NRC·CNRC

From Discovery
to Innovation...

Science
at work for
Canada

National Research Council Canada

Audit of Management of Information Technology (IT) Security

Internal Audit, NRC

June 2007

National Research
Council Canada

Conseil national
de recherches Canada

Canada

TABLE OF CONTENTS

1.0 Executive Summary

Background

The Treasury Board Secretariat (TBS) requires departments and agencies to carry out periodic internal audits to assess their compliance with the Government Security Policy (GSP) and the effectiveness of its implementation. The policy requires departments to actively monitor and carry out internal audits of their security program.

The Management of Information Technology Security Standard (MITS) defines the baseline security requirements that federal departments must fulfil to ensure that the information and information technology assets (e.g., software and hardware) which they control are secure. This operational security standard supplements the Government Security Policy. MITS indicates, among other things, that:

- departments must establish and manage a departmental security program; and
- departmental corporate risk profile will determine the implementation of baseline security measures to meet MITS requirements.

The last review of IT security at NRC was conducted in 1999. Subsequently, NRC's 2006-2007 to 2008-2009 Risk-Based Internal Audit Plan identified the audit of the management of IT security as a priority.

NRC's approach to the management of IT security involves creating a "technically open IT environment to facilitate research and innovation". At the same time, this environment must provide for safeguarding sensitive information and the information that NRC holds in trust for its clients and collaborators.

Audit objectives, scope and methodology

The objectives of this audit of IT security management were:

- To assess NRC’s compliance with the MITS Standard;
- To assess NRC’s adherence to its own IT security policies and standards;
- To determine the effectiveness, economy and efficiency of NRC’s IT security services; and
- To follow-up on observations and recommendations from the 1999 external IT Security Review.

NRC engaged a team of professionally-recognized and accredited IT specialists to carry out the audit work. The audit criteria were based on the requirements of MITS and those of NRC’s internal security policies and standards.

The scope of this audit included the IT security services that Information Management Services Branch (IMSB) provides for critical service components and the 12 institutes/branches and programs (I/B/Ps) and the Executive Offices that IMSB directly supports as well as three Institutes that IMSB does not provide IT security support services. The audit scope did not include computer equipment that is used only for research purposes in NRC Institutes. Audit findings are based on evidence gathered between July 2006 and April 2007.

Audit Opinion and Statement of Assurance

The audit was not able to assess NRC's overall exposure to risks related to IT security and subsequently, we are unable to conclude with reasonable assurance that IT security for NRC as a whole is compliant with the Government Security Policy (GSP) or the government Management of Information Technology Security Standard (MITS). This is due primarily to the fact that NRC has not formally identified and documented all of its enterprise-wide or business critical systems. This coupled with the fact that NRC's Information Management Services Branch (IMSB) neither provides IT security services to all institutes, branches and programs, nor does it have functional authority to monitor or enforce compliance, its high compliance rate of 97% cannot be inferred to NRC as a whole. If subsequent verifiable analysis demonstrates that there are no business-critical systems outside of IMSB's control, assurance could be provided that NRC as a whole is compliant with the GSP and MITS.

It's important to understand that MITS compliance rates while indicative of the probability of secured IT systems, they are not conclusive. In other words, high MITS compliance rates do not necessarily mean a high level of IT security and lower compliance rates do not necessarily mean unsecured IT systems. This can only be verified by a comprehensive IT security audit.

For the same reasons above, we are unable to conclude with reasonable assurance that NRC as a whole is compliant with its own IT security policies, standards and guidelines. We found that the recommendations made in the 1999 external Review of IT Security have for the most part been implemented. Finally, we found that there are opportunities for increased effectiveness, efficiency and economy in the management of IT security at NRC.

In my professional opinion as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, to the audit criteria. The evidence was gathered in accordance with Treasury Board policy, directives and standards on internal audit, and the procedures used to meet the professional standards of the Institute of Internal Auditors.

Conclusion and recommendations

The degree of compliance with MITS varied among IMSB and the three Institutes that we looked at. Overall, IMSB is compliant with MITS at 97 percent. However, the three Institutes were less compliant at 86 percent, 76 percent and 76 percent in key areas of risk management. All areas of non-compliance are related to undertaking sensitivity analyses of all systems, completing threat and risk assessments for all business critical systems and the certification and accreditation of these systems as well as business continuity and disaster recovery planning. It's important to understand that MITS compliance rates while indicative of the probability of secured IT systems, they are not conclusive. In other words, high MITS compliance rates do not necessarily mean a high level of IT security and lower compliance rates do not necessarily mean unsecured IT systems. This can only be verified by a comprehensive IT security audit.

It is important to note that it is not possible for the audit team to conclude on whether NRC as a whole is compliant with MITS. This is due to the fact that NRC has not clearly defined and formally documented all its business critical systems – the foundation upon which NRC's governance model for IT security is based.

In our view, the following gaps in compliance represent areas of risk for NRC:

- Organization-wide monitoring and oversight of IT security are lacking. We found that NRC's IT Security Coordinator for MITS does not have the authority needed to carry out the role as principal contact for IT security matters. Therefore the Coordinator cannot assure senior management that all IT systems at NRC incorporate adequate and appropriate safeguards.
- Risk management with respect to IT security is inconsistent across the organization. As a result, the NRC does not have a clear picture of either its exposure to IT security risks, or whether its IT systems provide the level of security that is commensurate with the sensitivity of the information they contain.
- The wide range of technologies and protocols for enabling NRC employees working off-site to access NRC's IT systems poses a continuing risk for the organization.

We found varying levels of compliance with NRC's policies and standards governing IT security. IMSB was compliant overall. However, for two of the three Institutes that we looked at, compliance levels were substantially lower at 58%.

We have concluded that opportunities exist to improve the economy, efficiency and effectiveness of the management of NRC's IT security services. These opportunities exist with respect to monitoring and oversight, risk management, asset management, storage, remote access, anti-virus protection and change management.

NRC has responded to almost all of the recommendations in the 1999 External Review of IT Security. Of most concern, is the continuing lack of an organization-wide business continuity plan.

Key recommendations

1. To institute better monitoring and oversight of IT, NRC's senior management should designate an IT Security Coordinator for NRC who has responsibility and authority for IT security throughout the organization.
2. To strengthen risk management for IT security, NRC should:

   (a) define what is meant by "enterprise-wide" and "business critical" for IT systems;

   (b) specify the sensitivity of all its IT systems including systems used only for research purposes and document the rationale or criteria for designating them as enterprise-wide and/or business-critical ; and

   (c) carry out other specific risk-management work such as sufficiently robust threat and risk assessments and certification and accreditation on all business critical systems, as required by NRC Policies and MITS.
3. NRC should develop an organization-wide business-continuity plan for IT security.
4. NRC should develop a remote-access policy with the goal of eliminating the use of insecure protocols, reducing the range of protocols in use, and strengthening the security of remote access for tele-workers.
5. Management should examine the potential costs, benefits and feasibility of

centralizing the asset management, storage, remote access, anti-virus and change-management services that the Institutes currently provide.

J. Hinchliff-Milne

Jayne Hinchliff-Milne, CMA, Chief Audit Executive

NRC Audit Team Members[1]:

Irina Nikolova, CA, CIA, CISA

Overall Management Response:

This audit has served to underscore a number of areas where NRC's management practices with respect to IT security need to be clarified and formalized across the organization. But notwithstanding the audit recommendations, which will be addressed in the coming months, NRC continues to manage an effective Council-wide protection program designed to safeguard its information and valuable IT assets. The program's four core components include: a suite of current policies and standards that represent executive management's direction regarding IT security; a flexible organizational structure comprising NRC-IMSB's Information Protection Centre and a network of IBP-level Information Systems Security Officers, designed to meet the challenges that NRC's distributed environment poses for IT security; several well-established IT security processes that address risk management, incident response, IT staff training and user awareness; and, a technical security architecture aimed at better protecting NRC systems and information while enabling the Council's core business. These components exist today and are fundamental to NRC's information protection strategy. Addressing this audit's recommendations will allow NRC to fine-tune an already effective strategy and fully leverage its IT security investment.

[1] The NRC Audit team was supplemented by a team of professionally recognized and accredited IT specialists to carry out the audit work.

2.0 Introduction

2.1 Background and context

The Treasury Board Secretariat (TBS) requires departments and agencies to carry out periodic internal audits to assess their compliance with the Government Security Policy (GSP) and the effectiveness of its implementation. The policy came into effect in February 2002 and prescribes the application of safeguards for employees and assets in departments and agencies. The purpose of these safeguards is to support the delivery of services and the achievement of the government's business objectives. More specifically, the GSP requires departments to actively monitor and carry out internal audits of their security program.

The Management of Information Technology Security Standard (MITS) defines the baseline security requirements that federal departments must fulfil to ensure that the information and information technology assets (e.g., software and hardware) which they control are secure. This operational security standard supplements the Government Security Policy. It also supports the Policy on the Management of Government Information and the National Security Policy.

MITS indicates, among other things, that:

- departments must establish and manage a departmental security program; and
- departmental corporate risk profiles will determine the implementation of baseline security measures to meet MITS requirements.

In 2005, the Auditor General of Canada carried out a government-wide audit of Information Technology (IT) Security. Subsequently, the Treasury Board Secretariat asked government departments, including NRC, to complete an action plan for dealing with the Auditor General's key recommendations from the audit. TBS also asked departments to prepare a status report on their progress in complying fully with MITS and GSP. These reports were to be completed by January 2007.

An internal audit of NRC's security function had been carried out in 2001. However, the audit did not cover IT security, as required by the GSP, because a consulting firm had done an NRC-wide, comprehensive review of this area in 1999. Since then, Internal Audit has done minimal work in IT security to give NRC time to complete the initiatives which had been undertaken in response to the recommendations of the external review. Subsequently, NRC's 2006-2007 to 2008-2009 Risk-Based Internal Audit Plan identified the audit of the management of IT security as a priority.

2.2 Management of IT security at NRC

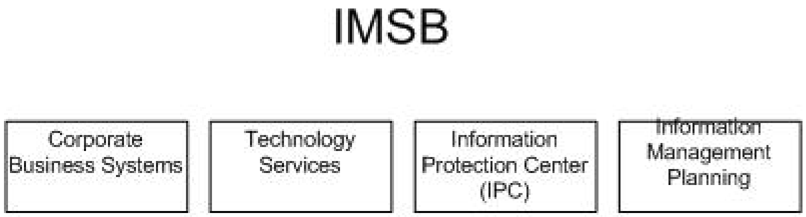
NRC's approach to the management of IT security involves creating a "technically open IT environment to facilitate research and innovation". At the same time, this environment must provide for safeguarding sensitive information and the information that NRC holds in trust for its clients and collaborators.

NRC's centralized/decentralized model for IT

To maintain an open IT environment while ensuring that it properly safeguards its information and systems, NRC has instituted a flexible organizational structure for managing IT and IT security. This management framework was developed in response to the 1999 external IT Security Review and features both centralized and de-centralized or "dispersed" components.

The centralized components: The Information Management Services Branch (IMSB) provides organization-wide IT services and is responsible for major elements of NRC's IT infrastructure. Exhibit 1 presents a simplified schematic of IMSB's four functions which affect IT security services: Corporate Business Systems Directorate; Technology Services; the Information Protection Centre; and Information Management Planning.

Exhibit 1: Information Management Services Branch


IMSB
Corporate Business Systems
Technology Services
Information Protection Center (IPC)
Information Management Planning

Corporate Business Systems Directorate is responsible for developing, operating, managing and supporting corporate-wide business systems, and maintaining master data. Corporate-wide business systems include data and voice communications, web applications, and “Sigma”, a SAP-based system which supports key functions such as accounting, budgeting, human resource management, and procurement.

IMSB’s Technology Services has a dual function. It provides key parts of NRC’s IT infrastructure across Canada. It also provides IT support services to Institutes, Branches and Programs in the National Capital Region that have chosen not to provide these services internally.

The Information Protection Centre (IPC) is a unit within IMSB that works to ensure that NRC takes appropriate measures to safeguard its information holdings and information technology assets from IT security threats. IPC takes a lead role, through widespread consultation, in developing IT security policies, standards and procedures. It is NRC’s single point of contact for reporting security-related incidents. The Centre’s key services aimed at protecting information include:

- monitoring NRC’s wide-area network to detect intrusions;
- responding to and investigating security incidents;
- carrying out threat and risk assessments;
- computer forensics; and
- IT security awareness and training.

Finally, Information Management (IM) Planning supports and participates in committees that constitute NRC's IM/IT governance.

The decentralized components: Responsibility for IT security at the institute, branch and program (I/B/P) levels is ultimately delegated to the respective Directors General. Exhibit 2 provides an organization chart of NRC depicting which I/B/Ps obtain their services through IMSB and those which have chosen to provide their own IT security services internally. IMSB provides complete support services to 12 I/B/Ps and the Executive Offices. Only limited services are provided to some of the other Institutes, e.g., IMSB provides only virus protection services to five I/B/Ps .

All I/B/Ps have an Information Systems Security Officer (ISSO). The ISSO reports to the Institute or Branch Director General on security matters and assists system managers and their staff in developing the security functions necessary for managing the information systems in their locales on a day-to-day basis. The ISSO is also responsible for monitoring compliance with IT security policies at the I/B/P level.

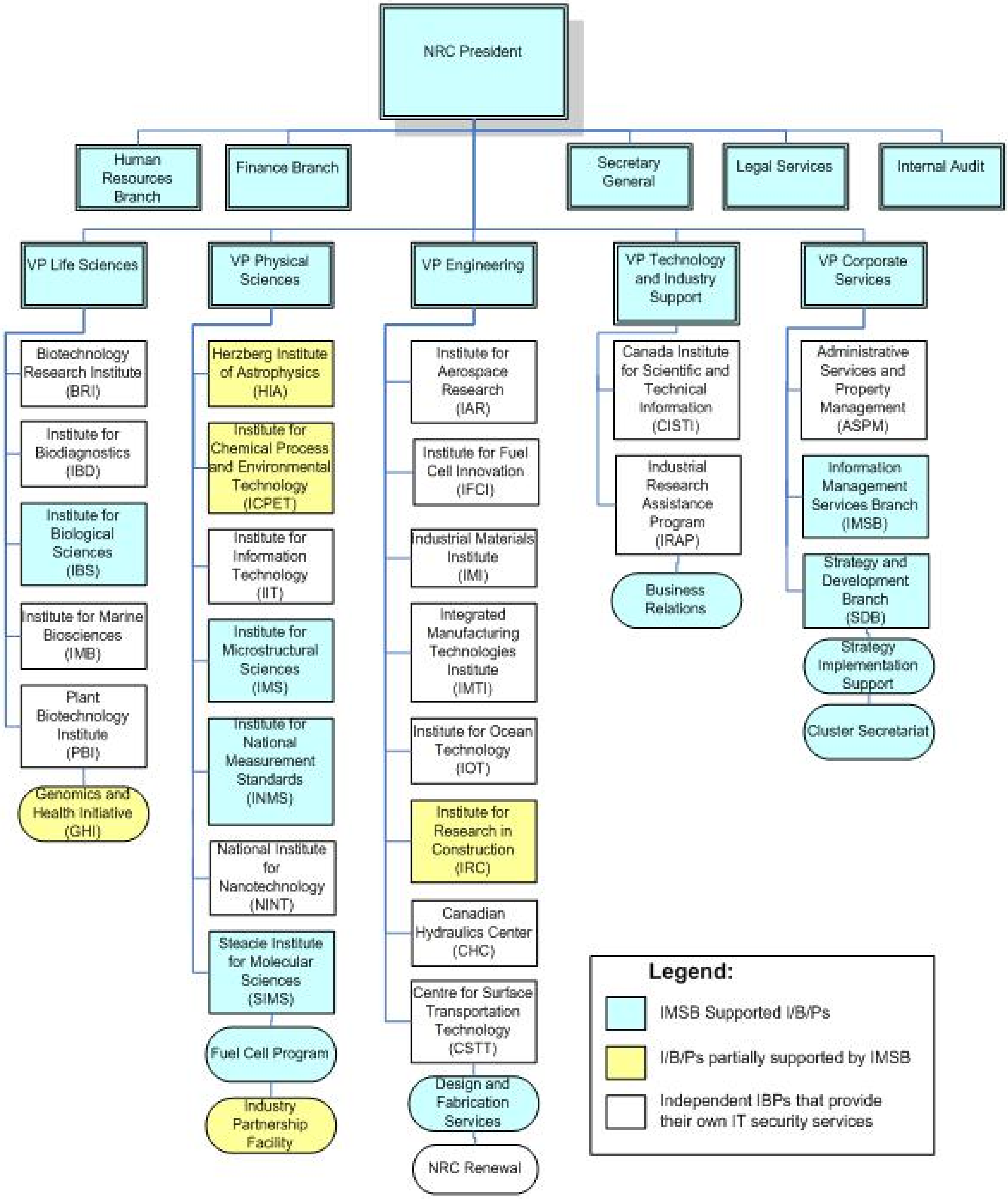
An "ISSO Forum" — a consensus-based group — provides input in developing NRC's security policies and guidelines. The forum is chaired by NRC's IT Security Coordinator, however, the Coordinator has no functional authority for IT security outside of IMSB. This "virtual" forum communicates electronically with other members to discuss and resolve on a consensus basis specific issues as they arise. Formal minutes of meetings are not kept.

Three additional components complete the management framework for IT security at NRC: the Senior Executive Committee; the Chief Information Officer (formerly provided by the NRC Information Council); and the IM/IT Advisory Committee (IAC). The Senior Executive composed of NRC's President, Vice-presidents and Directors General for Human Resources and Finance, are responsible for providing executive-level support and approval for NRC's IT security policy.

The NRC Information Committee was disbanded in March 2007 upon the completion of its mandate to create the current comprehensive Information Management / Information

Technology suite of policies and standards. In its place, the Vice-President of Corporate Services serves as the Chief Information Officer (CIO) for NRC in accordance with MITS requirements. The IM/IT Advisory Committee (IAC) develops recommendations for the adoption of IT security policies, standards and guidelines, which are approved by either the Vice President Corporate Services or Senior Executive Committee. Meetings to discuss IT security occur on an as needed basis for these two functions (CIO and IAC) which have corporate governance responsibilities in addition to IT security.

Exhibit 2: NRC Organizational Structure for IT Security Services


NRC President
Human Resources Branch
Finance Branch
Secretary General
Legal Services
Internal Audit
VP Life Sciences
VP Physical Sciences
VP Engineering
VP Technology and Industry Support
VP Corporate Services
Biotechnology Research Institute (BRI)
Institute for Biodiagnostics (IBD)
Institute for Biological Sciences (IBS)
Institute for Marine Biosciences (IMB)
Plant Biotechnology Institute (PBI)
Genomics and Health Initiative (GHI)
Herzberg Institute of Astrophysics (HIA)
Institute for Chemical Process and Environmental Technology (ICPET)
Institute for Information Technology (IIT)
Institute for Microstructural Sciences (IMS)
Institute for National Measurement Standards (INMS)
National Institute for Nanotechnology (NINT)
Steacie Institute for Molecular Sciences (SIMS)
Fuel Cell Program
Industry Partnership Facility
Institute for Aerospace Research (IAR)
Institute for Fuel Cell Innovation (IFCI)
Industrial Materials Institute (IMI)
Integrated Manufacturing Technologies Institute (IMTI)
Institute for Ocean Technology (IOT)
Institute for Research in Construction (IRC)
Canadian Hydraulics Center (CHC)
Centre for Surface Transportation Technology (CSTT)
Design and Fabrication Services
NRC Renewal
Canada Institute for Scientific and Technical Information (CISTI)
Industrial Research Assistance Program (IRAP)
Business Relations
Administrative Services and Property Management (ASPM)
Information Management Services Branch (IMSB)
Strategy and Development Branch (SDB)
Strategy Implementation Support
Cluster Secretariat
Legend:
IMSB Supported I/B/Ps
I/B/Ps partially supported by IMSB
Independent IBPs that provide their own IT security services

2.3 About the audit

Objectives

The objectives of this audit of IT security management were:

- To assess NRC's compliance with the MITS Standard;
- To assess NRC's adherence to its own security policies and standards;
- To determine the effectiveness, economy and efficiency of NRC's IT security services; and
- To follow-up on observations and recommendations from the 1999 external IT Security Review.

Scope

The scope of this audit included the IT security services that IMSB provides for critical service components. The scope also included the 12 institutes/branches and programs and Executive Offices that IMSB directly supports. In addition we looked at IT security management in three Institutes that IMSB does not provide IT security support services: a medium-size Institute with a number of locations across Canada; a larger Institute that is highly representative of NRC as a whole, and which does some sensitive work; and a very large Institute with offices across Canada. The audit scope did not include computer equipment that is used only for research purposes in NRC Institutes.

The audit team gathered evidence between July 2006 and April 2007.

Approach and methodology

NRC engaged a team of professionally-recognized and accredited IT specialists to carry out the audit work. The audit criteria were based on the requirements of MITS and those of NRC's internal security policies and standards.

To date, TBS has not provided an assessment tool for measuring the extent to which departments are complying with the 144 detailed MITS requirements. Nor has TBS indicated what minimum level of compliance departments must achieve before they can be considered as being "MITS-compliant". In the absence of such guidance, the audit team chose to group the detailed MITS criteria into 29 audit criteria for assessing control practices. These were derived from the four areas of IT security that MITS covers:

- Departmental IT Security Organization and Management,
- IT Security Resources for Projects,
- Management Controls, and
- Technical and Operational Safeguards.

Exhibit 3, below, provides more detail on each area. The IT audit team used professional judgement in developing the 29 control objectives for assessing the level of NRC's compliance with MITS. These criteria were shared and discussed with IMSB and the three institutes scoped in for audit as part of the planning phase of the audit and included in the terms of reference. A complete listing of the 29 audit criteria employed to assess MITS compliance can be found in Appendix A.

We assessed the extent to which NRC complies with its own IT security policies and standards against 19 criteria derived from NRC's IT security policies. A complete listing of the detailed audit criteria used for the audit assessment against NRC security policies can be found in Appendix B.

In assessing compliance with MITS and NRC's standards (Objectives One and Two), we interviewed IMSB and Institute staff and reviewed policies, procedures and standards and other documentation such as log files and e-mails.

In determining the effectiveness, economy and efficiency of NRC's IT security services (Objective Three) we interviewed appropriate staff and analysed various control activities and policies for evidence of inefficiencies and lack of economy.

Our follow-up on the 1999 external IT Security Review (Objective Four) which consisted of interviews, and review and analysis of documentation and control activities, focussed on gathering evidence on the extent to which NRC has implemented that review's recommendations. A complete list of the 1999 external review's recommendations can be found in Appendix C.

EXHIBIT 3: MITS Four Major Areas of Controls

MITS Area	Overview
Area #1: Departmental IT Security Organization and Management	This area refers to how a departmental IT security program should be organized and managed. It covers roles and responsibilities, policy, resources and management.
Area #2: IT Security Resources for Projects	MITS specifies what IT managers must do as part of planning new programs, services or major upgrades to existing programs or services. These requirements include, at the earliest stage of the funding and approval process, determining the IT security requirements for these programs, services or upgrades; and indicating resource requirements in funding requests.
Area #3: Management Controls	This area refers to the management controls that apply to all departmental programs and services. Part III of MITS defines the technical and operational safeguards that support these controls.
Area #4: Technical and operational safeguards	MITS provides direction and guidance on some of the technical and operational safeguards that are available. Departments select a combination of these and, possibly, others. Together, they are intended to reduce risk to an acceptable level. Other security standards and technical documentation describe additional safeguards.

3.0 Audit Findings

3.1 Audit Objective One: To assess NRC's compliance with the MITS Standard

Overall conclusion

The degree of compliance with MITS varied among IMSB and the three Institutes that we looked at. With the exception of business continuity planning, IMSB is compliant with MITS. However, the three Institutes were less compliant in key areas such as risk management and the certification and accreditation of their systems.

It is important to note that that it is not possible for the audit team to conclude on whether NRC as a whole is compliant with MITS. This is due to the fact that NRC has not clearly defined and formally documented all its business critical systems – the foundation upon which NRC's governance model for IT security is based.

In our view, the following gaps in compliance represent areas of risk for NRC:

- Organization-wide monitoring and oversight of IT security are lacking. We found that NRC's Director of IT Security, NRC's IT Security Coordinator for MITS does not have the authority needed to carry out the role as principal contact for IT security matters. Therefore the Coordinator cannot assure senior management that all IT systems at NRC incorporate adequate and appropriate safeguards.
- Risk management with respect to IT security is inconsistent across the organization. As a result, NRC does not have a clear picture of either its exposure to IT security risks, or whether its IT systems provide the level of security that is commensurate with the sensitivity of the information they contain.
- The wide range of technologies and protocols for enabling NRC employees working off-site to access NRC's IT systems poses a continuing risk for the organization.

Findings

The audit team noted a number of strengths with respect to compliance with MITS. For example, NRC has specified the roles and responsibilities for managing IT security. It has also issued a comprehensive set of policies, procedures and standards for managing this function and instituted a security-awareness program for its employees. NRC screens staff to determine who will have access to which sensitive information, and has employed security zones. These zones partition the network and provide higher levels of security, depending on the sensitivity of information.

We expected to find that the Institutes, Branches and Programs (I/B/Ps) had, for the most part, adhered to the MITS standards. In meeting these standards, organizations can demonstrate that they have done what they need to do to adequately protect the information which they hold.

In August 2005, NRC presented to TBS its action plan and approach for achieving compliance with MITS. NRC has chosen to follow a "holistic approach" to IT security with respect to its "enterprise-level and business-critical systems" while at the same time creating a "technically open IT environment to facilitate research and innovation". Enterprise-level and business critical systems are those which are critical to enabling the organization to operate effectively.

We assessed NRC against the 29 groupings of MITS criteria, as noted above, and found that IMSB complies with 97% of them. The compliance rates for the three other institutes varied at 86%, 76%, and 76%, respectively. It should be noted that a "no" rating does not necessarily mean that there is zero compliance. In many cases, we saw activities which give partial compliance.

Although we were able to arrive at compliance rates for IMSB and the three Institutes examined, we could not do so for NRC as a whole. As shown in Exhibit 2 above, the reason for this is that IMSB is responsible for providing IT security services for only certain institutes, branches and programs. NRC does not have a single "master" document that provides a consolidated picture of which systems are either "enterprise-wide" or "business-critical". In the absence of such a document there is no reasonable assurance that IMSB is aware of and can therefore respond to all significant potential IT security risks in the I/B/Ps that it does not serve. Accordingly, it is not possible to conclude, with reasonable assurance, that IMSB's high compliance rate is applicable to NRC on a global basis.

Monitoring and oversight. NRC does not actively monitor and oversee IT security on an organization-wide basis. NRC's current arrangements for IT security neither require nor provide for program managers and IT project managers in the institutes to consult or communicate with NRC's IT Security Coordinator regarding arrangements for IT security for individual projects. MITS requires that these consultations take place. The objective is to ensure that all IT projects in an organization meet the necessary security requirements. These requirements vary according to individual projects.

MITS also requires that the IT Security Coordinator serve as a department's principal contact for this area. However, the Director for IT Security does not play this role at NRC; there is no documented mandate which gives the Director the responsibility and authority for IT security across the organization. Because communication and consultation among the parties involved in IT security is ad-hoc, NRC currently does not have a clear picture of either the IT security activities at its various institutes, or the IT security risks to which the organization as a whole is exposed. Because the Director's sphere of influence is limited, senior management has no assurance that every NRC IT system incorporates adequate and appropriate safeguards.

Managing IT security risks: Because risk management for IT security at NRC is inconsistent across the organization, senior management does not have a complete, organization-wide picture of the sensitivity of its systems and the information that they contain. Nor does it have comprehensive information on its exposure to risks related to IT security.

MITS requires that organizations continuously carry out activities designed to manage IT security risks. These activities include specifying the sensitivity of information and IT systems, carrying out threat and risk assessments (TRAs), and certification and accreditation of these systems. Statements of sensitivity identify and categorize information and related assets according to their sensitivity (level of confidentiality and required availability and integrity) and as such statements of sensitivity are an important step in the risk assessment process. The greater the sensitivity, the greater the risk associated with the particular asset or system. Threat and risk assessments involve assessing both the probability that a threat or risk could occur, and the impact of such an occurrence. Certification and accreditation represents a decision by management to operate a system, while acknowledging the risks involved in doing so. Once a system has been certified and accredited, responsibility for the security of the system transfers from those who built it, to those who operate it.

We expected to find that IMSB and the institutes in our sample had a formal risk-management process for IT security. We expected that this process would be sufficient to ensure that the information they held was adequately protected, given its sensitivity and factors such as potential threats, vulnerabilities and exposure to IT-related risks.

We found that IMSB and one of the three other institutes examined have formal risk-management processes. With some exceptions, they generally meet MITS requirements in this area. However, the two remaining institutes do not. Risk management in these institutes is informal and does not meet MITS standards. We noted that neither had formally assessed, nor documented the sensitivity of the information that they are responsible for. Therefore, we could not assess NRC’s exposure to risk associated with any failure to comply with MITS.

IT security staff in the two institutes told us that, despite the lack of statements of sensitivity and other gaps, the existing IT security regime is adequate to protect the information assets for which they are responsible. However, we could not objectively verify whether this is indeed the case. We found no documented evidence indicating the actual sensitivity of information in their various systems. Accordingly, we could not determine either whether their assessment of the level of sensitivity is correct or if the level of IT security is adequate and appropriate given the level of risk associated with their information assets. Therefore, the audit team could not determine whether the measures for safeguarding the information which these Institutes were holding were adequate.

We also found that none of the three institutes that we looked at have certification and accreditation processes in place for their IT security systems. Where an organization has not certified and accredited a system, management may be operating that system without clearly understanding the risks associated with it.

Finally, we found no evidence of a formal business-continuity plan which includes disaster recovery for NRC as a whole as required by MITS. We did observe that IMSB has a disaster recovery plan for the I/B/Ps it manages their IT security on their behalf. One of the other three institutes examined has a business continuity plan that requires comprehensive testing to be fully compliant. Another of the institutes examined has full built-in redundancy of their systems with the capability to provide uninterrupted service in the event of a complete power failure or other disaster; however, it has not been formally documented in a business continuity plan. The remaining institute examined has a partial disaster recovery plan for only part of its business. It should be noted however that the Director General for Administrative Services and Property Management has been tasked to develop a Business Continuity Plan for NRC. An effective business continuity strategy and plan is central in protecting an organization, especially critical business processes, from the effects of major failures or disasters and minimizing the damage caused by such events.

Mobile computing and tele-working: MITS includes a number of requirements relating to allowing personnel to securely access a department's information, networks and systems from off-site locations.

As required by MITS, we expected NRC to have taken specific steps to protect their computers, communications links, and the information that they contain from risks associated with activities such as mobile computing and tele-working. Typical measures that departments should institute include, but are not limited to, access controls, encryption, virus scanners and firewalls. They must also ensure that staff who are working off-site understand both their responsibilities for maintaining security, and the sensitivity and the criticality of the information they are able to access.

To assess the extent to which NRC is complying with these requirements, we interviewed the IT Security Coordinator and visited the three institutes in our sample. Of primary concern is the fact that NRC does not have any policy governing remote access to its IT resources and networks. We found that NRC, as compared to organizations of a similar size, is using an exceptionally wide range of “remote-access architectures”. This term refers to the technologies and protocols relating to remote access, i.e., access to NRC’s systems by employees who are working off-site. The range of protocols for remote access increases the possibility of a vulnerability that could be exploited and, subsequently, result in a serious compromise of NRC’s network.

We observed that in 2005-2006, NRC experienced eight high-risk incidents involving IT security. Five of the incidents were traced to weaknesses flowing from NRC’s current approach to providing remote access and resulted in unauthorized disclosure, destruction, removal, modification, interruption or use of NRC assets. Although in 2006-2007 there was only one high-risk incident reported to IMSB’s Information Protection Center, the current “menu” of remote-access architectures poses a continuing risk to NRC.

Recommendation 1:

To institute better monitoring and oversight of IT security, NRC’s senior management should designate an IT Security Coordinator for NRC who has responsibility and authority for IT security throughout the organization.

NRC Management Response:

Agreed; an IT Security Coordinator for NRC with organization-wide responsibility and authority for IT security will be appointed following consultation with the Senior Executive Committee (SEC). However, such a role will need to be supported by a strong IM/IT governance structure in general and a robust information security governance framework in particular. IM/IT governance will be addressed as part of a study that NRC has already initiated – a comprehensive IM/IT review to examine the current IT service delivery model and determine how NRC can enhance effectiveness and cost-efficiencies in this area. More specifically, the study will be broad in scope, encompassing all IM/IT services provided to NRC staff either centrally by IMSB or locally by individual institutes, branches and programs.

Terms of Reference have been developed and approved by SEC; the Director General for IMSB will co-lead this effort along with a Director General from a research institute still to be determined. The issues around IT service delivery will be examined and reported back to SEC by January 2008. Specific areas of opportunity or concern will also be identified for further study in a subsequent phase. It is anticipated that most of the audit recommendations will be addressed within the context of this review.

Recommendation 2:

To strengthen risk management for IT security, NRC should:

(a) define what is meant by “enterprise-wide” and “business critical” for IT systems;

(b) specify the sensitivity of all its IT systems including systems used only for research purposes and document the rationale or criteria for designating them as enterprise-wide and/or business-critical; and

(c) carry out other specific risk-management work such as sufficiently robust threat and risk assessments and certification and accreditation on all business critical systems, as required by NRC Policies and MITS.

NRC Management Response:

2. (a) Agreed: each IM/IT policy and standard is reviewed every two years as part of that policy’s lifecycle. All IT security policies and standards are scheduled for a comprehensive review during the July to September 2007 timeframe. “Enterprise-wide” and “business critical” will be added to NRC’s IM/IT Glossary of Terms, and appropriate definitions will be developed during the policy review.

2. (b) Agreed; once the definitions above for “enterprise-wide” and “business critical” are made available, all institute systems will be examined and appropriately identified. The IT Security Coordinator for NRC will have the responsibility that all institutes, branches and programs identify “enterprise-wide” and “business critical” systems and conduct appropriate risk analysis.

2. (c) Agreed; threat and risk assessment analyses will be conducted on all “enterprise-wide” and “business critical” systems that are identified and appropriate certification and accreditation will be completed.

Recommendation 3:

NRC should develop an organization-wide business-continuity plan for IT security.

NRC Management Response:

Agreed; the Director General for Administrative Services and Property Management has initiated an organizational-wide business impact analysis to examine NRC’s business functions and the effect that specific risks may have upon them. This analysis represents a critical first step in preparing a business continuity plan for NRC. This effort will be completed by March 2008, at which time a more comprehensive project plan to address NRC’s business continuity requirements including those that impact IT security can be developed.

Recommendation 4:

NRC should develop a remote-access policy with the goal of eliminating the use of insecure protocols, reducing the range of protocols in use, and strengthening the security of remote access for tele-workers.

NRC Management Response:

Agreed; remote access services will be examined as part of the IM/IT review study. Once the study is complete, appropriate policy direction will be developed and implemented to resolve NRC's remote access situation. This issue should be resolved by December 2008.

3.2 Audit Objective Two: To assess NRC's adherence to its own security policies and standards

Overall Conclusion

We found varying levels of compliance with NRC's policies and standards governing IT security. IMSB was compliant overall. However, for two of the three institutes that we looked at, compliance levels were substantially lower at 58%.

Findings

NRC's security policies are substantially equivalent to the MITS standards. Therefore, to the extent that it complies with MITS, NRC also complies with its own policies. NRC's policy requires risk-management activities to be carried out only for its "business-critical" systems and high-risk technologies such as wireless networks. This risk-based approach is cost-efficient and aligns with MITS requirements.

IMSB continues to be compliant overall with NRC's policies and standards, meeting 95% of their requirements. The compliance rates for the other three institutes are 79%, 58% and 58% respectively.

We found that the key compliance issues for the institutes with the lowest compliance rates paralleled those discussed earlier under Audit Objective 3.1 with respect to weaknesses in risk-management processes, change management, and business continuity planning. Both institutes told us that they were complying with NRC policy on risk management for IT security. They said that carrying out risk-management activities on their IT systems had not been necessary because these systems were not business-critical. However, we could not determine whether this is, in fact, the case because neither institute was able to provide us with any Statements of Sensitivity. Accordingly we cannot determine whether the two institutes comply with NRC's IT policies and standards on risk management.

If further analysis shows that these two institutes do not have systems defined as being "business-critical", NRC's risk-management requirements may not apply to them. In that case, the institutes would be considered to be more compliant with NRC's applicable policies and standards.

We have no additional recommendations beyond those relating to managing IT security risks, noted earlier, under Audit objective 3.1.

3.3 Audit Objective Three: To determine the effectiveness, economy and efficiency of the management of NRC's IT security services

Overall Conclusion

We have concluded that opportunities exist to improve the economy, efficiency and effectiveness of the management of NRC's IT security services.

Findings

Effectiveness. We expected to find that IT security management had instituted the necessary levels of control to ensure that IT security services are effective in protecting NRC's information assets.

We found that IT security services at IMSB and in the three institutes examined in responding to the needs of their respective organizations, employ widely varying practices and methods and resulting in differing levels of compliance with MITS and NRC policies. However, as noted earlier under Objective 3.1, the effectiveness of IT security management could be improved with respect to better monitoring and oversight and risk management.

Economy and efficiency: We found the following two areas in which NRC could potentially improve economy and efficiency: asset management, storage, remote access, anti-virus and change management.

Certain potential inefficiencies have stemmed from NRC's decentralized management model. With respect to asset management, storage, remote access, anti-virus and change-management activities, we noted that under this model a number of institutes are providing their own services using a variety of hardware and software applications. In our view, it should be possible to provide centralized services in these areas, given that IMSB already provides anti-virus services to 17 I/B/Ps and change-management services to 12 I/B/Ps in addition to the Executive Offices.

Although savings in FTEs might not be significant if at all, by locating some or all of these services centrally NRC-wide or in part, NRC may be able to reduce both unnecessary duplication, and certain costs for software and hardware incurred by institutes that currently operate their own services. Our audit did not include an analysis to determine the potential savings from centralizing these services. Arriving at such a figure would form part of a business-case exercise which would also need to take into account the specific requirements of each I/B/P.

Centralizing the anti-virus program could also increase its effectiveness. Because anti-virus work is becoming more sophisticated, centralization would capitalize on the expertise that already exists in this area within IMSB. We observed that IMSB employs specialists in this area, and that the same level of expertise is not generally available in all of NRC's Institutes. This situation could affect NRC's ability to protect itself, as effectively as possible, from threats posed by viruses. While the statistics are incomplete as we noted during the course of the audit that not all incidents are reported, of note is that during 2005-2006, NRC experienced 42 reported virus incidents all of which were associated with a lack of a consistent, organization-wide approach to anti-virus protection. Although there are only 11 virus incidents reported to date in 2006-2007, the latest virus outbreak that occurred in January 2007, resulted in 28 compromised systems and five days of interrupted operations for one I/B/P not in receipt of IMSB's virus protection services. It should be noted that some I/B/Ps not in receipt of IMSB's services have also been successful at deterring virus outbreaks. A business case study should analyze the potential synergy of combining existing expertise at NRC that is necessary to ward off this more frequently occurring menace faced by all government and non-government organizations.

Recommendation 5:

Management should examine the potential costs, benefits and feasibility of centralizing the asset management, storage, remote access, anti-virus and change-management services that the Institutes currently provide.

NRC Management Response:

Agreed; as stated above, a comprehensive IM/IT review has been initiated to examine the current IT service delivery model and determine how NRC can enhance effectiveness and cost-efficiencies in this area. The services identified in this recommendation are all within the scope of the review, and the merits of further centralization of key IT services will also be explored. As stated above, the study will be completed and reported to NRC's Senior Executive Committee in January 2008.

3.4 Audit Objective Four: To follow-up on the observations and recommendations from the 1999 external IT Security Review

Overall Conclusion

NRC has responded to almost all of the recommendations in the 1999 external IT Security Review. Of most concern, is the continuing lack of an organization-wide business continuity plan.

Findings

In 2000, IMSB prepared an action plan to deal with the 20 observations and recommendations in the 1999 external Security Review. These covered areas such as—but not limited to—roles and responsibilities for IT, implementing an IT security program, additional IT support staff, remote access and training in IT security.

We found that of the 20 recommendations in the Review, 17 have been resolved, or are no longer applicable. The status of the remaining three is as follows:

- A response to the recommendation to implement intrusion detection systems into the networks is in progress. IMSB has acquired the necessary hardware.
- The recommendation to develop an NRC-wide business-continuity plan is still outstanding and needs to be finalized as identified earlier under objective 3.1.
- The recommendation to introduce safeguards for the protection of data and files (including e-mail) has not been fully addressed. The government's Public Key Infrastructure (PKI) represents a possible solution to meet NRC's intra-governmental communications requirements for sharing and protecting information. IMSB is promoting awareness throughout NRC of the PKI as a tool for protecting NRC's data. However, there is a known risk associated with sharing information extra-governmentally with NRC's clients and research collaborators for which neither the federal government nor the private sector have found a cost-effective technological solution for mitigating this risk.

See Appendix C for the individual assessments against each of the recommendations.

4.0 Conclusion

The degree of compliance with MITS varied among IMSB and the three institutes that we examined. Overall, IMSB is compliant with MITS at 97 percent. However, the three Institutes were less compliant at 86 percent, 76 percent and 76 percent in key areas such as risk management and the certification and accreditation of their systems.

It is important to note that it is not possible for the audit team to conclude on whether NRC as a whole is compliant with MITS. This is due to the fact that NRC has not clearly defined and formally documented all its business critical systems – the foundation upon which NRC's governance model for IT security is based.

In our view, the following gaps in compliance represent areas of risk for NRC:

- Organization-wide monitoring and oversight of IT security are lacking. We found that NRC's IT Security Coordinator does not have the authority needed to carry out the role as principal contact for IT security matters. Therefore the Coordinator cannot assure senior management that all IT systems at NRC incorporate adequate and appropriate safeguards.
- Risk management with respect to IT security is inconsistent across the organization. As a result, the NRC does not have a clear picture of either its exposure to IT security risks, or whether its IT systems provide the level of security that is commensurate with the sensitivity of the information they contain.
- The wide range of technologies and protocols for enabling NRC employees working off-site to access NRC's IT systems poses a continuing risk for the organization.

We found varying levels of compliance with NRC's policies and standards governing IT security. IMSB was compliant overall. However, for two of the three institutes that we looked at, compliance levels were substantially lower

We have concluded that opportunities exist to improve the economy, efficiency and effectiveness of the management of NRC's IT security services. These opportunities exist with respect to monitoring and oversight, risk management, asset management, storage, remote access, anti-virus protection and change management.

NRC has responded to almost all of the recommendations in the 1999 External Review of IT Security. Of most concern, is the continuing lack of an organization-wide business continuity plan.

Key recommendations

1. To institute better monitoring and oversight of IT, NRC's senior management should designate an IT Security Coordinator for NRC who has responsibility and authority for IT security throughout the organization.
2. To strengthen risk management for IT security, NRC should:
   (a) define what is meant by "enterprise-wide" and "business critical" for IT systems;
   (b) specify the sensitivity of all its IT systems including systems used only for research purposes and document the rationale or criteria for designating them as enterprise-wide and/or business-critical ; and
   (c) carry out other specific risk-management work such as sufficiently robust threat and risk assessments and certification and accreditation on all business critical systems, as required by NRC Policies and MITS.
3. NRC should develop an organization-wide Business-Continuity plan for IT security.
4. NRC should develop a remote-access policy with the goal of eliminating the use of insecure protocols, reducing the range of protocols in use, and strengthening the security of remote access for tele-workers.

5. Management should examine the potential costs, benefits and feasibility of centralizing the asset management, storage, remote access, anti-virus and change-management services that the Institutes currently provide.

See Appendix D for the detailed management action plans that will address the recommendations.

Appendix A: MITS Audit Criteria

No.	Audit Criterion
Departmental IT Security Organization and Management Controls	
1.	[MITS 9.0] MITS specified roles, responsibility and authority are documented in job descriptions and reflected in organization charts.
2.	[MITS 10.0] NRC has an IT Security Policy that is appropriate for the organization and meets the minimum standards specified in MITS.
Security Resources for Projects	
3.	[MITS 11.0] Funding requests for IT programs must identify IT security requirements and include these resource requirements in the funding request.
Technical and Operational Safeguards	

No.	Audit Criterion
4.	[MITS 13.0] IT security safeguards are deployed taking into consideration the sensitivity of assets, threats, vulnerabilities, incident history and exposure.
5.	[MITS 14.0] NRC has a control framework, policies and procedures to implement processes that support IT security, including but not limited to Configuration Management and Change Control, Help Desk and Problem Reporting, Capacity Planning and ancillary support services.
6.	[MITS 15.0] NRC must have a process that actively monitors for threats and vulnerabilities and takes appropriate preventive measures.
7.	[MITS 16.1] NRC must have a policy and standards for appropriate physical security of IT assets. (NOTE: responsibility for physical security is centralized within the Administrative Services and Property Management group at NRC)
8.	[MITS 16.2] NRC must have a policy, procedures and standards for safeguarding IT media throughout the media life cycle.

No.	Audit Criterion
9.	[MITS 16.3] NRC must have a policy and procedures for ensuring that staff are screened to a level appropriate for the sensitivity of IT assets that they access.
10.	[MITS 16.4.2] NRC must deploy an Identification & Authentication (I&A) mechanism that permits unique and unequivocal identification of each individual.
11.	[MITS 16.4.3] NRC must deploy an access control mechanism which ensures that users can only access information they are authorized for; with procedures to ensure that users are never authorized to access information at a greater sensitivity that the individual's security screening.
12.	[MITS 16.4.4] NRC must have a policy and technology for the use of GOC approved cryptographic technology where required.
13.	[MITS 16.4.6] NRC must have a policy for segregating networks into security zones, with graduated perimeter safeguards.
14.	[MITS 16.4.7] NRC must have procedures and technical safeguards for mobile computing and tele-workers.

No.	Audit Criterion
15.	[MITS 16.4.8] NRC must have a policy that controls the use of wireless devices on NRC premises.
16.	[MITS 17.0] The NRC IT architecture and IT operations must include tools and processes (including a security audit log function), that enable effective detection of incidents.
17.	[MITS 18.0] NRC must have an effective incident response capability (including staff with appropriate levels of authority), that can identify and prioritize incidents, respond, to report on and recover from incidents, and conduct post-incident analysis.
Management Controls	
18.	[MITS 12.1] NRC must have an IT system development life cycle (SDLC) that explicitly considers IT security requirements in each phase of the life cycle.

No.	Audit Criterion
19.	[MITS 12.2] NRC must have a documented method for determining the sensitivity of IT assets, and a process for ensuring that all IT assets are identified and categorized according to sensitivity.
20.	[MITS 12.3] The NRC SDLC must ensure that IT systems are accredited by the appropriate accreditation authority subsequent to an approved threat risk assessment and certification process.
21.	[MITS 12.5.1] NRC must have a process for the conduct of vulnerability assessments on highly sensitive or highly exposed systems.
22.	[MITS 12.5.2] NRC must have a policy and procedures (including a verifiable audit trail) for the review and application of security related patches.
23.	[MITS 12.6] NRC must have a policy to restrict the degree of privileged access that any single individual has to an IT system or major operational function.

No.	Audit Criterion
24.	[MITS 12.7] NRC must have a policy and process to ensure that all contracts properly reflect the appropriate IT security requirements.
25.	[MITS 12.8] NRC must have an IM/IT continuity plan to minimize the interruption of critical IT services.
26.	[MITS 12.9] NRC must have a documented policy for the application of sanctions in case of IT incidents due to misconduct or negligence.
27.	[MITS 12.10] NRC must have a policy and process for ensuring the security of NRC information provided to other organizations; and for ensuring the security of information received from other organizations while it is under NRC control.
28.	[MITS 12.11] NRC must have a policy for an annual self assessment of their IT security program, and for IT security audits to be included in the scope of NRC's internal audit program.

No.	**Audit Criterion**
29.	[MITS 12.12] NRC must have an ongoing security awareness program; and a policy to ensure that staff with specific IT security responsibilities receive appropriate specialized training.

Appendix B: NRC IT Security Policies Audit Criteria

No.	Audit Criterion
Departmental IT Security Organization and Management Controls	
1.	*[NRC Organization and Management Standard – Annex B 3.1.1]* DG is responsible for appointing an ISSO to coordinate and address IT security issues
Technical and Operational Safeguards	
2.	*[NRC Organization and* Management Standard 6.1.1] The confidentiality, integrity and availability requirements for each IS will be documented in a statement of sensitivity.
3.	*[NRC Organization and Management Standard 6.1.2]* A TRA will be conducted for each enterprise-level and other critical business system
4.	*[NRC Organization and Management Standard 6.1.3]* An IS Security Plan should be developed and maintained for each critical business system.

No.	Audit Criterion
5.	*[NRC Organization and Management Standard 6.1.4]* The appropriate management authority will accredit each critical business system.
6.	*[NRC IPP Policy Statement 7.5]* System security measures should be proportionate to the security levels of the information and assets involved, and must take into account the identified threats and vulnerabilities.
7.	*[Telecommunications Standard, Annex A]* 2. The change management inventory should include all communications/network hardware, software, services and data. 3. Any changes that impact the system in a permanent or semi-permanent way should be subject to configuration management. • 3.1 The change control process should include mechanisms for: Requesting changes, Recording and tracking outstanding changes, Approving requests, Testing and documenting changes, Incorporating changes and notification.
8.	*[Information Protection Operations Standard Annex C]* 2. IT media must be assigned a security classification or designation commensurate with the most sensitive information on the media. 3. IT media must be packaged, transported and transmitted in a manner that protects against rough handling, tampering, compromise, and environmental threats such as extreme heat, cold and humidity. 4. All IT media must be appropriately sanitized before being released from the IT environment for reuse, servicing or disposal.

No.	Audit Criterion
9.	*[Access Control Standard 5.2]* I/B/P must ensure access to IT systems, networks and data is permitted only to those with proper approval. Such approval is determined by the individual's security clearance etc. as well as that person's need to know.
10.	*[NRC Access Control Standard 5.4]* IT systems must authenticate all user identifiers to prevent impersonation where applicable.
11.	*[NRC Information Protection Program, Annex D, 3.1]* Any cryptographic module used to encrypt NRC data must conform to the standards detailed in FIPS 140-1 or 140/2, Security Requirements for Cryptographic modules.
12.	*[NRC Telecommunications Security Standard 5.8]* With the exception of computers used for telecommuting, the use of local modems to establish direct dial connections is generally not permitted.
13.	*[NRC Telecommunications Security Standard 5.6]* Wireless LAN technology can be used for NRCnet segments where wired connectivity is either impractical or impossible but they should be isolated from NRCnet.

No.	Audit Criterion
14.	*[Information Protection Operations Standard, Annex A, 2.1 and 2.2]* As a minimum, network based intrusion detection tools should be installed and configured to monitor all internet connections. As a minimum, host based intrusion detection tools should be installed and configured to monitor servers and systems which are critical assets.
15.	*[NRC documents]* -IT Security Incident Response Procedure -Computer Incident Response Team Standard -IT Security Investigative Procedures.
Management Controls	
16.	*[NRC Organization and Management Standard 6.1.1]* The confidentiality, integrity and availability requirements for each IS will be documented in a statement of sensitivity. The methodology is specified in Security Risk Management Guide, Annex B – Sensitivity Analysis.

No.	Audit Criterion
17.	[*NRC Information Protection Operations Standard 5.9]* An SRCL must also be included when there are physical security, information technology security or personnel security requirements.
18.	*[NRC Information Protection Operations Standard 5.8]* Each I/B/P is responsible for developing and maintaining fully tested and documented IM and IT continuity plans. The IT continuity plan must be capable of ensuring that critical services will be restored in timely and efficient manner…
19.	*[NRC Policy Governing the Use of NRC IT resources, 9]* …it should be clearly understood that NRC employees who willingly and deliberately violate this policy may be subject to administrative action or disciplinary action up to and including termination of employment.

Appendix C: 1999 External IT Security Review Recommendations and 2007 Audit Findings

Recommendation from 1999 external review	**Recommendation Implemented**
1. IT Resource Ownership, Governance and Support. The issue of IT resource ownership and governance is an issue, not only for IT security, but also for the development of an overall IT architecture. It must be clear to all involved who 'owns' and is responsible for the different portions of the IT infrastructure, e.g., workstations, servers, LANs, WANs, etc. In this manner the responsibility for the security of the IT infrastructure can be allocated. It also must be clearly stated what rules govern how the different 'owners' interact. For instance, the rules a system 'owner' must live by when they connect to the network should be specified. This will require that the various IT technical support groups distributed throughout NRC work co-operatively together.	Yes
2. Define an NRC IT Security Policy. NRC does not currently have a defined IT security policy. High-level supporting policy, that describes the objectives, strategies and rules that govern the program, is required in order to implement an IT security program. The IT security policy should be derived from, and directly related to, the business objectives and strategies of NRC.	Yes

Recommendation from 1999 external review	Recommendation Implemented
3. IT Security Roles and Responsibilities. The roles and responsibilities regarding IT security within NRC need to be defined and formalized. The overall organizational structure for IT security within NRC should be determined, and the roles and responsibilities of personnel at the various levels (NRC, Institute/Branch, system, etc.), need to defined and allocated. As a minimum, IT security responsibilities must be assigned to an individual for each NRC IT resource, and they must be given the resources, authority and mandate to exercise their responsibilities.	Yes
4. Develop Data Classification Scheme. Sensitive data exists within NRC, but there is no scheme for identifying and classifying this data as required by GSP. Sensitive data needs to be identified and labeled, and safeguards must be implemented to protect the information appropriately.	Yes
5. Consider Eliminating Part-Time System Administrators. The presence of part-time system administrators, particularly for server systems is a concern. These administrators frequently do not have the time, or skills, to properly manage, or secure, the systems they are responsible for. As a result, their systems tend to be the most vulnerable, since security is often the first thing skipped when people are in a hurry (the "just get the system working, we'll worry about security later" mentality).	Yes

Recommendation from 1999 external review	**Recommendation Implemented**
6. Provide Additional NRCNet Support Personnel. Currently, there are insufficient personnel to properly manage the NRCNet infrastructure. As a result, proper network planning, monitoring and maintenance is not occurring, with resources simply stretched trying to keep NRCNet running ('firefighting'). A number of sites observed that they normally advised the network operations personnel when segments of the network were down, vice being told of the problem. Securing the network infrastructure is simply an extension of sound network management principles. If there aren't enough people to support the basic network management functions, then clearly there will not be enough to secure NRCNet either.	Yes
7. Non-NRC Personnel Access. The recommendations arising from the NRC Network Access for Non-NRC Personnel Report [NRC] should be considered in the implementation of an NRC IT security program.	Yes

Recommendation from 1999 external review	Recommendation Implemented
8. Develop and Implement an IT Security Program. An NRC IT security program should be developed and implemented. The primary activities that need to be planned and executed include: ▪ development of NRC security policies; ▪ identification of the assets to be protected, i.e., what is important in terms of data, systems, services, etc.; ▪ conduct of a high-level risk analysis for the identified assets; ▪ development of an IT security architecture, and identification of the safeguards required to protect critical assets; ▪ implementation of the safeguards; ▪ periodic evaluation of safeguards, security compliance checks, ongoing monitoring of system security, vulnerabilities, threats, etc.; ▪ implementation of a security awareness program; and ▪ incident handling.	Yes
9. IT Security Training. Implement IT security training for those staff that are responsible for IT security. This could be accomplished by running in-house courses, or by having personnel attend commercial courses. The co-ordination and tracking of this training should be conducted by the central IT security organization.	Yes

Recommendation from 1999 external review	**Recommendation Implemented**
10. Define and Gain Control of Electronic Perimeter. Currently, NRCNet does not have an established electronic perimeter, with most of the network infrastructure simply being an extension of the Internet. A perimeter is required in order to segregate public and private information, and to control access between these two domains. The primary goal of establishing the perimeter is to manage external access to NRC information and IT resources. The public, collaborators, contractors and NRC employees should only have external access to the NRC IT resources that they need – no more, no less.	Yes
11. Segregation of Data, Systems and Services. The IT infrastructure of NRC should segregate systems based on the information they store, the services they provide and who requires access to them.	Yes
12. Protect Information on NRCNet Backbone. Currently, NRC is using CA*net II as the NRCNet backbone between regional sites. All inter-site information flows over this semi-public backbone, and is generally transmitted 'in-the-clear'. As such, it is susceptible to network 'sniffing' and compromise while in transit between NRC sites. Consideration should be given as to the sensitivity of this information, and whether safeguards (e.g., encryption), are required. In particular, an encrypted virtual private network (VPN) between the NRC regional sites may be appropriate.	Yes

Recommendation from 1999 external review	**Recommendation Implemented**
13. Consider Implementing Network Intrusion Detection. The implementation of network intrusion detection should be considered for key network connections. Regardless of how well NRC's IT infrastructure is secured, intrusion detection is the 'burglar alarm' that warns of an attack, and enables a timely response. Initially this capability should be concentrated on the external points of access to counter the external threat. Depending on requirements, it could later be expanded to cover key internal areas, or complemented with host-based intrusion monitoring systems of critical systems (to counter the internal threat).	In progress.
14. Individual Data and File Protection. NRC staff exchange information with others world-wide. Some of this information is sensitive, and requires appropriate protection, e.g., encryption. As well, the Canadian government is implementing a PKI infrastructure for the protection and sharing of information among government departments. While this could be used to meet NRC internal and intra-department requirements, many collaborators and clients require secure communications with NRC personnel or services (e.g., CISTI). Safeguards to support the protection of files and e-mail need to be put in place.	No

Recommendation from 1999 external review	**Recommendation Implemented**
15. Implement CM of Significant IT Resources. A number of IT resources, including the NRCNet infrastructure and significant public and business systems, are critical to the operation of NRC. A CM program should be implemented to manage these systems, including a formal process by which they are modified, brought on-line, etc. By bringing these systems under formal control, the integration of IT security requirements will be facilitated. For instance, the consideration of IT security issues can be a mandated part of the system change process, verification testing can be required before activating a system for production, etc. If you are not actively managing the configuration of your systems, then the security of them cannot be assured.	Yes
16. Develop Business Continuation Plan. A business continuation plan should be developed and implemented for critical NRC IT resources required to support NRC operations. As a minimum, it should address NRCNet itself (including external connectivity), Sigma, major business support systems, and the significant public IT resources identified in 3.2.2	In progress.
17. Remote Access. Remote access of NRC resources should be transitioned from insecure protocols to more secure ones that include strong identification and authentication, and that also encrypt the data being transmitted between the systems. For instance, the use of insecure protocols such as Telnet, X, rlogin, etc. to remotely access NRC systems should be eliminated, and replaced by secure protocols such as SSH, etc.	Yes

Recommendation from 1999 external review	Recommendation Implemented
18. Integrate IT Security into the System Life-Cycle. IT security needs to be integrated into the life-cycle of the NRC IT infrastructure, systems, and software. This includes design, development, procurement, implementation, operation and de-activation. IT security should just become another important consideration in how NRC does business, and should not be viewed as something extra that is tacked onto a system when it is ready for deployment. If IT security requirements are considered 'up front', significant costs can be saved in the long run.	Yes
19. System Security and Monitoring. The security of individual systems should be improved. Guidance and training should be provided to system administrators on how to secure, maintain, and monitor the security of their systems. Regular vulnerability scanning, using up-to-date commercial tools will help identify system weaknesses. Due to the specialized knowledge required to run these tools, this is a service that might be best provided by the NRC central IT security organization. In the end, the securing of the individual systems provides protection from the inside threat, and also provides a second layer of 'defence' should the electronic perimeter be breached.	Yes
20. NRCNet Protection and Availability. Some parts of NRC rely on NRCNet and in particular, it's external connectivity, to earn money (e.g., CISTI, and others). Appropriate agreements should be reached on the level of service that is to be provided by NRCNet to support these activities, e.g., integrity and availability requirements.	Partially resolved. Institutes need comprehensive SOS documents to conclusively determine if safeguards are adequate and appropriate for the sensitivity of the systems.

Appendix D: Management Action Plans

Audit Recommendations	Corrective Management Action Plan	Expected Completion Date	Responsible NRC Executive
1. To institute better monitoring and oversight of IT, NRC's senior management should designate an IT Security Coordinator for NRC who has responsibility and authority for IT security throughout the organization.	Appointment of IT Security Coordinator following consultation with the Senior Executive Committee (SEC). IT Security Coordinator role to be supported by a strong IM/IT governance structure in general and a robust information security governance framework in particular. IM/IT governance will be addressed as part of a study that NRC has already initiated – a comprehensive IM/IT review to examine the current IT service delivery model and determine how NRC can enhance effectiveness and cost-efficiencies in this area.	January 2008 January 2008	VP Corporate Services
2. To strengthen risk management for IT security, NRC should: (a) Define what is meant by "enterprise-wide" and "business critical" systems for NRC:	IM/IT policy and standard is reviewed every two years as part of that policy's lifecycle. All IT security policies and standards are scheduled for a comprehensive review during the July to September 2007 timeframe. "Enterprise-wide" and "business critical" will be added to NRC's IM/IT Glossary of Terms, and appropriate definitions will be developed during the policy review.	September 2007	VP Corporate Services

Audit Recommendations	**Corrective Management Action Plan**	**Expected Completion Date**	**Responsible NRC Executive**
(b) specify the sensitivity of all its IT systems and document the rationale or criteria for designating them as enterprise-wide and/or business-critical ; and	Once the definitions above for "enterprise-wide" and "business critical" are made available, all systems will be examined and appropriately identified. The IT Security Coordinator for NRC will have the responsibility that all institutes, branches and programs identify "enterprise-wide" and "business critical" systems and conduct appropriate risk analysis.	March 2008	Heads of I/B/Ps NRC IT Security Coordinator
(c) carry out other specific risk-management work such as sufficiently robust threat and risk assessments and certification and accreditation on all business critical systems, as required by NRC Policies and MITS.	Threat and risk assessment analyses will be conducted on all "enterprise-wide" and "business critical" systems that are identified and complete appropriate certification and accreditation. The IT Security Coordinator for NRC will have the responsibility that all institutes, branches and programs identify "enterprise-wide" and "business critical" systems and conduct appropriate risk analysis.	March 2008	Heads of I/B/Ps NRC IT Security Coordinator
3. NRC should develop an organization-wide Business-Continuity plan for IT security.	The Director General for Administrative Services and Property Management has initiated an organizational-wide business impact analysis to examine NRC's business functions and the effect that specific risks may have upon them. This analysis represents a critical	March 2008	VP Corporate Services

Audit Recommendations	Corrective Management Action Plan	Expected Completion Date	Responsible NRC Executive
	first step in preparing a business continuity plan for NRC. This effort will be completed by March 2008, at which time a more comprehensive project plan to address NRC's business continuity requirements including those that impact IT security can be developed.		
4. NRC should develop a remote-access policy with the goal of eliminating the use of insecure protocols, reducing the range of protocols in use, and strengthening the security of remote access for tele-workers.	Remote access services will be examined as part of the IM/IT review study. Once the study is complete, appropriate policy direction will be developed and implemented to resolve NRC's remote access situation.	December 2008	VP Corporate Services
5. Management should examine the potential costs, benefits and feasibility of centralizing the asset management, storage, remote access, anti-virus and change-management services that the Institutes currently provide.	A comprehensive IM/IT review has been initiated to examine the current IT service delivery model and determine how NRC can enhance effectiveness and cost-efficiencies in this area. The services identified in this recommendation are all within the scope of the review, and the merits of further centralization of key IT services will also be explored.	January 2008	VP Corporate Services

Appendix E: Glossary

List of Abbreviations

ASPM	Administrative Services and Property Management
BRI	Biotechnology Research Institute
CHC	Canadian Hydraulics Center
CIO	Chief Information Officer
CISTI	Canada Institute for Scientific and Technical Information
CM	Change management
GSP	Government Security Policy
HIA	Herzberg Institute of Astrophysics
IAR	Institute of Aeronautical Research
IBD	Institute for Biodiagnostics
I/B/P	Institutes, Branches and Programs
IBS	Institute for Biological Sciences
ICPET	Institute for Chemical Process and Environmental Technology
IFCI	Institute for Fuel Cell Innovation
IIT	Institute for Information Technology
IM	Information Management
IMB	Institute for Marine Biosciences
IMI	Industrial Materials Institute
IMS	Institute for Microstructural Sciences
IMSB	Information Management Services Branch
IMTI	Integrated Manufacturing Technologies Institute

INMS	Institute for National Measurement Standards
IOT	Institute for Ocean Technology
IPC	Information Protection Center
IRAP	Industrial Research Assistance Program
IRC	Institute for Research in Construction
ISSO	Information Systems Security Officer
MITS	Management of Information Technology Security Standard
NINT	National Institute for Nanotechnology
PBI	Plant Biotechnology Institute
SEC	Senior Executive Committee
SDB	Strategy and Development Branch
SIMS	Steacie Institute for Molecular Sciences
SOS	Statement of Sensitivity
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment