), and third parties. Under a 2005 Memorandum of Understanding (MOU), Health Canada provides PHAC with IM/IT direct services, shared services,

and corporate IM/IT infrastructure.

8. The IMITD budget for the fiscal year 2009-10 was $26 million and as of September 2010, the forecast is $29.7 million for 2010-11. The CIO has indicated that the IT Security budgets for the same periods are respectively $1.3 million and $1.4 million.

Review Findings and Recommendations

IT Security Governance

Criteria: PHAC uses appropriate governance principles to organize and manage its IT security program.

9. The IT Security Policy was approved in 2006 and over time, complementary policies, directives and guidelines have been developed. However the suite of security policies that have been developed is incomplete. The roles and responsibilities of the CIO, ITSC and the DSO are well documented in the IT Security Policy, subject to the comments in the following paragraph. Well-documented standard operating procedures are in place to ensure that employees and contractors are screened or security cleared at the appropriate security level prior to appointment.

10. While the ITSC has been assigned responsibility for IT Security for the whole Agency, in practice, the ITSC has not been empowered to act on this authority in the National Microbiology Laboratory (NML). The Director, Informatics Services, Laboratories and Regions actually oversees IT Security in NML. This fragmentation of responsibility exposes PHAC to the possible risk that security will not be managed consistently and effectively. It also precludes clear accountability for IT Security across the Agency.

11. The IM/IT Management Committee, which is responsible for reviewing and making decisions on IM/IT items of significance and materiality, reports as a sub-Committee to the Executive Committee since July 2010. The CIO presented to this oversight Committee an Information Security Capacity business case addressing the state of IT security at PHAC and outlining priority investments to be made in subsequent years. We did not find regular systematic reporting to this oversight Committee on the state of IT Security. As a result, Senior Management is not well informed on the state of the IT Security program, practices and controls, policy compliance status and IT Security risks.

12. IM/IT has in place an operational plan to support the IM/IT Strategic Plan. However, the operational plan should provide more information to support the IT Security strategy, namely on improving TB Management Accountability Framework ratings and Integrated Security effectiveness.

13. The threat and risk assessments for some systems and applications have not

been completed and documented. Furthermore, the Agency does not have a rigorous and systematic certification and accreditation (C&A) process to ensure that new systems and major applications adhere to formal and established security requirements prior to being implemented in the operating environment. In the absence of a rigorous risk management program, the Agency is not well-informed of risks associated with its information and IT assets. A draft C&A framework document describing a proposed new process is currently being completed.

14. The PHAC-Health Canada MOU/Service Level Agreement (SLA) does not include IT service level indicators. In the absence of service management measures, including appropriate IT service level indicators, the CIO cannot effectively manage the performance of the IT infrastructure services received from Health Canada including security.

15. There is no comprehensive strategy and program in place to explain the importance of IT Security and describe the related PHAC staff responsibilities. A lack of awareness exposes PHAC to risk of security breakdowns. We noted that in July 2010, the Agency hired a new Security Training and Awareness Officer who's first tasks were to define the requirements for a comprehensive security awareness strategy and program. We also noted that individuals with specific IT security duties have received proper security training and follow their individual professional development plans that are updated annually.

Recommendations:

16. The Chief Information Officer should revise the operational plan to support the Information Technology Security strategy, complete a policy suite covering all significant risks, and implement ongoing monitoring processes and report to Senior Management on the state of Information Technology Security.

17. The Chief Information Officer should implement a formal Certification and Accreditation process for new systems and major applications for the Agency.

18. The Departmental Security Officer, in collaboration with the Information Technology Security Coordinator, should:

    a) identify and conduct risk assessments that need to be completed; and

    b) support the efforts of the Security Training and Awareness Officer to develop an Agency-wide comprehensive strategy and program to maintain employee awareness of security issues at an appropriate level.

19. The Assistant Deputy Minister, Emergency Management and Corporate Affairs should seek amendments to the Memorandum of Understanding and Service Level Agreement with Health Canada with respect to Information Technology security so that PHAC can assure itself that it is receiving the level of service it requires. The amendment should encompass the inclusion of service level indicators to establish the quality of services, costs, performance level expected, and timeframes required. Amendments should also include annual assurance

from Health Canada on the extent to which Health Canada is delivering on its service commitments to PHAC for Information Technology Security.

Network Operations

Criteria: Computer networks used by PHAC are protected by adequate controls, security measures and safeguards.

20. The process to obtain a network account is working well. However, there is no coordinated process across all networks to inform IM/IT of the departure of staff or contractors. Risks exist that user-id and access rights will remain active even when employees or contractors have left the Agency or occupied new responsibilities due to a change of responsibility.

21. There are not uniform and documented standards and guidelines by which Agency systems, servers and desktops are monitored in regard to authorizing access and controlling information flows. We observed that the Agency generally had sound password management practices in place.

22. The Agency has a change management process to manage security patches. However, the configuration management system is not robust, reducing the effectiveness of control over IT assets.

23. When external parties are granted access to PHAC's information, it is essential that they understand, and commit to, their responsibilities to protect the information. Typically, this is accomplished by means of documented security clauses in MOUs or SLAs. We found that responsibility for security over such information is dispersed throughout the organization. By distributing such responsibility throughout the organization, PHAC has incurred the risk that different standards may be applied in different parts of PHAC and that some of the standards may not be sufficiently robust.

24. Processes governing the physical security measures are generally mature as respective responsible parties are involved and physical security measures provide adequate safeguards.

25. Backup of data files are taken on a systematic basis, however only monthly backup files are stored at off-site location. If a physical incident occurs and destroys or renders the on-site backup tapes unusable, PHAC is exposed to risk of data loss and users could be exposed to a lengthy process to recover lost data.

Recommendations:

26. The Departmental Security Officer, in collaboration with the Director General, Human Resources should strengthen the current process to manage user access to ensure that Information Management and Information Technology Operations cancel all non required access to PHAC networks for departures of employees and contractors, and for employees movements, on a timely basis.

27. The Chief Information Officer should:

    a) establish guidelines and standards by which all Agency systems, servers and desktops are routinely monitored to authorize access and control information flows from and to networks;

    b) complete the Agency-wide Information Technology configuration management processes to manage and control significant configuration items in place; and

    c) review the storage practices of electronic data backup media and develop a plan to reduce the risk of data loss as a result of a disaster to one of the server rooms.

28. The Departmental Security Officer, in collaboration with the Chief Information Officer, should put in place a rigorous process to support the development of sufficiently robust Memorandum of Understanding or Service Level Agreements to protect information to which external parties are granted access throughout PHAC, and monitor compliance with these Agreements.

IT Incident Management

Criteria: Measures are in place to manage IT incidents from their discovery to the implementation of appropriate responses.

29. To detect IT incidents, both Health Canada and PHAC use a variety of tools and techniques. We noted that PHAC has not taken advantage of some of the detection systems and software throughout the Agency. Risks of not detecting IT incidents are therefore increased.

30. The Security Event Notification Database system, which is the system currently used to report all security incidents, appears not to be used extensively. As a result, effectiveness of the IT Incident management is reduced.

Recommendation:

31. The Departmental Security Officer, in collaboration with the Chief Information Officer, should make a decision on the future use and change required to the Security Event Notification Database system.

Conclusion

32. While efforts have been made to introduce and operate IM/IT security processes, practices and controls that meet government standards, PHAC IT security infrastructure needs to be strengthened to achieve compliance with MITS standards and make use of COBIT best practices. The IT Security operational plan and policy framework, risk management, monitoring and awareness, certification and accreditation of new systems and major applications are the most notable areas that need management's attention.

33. Implementing the recommendations outlined in this report will contribute in enhancing the Agency's IT Security program and mitigating the security risks to the extent possible.

Statement of Assurance

34. In my professional judgment as A/Chief Audit Executive, sufficient and appropriate review procedures have been conducted and evidence gathered to support the accuracy of the review conclusion provided and contained in this report. The review conclusion is based on a comparison of the conditions, as they existed at the time, against pre-established review criteria (see Appendix A) within the scope described herein. Further, the evidence was gathered in accordance with the Internal Auditing Standards for the Government of Canada.

Daniel Surprenant, B. Comm., CA
A/Chief Audit Executive

Management Response

35. The Agency's management agrees with our findings and recommendations and a management action plan is presented in Appendix B.

Acknowledgments

36. We wish to express our appreciation for the cooperation and assistance afforded to the review team by management and staff during the course of this review.

Appendix A: Review Criteria

IT Security Governance
PHAC uses appropriate governance principles to organize and manage its IT Security program.

Network Operations
Computer networks used by PHAC are protected by adequate controls, security measures and safeguards.

IT Incident Management
Measures are in place to manage IT incidents from their discovery to the implementation of appropriate responses.

Appendix B: Management Action Plan

Recommendation	Management Action Plan	Officer of Prime Interest	Target Date
IT Security Governance			
16. The Chief Information Officer should revise the operational plan to support the Information Technology Security strategy, complete a policy suite covering all significant risks, and implement ongoing monitoring processes and report to Senior Management on the state of Information Technology Security.	Agree.		
	i) The IT Security strategy outlined in the IMITD 2010-2013 Strategic Plan has recently been endorsed by the IM/ITMC. The CIO will revise and incorporate the MITS compliance action plan into a comprehensive operational plan to support the IT Security strategy, and will obtain endorsement from IM/ITMC. The operational plan will detail various initiatives including level of effort, costs and timelines, and outline necessary resource investments to address issues related to IT Security such as MITS compliance and integrated security effectiveness. Implementation of the various components of the IT Security strategy and operational plan is contingent on EC endorsement and resourcing to sustain activities.	CIO	March 2011 Start Imple-mentation April 2011
	ii) The Office of the CIO will develop an IT Security policy suite to address priority risk issues, security incidents, detection systems and investigative processes.	CIO	March 2011
	iii) Steps have been taken to improve the	CIO	March 2011

Recommendation	Management Action Plan	Officer of Prime Interest	Target Date
	overall security posture reporting process (e.g. monthly metrics). Additional attention will be placed on policy and procedural consistency as a result of this recommendation. Monitoring control is evolving and additional funding received in July 2010 has been allocated to improve monitoring capacity in both the National Capital Region and NML. Capacity monitoring improvements with IMITD will compliment proactive response initiatives of DSO.		
17. The Chief Information Officer should implement a formal Certification and Accreditation process for new systems and major applications for the Agency.	Agree. The CIO will obtain approval of the formal C&A process from the IM/ITMC.	CIO	March 2011
18. The Departmental Security Officer, in collaboration with the Information Technology Security Coordinator, should:			
a) identify and conduct risk assessments that need to be completed; and	Agree. The DSO, in collaboration with the IT Security Coordinator and the appropriate Program Managers, will produce an integrated plan to identify the risk assessments of key infrastructure required, their priority, the estimated resources required, and a schedule for their completion.	DSO	March 2011
b) support the efforts of the Security Training and Awareness Officer to develop an Agency-	Agree. The DSO in collaboration with the IT Security Coordinator will support the efforts of	DSO	March 2011

Recommendation	Management Action Plan	Officer of Prime Interest	Target Date
wide comprehensive strategy and program to maintain employee awareness of security issues at an appropriate level.	the Security Training and Awareness Officer to develop and implement an Agency-wide program to provide mandatory training to all employees.		
19. The Assistant Deputy Minister, Emergency Management and Corporate Affairs should seek amendments to the Memorandum of Understanding and Service Level Agreement with Health Canada with respect to Information Technology security so that PHAC can assure itself that it is receiving the level of service it requires. The amendment should encompass the inclusion of service level indicators to establish the quality of services, costs, performance level expected, and timeframes required. Amendments should also include annual assurance from Health Canada on the extent to which Health Canada is delivering on its service commitments to PHAC for Information Technology Security.	Agree. The ADM, EMCA will obtain amendments to the MOU between PHAC and Health Canada to include IT security service level indicators and annual assurance as recommended.	ADM, EMCA	March 2011

Recommendation	Management Action Plan	Officer of Prime Interest	Target Date
Network Operations			
26. The Departmental Security Officer, in collaboration with the Director General, Human Resources should strengthen the current process to manage user access to ensure that Information Management and Information Technology Operations cancel all non required access to PHAC networks for departures of employees and contractors, and for employees movements, on a timely basis.	Agree. i) The DSO will strengthen and implement required changes to the process of modifying user access, and provide appropriate training. ii) IM/IT Operations will strengthen and implement required changes to the process of modifying user access, on a timely basis	DSO CIO	March 2011 March 2011
27. The Chief Information Officer should: a) establish guidelines and standards by which all Agency systems, servers and desktops are routinely monitored to authorize access and control information flows from and to networks;	Agree. Current processes for monitoring desktops, servers and systems under the control of the CIO are monitored using industry accepted Incident Detection/Incident Response tools and techniques, are systematically assessed and improved on an ongoing basis. For the monitoring of computing devices operated by clients or those which reside on the network of service providers (e.g. Health Canada or Public Works and Government Services Canada), Services Agreements and enhanced perimeter security and IDS/IPS tools will be developed and used to ensure	CIO	Starting April 2011

Recommendation	Management Action Plan	Officer of Prime Interest	Target Date
	appropriate monitoring and control.		
b) complete the Agency-wide Information Technology configuration management processes to manage and control significant configuration items in place; and	Agree. The CIO will design and implement a comprehensive program for the management of system integrity and security configuration for all PHAC network attached devices.	CIO	March 2011 Start Imple-mentation June 2011
c) review the storage practices of electronic data backup media and develop a plan to reduce the risk of data loss as a result of a disaster to one of the server rooms.	Agree. The CIO will conduct a review of data storage, retrieval, archiving and recovery practices within the Agency.	CIO	Starting April 2011
28. The Departmental Security Officer, in collaboration with the Chief Information Officer, should put in place a rigorous process to support the development of sufficiently robust Memorandum of Understanding or Service Level Agreements to protect information to which external parties are granted access throughout PHAC, and monitor compliance with these Agreements.	Agree. i) The DSO, in collaboration with the CIO will produce mandatory security service requirements to protect information to which external parties are granted access throughout PHAC. Statements will be provided to the Asset and Materiel Management Division for inclusion in PHAC contracts; and	DSO	June 2011
	ii) The DSO will undertake to implement a process that will make it mandatory for all Program Managers to have all agreements including MOU's and SLA's uploaded to existing Materiel Management systems. The DSO will obtain the list of agreements, review annually and confirm with business owners the relevance and compliance of these	DSO	November 2011

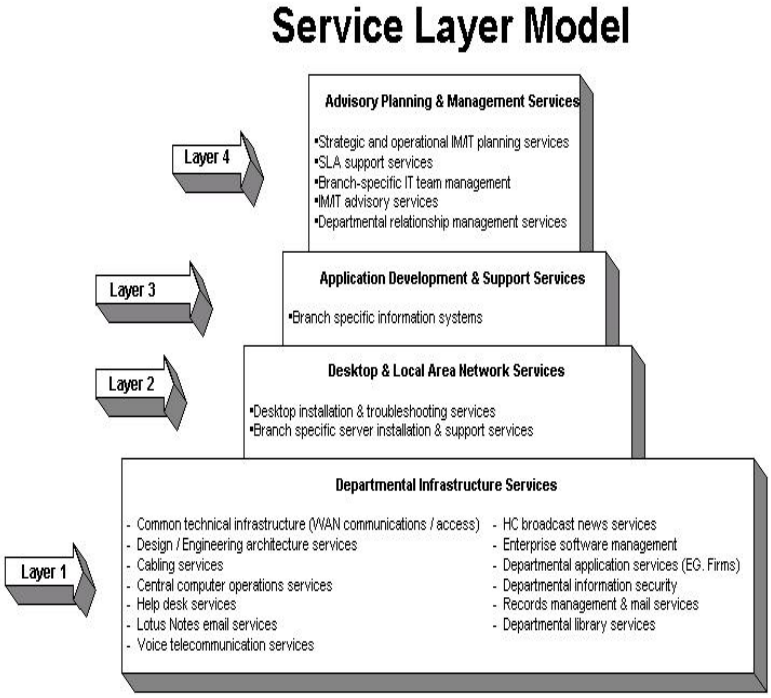
Recommendation	Management Action Plan	Officer of Prime Interest	Target Date
	agreements with respect to an integrated security methodology.		
IT Incident Management 31. The Departmental Security Officer, in collaboration with the Chief Information Officer, should make a decision on the future use and change required to the Security Event Notification Database system.	Agree. The DSO, in collaboration with the IT Security Coordinator will support the conduct of a TRA and privacy impact assessment of the SEND data base with a view to assessing the feasibility of adopting the SEND database for wider use, and adequate training on its use will be provided.	DSO	March 2011

Appendix C: Description of Networks Used by PHAC [1]

Currently, the Agency uses four networks: HC NET, PHAC NET, Science NET and Bioinformatics NET.

HC NET - Since its creation, PHAC has been faced with managing the security of its electronic information mainly stored on the HC NET managed by Health Canada. An existing Memorandum of Understanding and Service Level Agreement have been ratified between PHAC and Health Canada concerning the network support services provided by Health Canada.

The Service Agreement specifies that service delivery is to be shared between Health Canada and PHAC. Generally, the Health Canada CIO/IMSD provides provide Layer 1, 3 and 4 Services to PHAC while PHAC CIO delivers Layer 2 and 3 services to PHAC users.



The network infrastructure used by PHAC is under Health Canada authority. The functional authority for the HC NET is the Health Canada, CIO as long as PHAC and Health Canada operate within a shared technical infrastructure which is not separate (either physically or logically).

Within PHAC, all employees and contractors are connected to the HC NET and receive the services specified in Layer 1 above such as access to the network infrastructure, e-

[1] Information on the HC NET was obtained from the Health Canada / PHAC MOU & SLA. Information on other networks was provided by the IMITD.

mail, network security protection measures, and internet, national service desk, server and operating systems and user account management.

PHAC NET – PHAC IM/IT initiated three years ago the development of its PHAC NET. PHAC NET is not yet fully operational. This network will be an autonomous (managed by PHAC) segregated network (connected to HC NET), created to meet the unique needs of the Agency:

- to address low risk tolerance with respect to service continuity;
- to facilitate the Agency's mandate as a first responder in national Health Emergency situations; and
- to provide international collaborative hosting environment for data sharing with external health partners.

Science NET – The NML created its own sub network to facilitate the sharing of health research and laboratory results data between scientists working for the NML and other Federal and Provincial / Territory laboratories. The network was conceived and architected to provide scientists and NML employees with a high speed, high storage capacity computer network used by the scientific community to collect and exchange information and construct database of information to be used by the PHAC and external scientific community.

Bioinformatics NET – The NML created a centralized platform for biological research requiring high performance computing, and advanced scientific computing resources and expertise. The principal users on this system are the members of the NML bioinformatics core facility, external PHAC scientists, and invited collaborators. The Bioinformatics NET exists for the purpose of improving public health by advancing scientific knowledge, developing advanced diagnostics and therapeutics, and facilitating public health surveillance programs. The Bioinformatics NET provides processed database of information to all labs within NML.

Appendix D: List of Acronyms

ADM	Assistant Deputy Minister
Agency	Public Health Agency of Canada
C&A	Certification and Accreditation
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
DG	Director General
DSO	Departmental Security Officer
HR	Human Resources
IM/IT	Information Management/Information Technology
IM/ITMC	Information Management/Information Technology Management Committee
IMITD	Information Management/Information Technology Directorate
IMSD	Health Canada Information Management Services Directorate
IT	Information Technology
ITSC	Information Technology Security Coordinator
MITS	Management of Information Technology Security
MOU	Memorandum of Understanding
NML	National Microbiology Laboratory
PHAC	Public Health Agency of Canada
SANS	Servers and Storage Areas
SEND	Security Event Notification Database
SLA	Service Level Agreement
TB	Treasury Board
TRA	Threat and Risk Assessment