Audit of Information Technology Security

May 2001

Audit and Evaluation Branch

Environment Canada Environnement Canada

Canada

Report Clearance Steps

Planning phase completed	October 2000
Implementation phase completed	December 2000
Report completed	February 2001
Report approved by Departmental Audit and Evaluation Committee (DAEC)	May 3, 2001

Acronyms used in the report

ACE	Access Control and Encryption
BRP	Business Resumption Plan
CMC	Canadian Meteorological Centre
EC	Environment Canada
EMF	Enhanced Management Framework
GWMC	Government-wide Mission Critical
IM	Information Management
ITS	Information Technology Security
MSC	Meteorological Service of Canada
PC	Personal Computer
RCMP	Royal Canadian Mounted Police
SID	Systems and Informatics Directorate
TB	Treasury Board
TBS	Treasury Board Secretariat
UPS	Uninterruptible Power Supply
Y2K	Year 2000 Preparedness

Acknowledgments

The Review Branch Team under the direction of Elizabeth Murphy-Walsh, was lead by V. Neimanis and included Lucie Héon and Erin Campbell, under contract. Part of the interviews as well as the organization and the facilitation of the focus group were done under contract respectively by Arnie Frances from Hallux and David Prime from PriceWaterhouseCoopers. The team would like to thank those individuals who contributed to this project and particularly:

- departmental interviewees who provided expertise, insight, comments and documentation crucial to this review;
- those employees who supplied detailed comments on the draft version.

Table of Contents

Executive Summary

Context

Treasury Board Secretariat (TBS) requires that each Department periodically conduct an audit of Information Technology Security (ITS) to assess the compliance of the Department with TBS Security Policy. In addition, the Department was undertaking the development of an *IM/IT Strategy* and had to assess the level of ITS. Therefore, in the *2000-2001 Review Plan,* DAEC approved the conduct of an ITS audit to comply with TBS Security Policy and to provide assurance to senior management that ITS strongly supports the Department in achieving its objectives.

This Information Technology (IT) security audit encompassed a review of the organization and administration of ITS, personnel security, physical security, hardware security, software security, communications security and operations security throughout the Department. The work being done for the *IM/IT Strategy* was taken into account and integrated where appropriate. This audit reports on the Department's level of compliance with the Treasury Board ITS policy, departmental best practices and vulnerabilities, and provides recommendations.

Findings

The overall conclusions of this audit are that:

- EC has a Government-wide Mission Critical (GWMC) level A system for the Meteorological Service of Canada (MSC) requiring 24hour/7day operations and robust ITS management. EC meets the security requirements for such a system, as demonstrated by the Y2K preparedness exercise, the 1998 ice storm and the "I luv you" virus.

- MSC maintains high value information and is responsible for the management of the network on which departmental IT is built. It has excellent practices and in some cases exceeds Treasury Board standards. However, such best practices are not shared across the Department, causing inconsistency in the application of policies and procedures.

- Many good or best practices were found and, if their use was generalized throughout the Department, the ITS would be strengthened. However, ITS procedures are not implemented nor monitored in a consistent manner across the Department; some areas fall short while others exceed policy requirements. The issue here is strong leadership to apply and monitor policies and procedures systematically and standardize them in an easily-accessible repository.

- Generally, the Department partially meets most of the objectives outlined in the Treasury Board ITS Audit Guide (1995).

- Training for users and technicians as well as increasing user awareness were identified as key components in improving ITS management.

- Departmental staff involved in the development of secret or sensitive documents do not have secure tools to ensure quick and proper consultation across the Department, while meeting senior management deadlines.

- Government-wide initiatives such as Government On-Line will accelerate the deployment of information technology and thus may accentuate current weaknesses in the application of ITS.

Recommendations

The overall findings and the analysis led the audit to submit the following recommendations under the categories of management, communication and training and tools.

Management

1. **It is recommended that the ADM of Corporate Services in consultation with the ADM of MSC review the role of ITAC. This review should include: a revised mandate for the committee and its sub-committees; a change in the reporting relationship of the committee; and an examination of membership and roles to ensure all stakeholders are appropriately represented.**

2. **It is recommended that the DG of SID undertake to strengthen the management framework for ITS in the department. This would include: greater clarification of roles and responsibilities of ITS; improved coordination and consistency in policy application and procedures; enhanced ITS planning; and, reporting.**

Communication and Training

3. **It is recommended that the DG of SID, in consultation with the Director of Informatics at MSC, the DG, HR and the Departmental Security Office (DSO), develop an ITS awareness/ communication/ marketing strategy.**

Tools

4. **It is recommended that the DG of SID, in consultation with ITAC members, review options to implement appropriate software to monitor ITS logs on a departmental level.**

5. **It is recommended that the DG of SID, in consultation with the Director of Informatics at MSC and the Departmental Security Office, identify and make available improved electronic tools to facilitate the transmission of secure communication.**

Management Response

Recommendation #1: Agree
SID is working with representatives from the Services/Regions in evaluating the role of all groups reporting to the e-Government Integration Committee (EGIC). ITAC is being addressed as part of this exercise. We recognize the importance of having all players involved in Information Technology Security (ITS) and all program/table interests addressed through this exercise. The resulting realignment of roles and reporting relationships will, hopefully, allow us to address the concerns that you have identified in this area.

Timeline: June 2001

Proposed Action: Complete EGIC Review of Reporting Sub-Committees, under responsibility of DG/SID.

Recommendation #2: Agree
SID has, as part of the IM/IT Strategy development process, been examining the roles and responsibilities relating to the ITS management framework. We recognize that there are numerous shortcomings relating to functional and operational activities in this domain and have requested and will be receiving funding through Program Integrity II to address them. However, this supplementary funding is only available for the next two years.

Timeline: March 2002

Proposed Action: We will take steps to clarify roles, improve policy application consistency, improve ITS planning/reporting. Specific actions will include: 1) strengthening the ITS team by creating more positions to support the program in the NCR; 2) developing/updating departmental guidelines/policies in the role of national ITS Coordinator, and; 3) by acquiring tools to maintain operations. Actions will be under the responsibility of DG/SID.

Recommendation #3: Agree
We are very supportive of an ITS awareness campaign. We have, to date, taken some limited measures (regular notices to staff, special messages when particularly notable threats have been identified, etc.) and ITAC has asked that we do more. We will be promulgating more substantive products on this in the coming months.

Timeline: March 2002

Proposed Action: We will be taking steps to improve information packaging and messaging to improve impact and prepare training material for delivery to staff on an as-and-when required basis. National and Regional ITS Coordinators are assembling a communications plan to inform users on the role of ITS and why certain measures are necessary to secure the network infrastructure. This plan will combine NCR and Regional office activities to increase national consistency. Actions will be under the responsibility of DG/SID.

Recommendation #4: Agree
This recommendation has raised some technical issues that we will be addressing with regional and service IT staff (required hardware, software, technical skills, personnel required, etc.) in the coming weeks. We will provide further feedback following our discussions with these groups.

Timeline: June 2001

Proposed Action: Review recommendation with technical staff and provide a formal response to Review Branch under direction of DG/SID.

Recommendation #5: *A*gree
We are presently involved in planning for a secure messaging pilot. As you may be aware, the government-wide efforts in this area will only allow for transmission of documents up to the "Secure B" level. The results from our pilot should provide us with a better understanding of the relative costs and benefits of implementing the tools and processes needed to transmit at the B level.

Timeline: September 2001

Proposed Action: SID to work with regions on pilot project to exchange encrypted and/or digitally signed e-mail messages up to Protected B level. Other decisions with respect to feasibility/implementation to follow. Actions will be under the responsibility of DG/SID.

Introduction

Context of the Audit

Treasury Board Secretariat (TBS) requires that each Department periodically conduct an audit of Information Technology Security (ITS) to assess the compliance of the Department with TBS Security Policy. In addition, the Department was undertaking the development of an *IM/IT Strategy* and had to assess the level of ITS. Therefore, in the *2000-2001 Review Plan,* DAEC approved the conduct of an ITS audit to comply with TBS Security Policy and to provide assurance to senior management that ITS strongly supports the Department in achieving its objectives.

Context of ITS

> *The consensus on all fronts is that no one is ever 100 percent secure. The real art in network security is understanding the nature of your exposure, the inherent risks and most importantly the value of the data you are trying to protect.*[1]

ITS relates to the measures taken by an organization to ensure the integrity of the information processed with information technology systems. An inherent level of risk must be accepted when an organization implements IT into its operations and is accentuated in a world where technologies become obsolete very quickly. While a number of procedures and practices may be employed to safeguard IT, it is impossible to protect IT against all threats, accidental or deliberate, with 100 percent certainty.

> *Managing risk can help make better use of budget and resources. So often we see people building million dollar fences around five dollar assets. But we also see huge assets with very little security around them.*[2]

Environment Canada (EC) strives to achieve a balance between those measures that are considered diligent and reasonably practical, and those that may be overly expensive or cumbersome to use. ITS is managed in accordance with the degree of risk and the likelihood of occurrence in relation to the value of information for the Department. Treasury Board Security Policy provides guidelines to ensure adequate departmental ITS; even when fully implemented such guidelines will not protect the organization with absolute certainty. The objective is to employ reasonable measures to manage and minimise risk.

Additionally, EC is a science-based Department. This implies a need to balance ITS requirements with the necessity of sharing information with partners and stakeholders. Some program areas, including Environmental Protection (Enforcement), Environmental Conservation, Policy and Communication and Human Resources, retain sensitive

---

[1] Deveau, Denise, When to say “no access”, Computing Canada, vol 26, issue 26, December 15, 2000, p. 14.

[2] Ibid., p. 15

information and require an elevated level of security. In contrast, Meteorological Service of Canada (MSC), which carries out a Government-wide Mission Critical (GWMC) function, must operate in real time everyday of the year to ensure the safety of the public. This function requires elevated security measures to protect networks against damage. Thus, EC has an array of security requirements resulting from the diversified nature of the Department's business and has to find an adequate balance to manage ITS.

Scope and Methodology

The objective of this audit was to determine the degree to which the Department is in compliance with the Treasury Board Secretariat (TBS) ITS Guide (1995); to identify best practices and vulnerabilities; and to provide recommendations. The audit also considered five complementary departmental initiatives conducted as part of the development of the IM/IT Strategy:

- the E-Government capacity check, a study conducted by KPMG;
- the inventory of all E-related committees by CGI;
- the assessment of the current capacity of the Department pointing to IM/IT vulnerabilities by EDS;
- a telecommunications study contracted out by MSC, due March 2001; and
- an intrusion analysis test conducted on the Green Lane.

The TBS ITS Audit Guide (1995) was used to define the audit criteria. These criteria provided an analytical basis for developing observations and findings. Three lines of evidence were utilized to develop findings for this audit, including more than 50 interviews, a comprehensive file review and a focus group. Personnel responsible for the management and administration of ITS and a cross section of staff working in support of each of the Department's four business lines were selected from the five regions and headquarters for interview. Throughout the data collection process, a concentrated effort was made to collect ITS related documentation. Finally, the initial findings derived from the previous two lines of evidence were presented to a focus group held with the Information Technology Advisory Committee (ITAC). The activities of the focus group included endorsing and ranking the risk statements, and identifying some initial management strategies to address them. For details refer to Annex 1.

Supplementary information related to the Government On-Line (GOL) strategy and the use of official languages as they relate to ITS was also gathered and is discussed later in this report under the heading "Other Issues".

Findings

The overall conclusions of this audit are that:

- EC has a Government-wide Mission Critical (GWMC) level A system for the Meteorological Service of Canada (MSC) requiring 24hour/7day operations and robust ITS management. EC meets the security requirements for such a system, as demonstrated by the Y2K preparedness exercise, the 1998 ice storm and the "I luv you" virus.

- MSC maintains high value information and is responsible for the management of the network on which departmental IT is built. It has excellent practices and in some cases exceeds Treasury Board standards. However, such best practices are not shared across the Department, causing inconsistency in the application of policies and procedures.

- Many good or best practices were found and, if their use was generalized throughout the Department, the ITS would be strengthened (see details in Annex 2). However, ITS procedures are not implemented nor monitored in a consistent manner across the Department; some areas fall short while others exceed policy requirements. The issue here is strong leadership to apply and monitor policies and procedures systematically and standardize them in an easily-accessible repository.

- Generally, the Department partially meets most of the objectives outlined in the Treasury Board ITS Audit Guide (1995).

- Training for users and technicians as well as increasing user awareness were identified as key components in improving ITS management.

- Departmental staff involved in the development of secret or sensitive documents do not have secure tools to ensure quick and proper consultation across the Department, while meeting senior management deadlines.

- Government-wide initiatives such as Government On-Line will accelerate the deployment of information technology and thus may accentuate current weaknesses in the application of ITS.

The findings are presented under seven broad categories, which cover all 15 objectives of the TBS ITS Guide.

The study found that three objectives of Treasury Board ITS Guide were not applicable to EC. These are:
- Management of cryptographic material; EC does not use cryptography to encode information.
- Use of electronic authorization or digital signature; EC has very limited electronic authorization at this time, except for a pilot project developed in the Atlantic region, related to leave forms and travel authorization.
- Emanations security for IT systems processing top secret or extremely sensitive information; this does not apply to EC.

1. Organization and Administration

Included in this category of findings are the management structure of ITS, the risk management framework, the access to IT, and the monitoring of ITS.

Management

The audit assessed how management responsibilities are defined and assigned, whether a planning process is in place, and how policies and procedures are communicated to staff.

The audit found that ITS responsibilities are assigned to SID and the management of the network to CMC/MSC; the relationships are defined in an architecture document which is being updated thus meeting the TBS Policy objective of assigning management responsibilities. The national ITS responsibilities are assigned to SID with 1.5 FTE dedicated to the coordination of this function. CMC/MSC plays a crucial role in ITS by operating ECONet, the backbone of the department's system and their staff possess much technical and operational expertise.

However the delivery and management of ITS in services and regions is **organizationally** dispersed among many staff who employ different practices. This results in inconsistencies in the application of ITS measures across the Department and in the roles and detailed responsibilities assigned to staff responsible for ITS.

The Department does have an Information Technology Advisory Committee (ITAC) in place to provide advice to the DG of SID. However, this committee is not linked to the business tables and consequently to the decision-making and management process of the Department. It was observed that given that CMC/MSC manages the departmental network, its role and standing at this committee does not appear commensurate with its responsibilities as manager of the network.

With respect to **planning**, there is no formal and integrated ITS national plan nor dedicated funds across the Department as called for in the TB Policy. While some program areas have formal plans, they are not identified and integrated into the annual planning process nor developed in consultation across the Department. The Y2K preparedness exercise reinforced the contingency and Business Resumption Planning (BPR); however, the updating process has not been subsequently implemented as also noted in the Audit of Security (2000) conducted by the Review Branch.

There are **linkages** within the Department between the ITS function and other administrative functions thus meeting this aspect of TBS policy specifications. However, these linkages are not as formal as they should be to ensure that all dimensions of ITS are systematically considered. The lack of formal linkages within the Department is partially demonstrated by the inconsistency in functional and organizational roles and responsibilities and the absence of a formal Department-wide ITS plan. External linkages with the RCMP and the Communication Security Establishment are adequate and maintained from a central point of contact in SID.

Some departmental policies and procedures can be found on the Intranet; EC meets partially TBS Policy requirement. However they are not **communicated** in a very effective manner. Thus unless personnel are frequently involved in the application of the ITS policies and standards, knowledge of them was generally quite low even if bulletins and directives are frequently broadcast through e-mail. In summary, the Department lacks a strategic approach to communicate, market and distribute information related to ITS to ensure maximum impact.

Overall, two key organizations are responsible for IT, SID and MSC; the roles and responsibilities of these groups are defined in an architecture document currently being updated; thus there is little chance that ITS gaps will be overlooked and system breaches occur. With respect to planning, ITS activities may not be addressed strategically and consistently on a departmental priority basis due to the absence of a departmental ITS plan.

In addition, the Department's timeliness of response may be slowed in emergency situations due to weaknesses and currency of contingency and BRP processes. The Department does have in place the decision-making and planning infrastructure to address this issue, namely ITAC and the business tables.

Risk Management

The purpose of a risk management approach in the area of ITS aims at having in place an adequate management methodology, procedures and the capability to ensure that decisions are based on adequate information and that new IT is developed under a common Department framework.

The audit found that SID has developed a risk management framework based on Treasury Board's Enhanced Management Framework (EMF) approach to be used for all new systems. This formal departmental risk management approach is not consistently applied throughout the Department for new systems under development nor used to revisit current operating systems. Several program areas have an excellent risk management strategy, including risk management methodology, procedures and capabilities, and rigorously apply it. Accordingly, some areas are able to make decisions based on adequate information. While the majority of programs report only using a risk management approach informally, program areas with critical systems do apply formal risk management.

The systematic use and monitoring of a risk management approach consistently throughout the Department for systems in place as well as systems under development is an issue in need of some attention. In fact, one third of those interviewed specifically commented on this as a weak point. It was also found that some threat and risk assessments (TRA) that had been initiated for new IT were never formally completed (e.g., Nemesis) and many TRA completed over five years ago are considered outdated. SID now employs a modified EMF and applies it to all new systems, and critical areas such as MSC use this framework, one can consider the degree of non-compliance with TBS specifications as of lesser concern.

Access to IT

The audit assessed whether the Department has procedures in place to control the authorization and access to IT systems. This includes access privileges for staff, the use of codes, keys and passwords. The study found that departmental policies and procedures for access are defined and implemented. However, the procedures related to the management of accounts are not consistent throughout the Department. Some areas monitor stale accounts and force periodic password renewal while others do it less regularly. In addition, staff do not consistently use password protection to prevent improper access to their own personal computer. It was also found that the password feature for screen savers, blackberries, palm pilots etc., is frequently left to the user's discretion and as a result often not applied. With respect to access to IT from home or from outside departmental buildings through the network, there is a standard procedure applied throughout the Department that exceeds TBS requirements. This procedure involves the use of a personal identification password in conjunction with an access control card (ACE). Overall, the procedures in place exceed TBS requirements; however, the account management procedures could be more consistently applied. Further details can be found under the heading *Communications Security*.

There is an opportunity to achieve greater assurance by consistently applying password protocols throughout the department. Areas with crucial and valuable information requiring a

24hour/7day operations do adhere to strict access procedures within and exceed the requirements for external access.

Monitoring of Security

The TBS policy objective states that departmental ITS should undergo a regular monitoring and review cycle as well as involve the RCMP to conduct a SEIT review. EC has called upon the RCMP in specific cases: the RCMP did a review of CCIW for new enforcement equipment installation due to relocation. MSC's Dorval facility does undergo annual assessment by facility management and RCMP's SEIT division is called in every 5 years. In addition, some internal examinations of ITS have also occurred. Ice Services did conduct a management-led audit last year for their unit. In 1991 the Review Branch also conducted a focused audit covering aspects of ITS. Nevertheless, no formal departmental RCMP\SEIT review has been conducted within the last ten years nor has one been requested. Although the past monitoring of ITS has not been comprehensive and does not meet TBS policy, the combination of specific important site investigations along with undertaking this current audit, should provide the Department with the necessary elements to update the ITS.

2. Personnel Security

In reviewing personnel security, interviewees were asked to comment on the following areas:

- the extent to which Statements of Sensitivity are completed and available for IT;
- the processes in place for screening new staff and revoking access privileges for departing staff;
- the measures taken to ensure users have adequate knowledge of ITS policies and procedures; and
- whether staff involved in the application and maintenance of ITS receive adequate training.

Statements of Sensitivity

Statements of Sensitivity are documents which indicate the confidentiality, integrity and availability requirements and are used to determine personnel access privileges to IT systems. Formally conducting this process provides assurance on access privileges. It was found that most program areas do not consistently or systematically complete Statements of Sensitivity, with the exception of CMC/MSC. As a result, EC does not meet TBS policy in this regard. The absence of a formal control framework which would provide assurance that systems, the network and applications have Statements of Sensitivity adequately completed, may explain this issue. Although no incidents were reported, greater assurance would be gained if such processes were to be employed.

System Access Rights and Screening Processes

Personnel who access IT systems should be appropriately screened and their access privileges adjusted based on their status. The screening processes for initiating and disabling user access are implemented and are in compliance with TBS policy. Some confusion exists around the application of basic and enhanced clearance for the purpose of extending access privileges to new users or special status users such as visiting scientists. In addition, no formal processes are in place for personnel who temporarily leave the organization on assignment. Overall, these processes could be improved by implementing an automatic link with Human Resource Systems (HR) to ensure that user status and access information remains up-to-date.

ITS Training (User Training, Maintenance and Application Training)

While some formal training is available for staff involved in the maintenance and application of ITS, most areas do not employ a formal training plan for their IT staff, and the training available is inconsistent across regions and programs. A significant number of employees interviewed expressed concern about the level of ITS user awareness. Specifically, it was noted that because of the limited training, awareness about potential threats is generally low. However, personnel in some areas, including Aviation and Defence (MSC), Policy and Communication (HQ), and Enforcement, are more aware of security issues generally and accordingly have more knowledge of ITS issues. Because those areas dealing most directly with sensitive information do have adequate awareness training, TBS policy is partially met. However, the low level of awareness and understanding of ITS in other areas of the Department could represent a potential risk that ITS could be compromised.

3. Physical Security

Evidence of adequate physical security measures associated with ITS including sprinkler systems, fire extinguishers, secure doorways (i.e., magnetic pass cards or locks), perimeter access controls, raised floors etc., was sought in reviewing physical security.

Physical and Environmental ITS Requirements

The physical security measures as observed by the audit team are generally adequate and the Department was found to be in compliance with TBS policy. Nevertheless, the Department IT zones are not consistently or uniformly secured since physical security measures vary by region and program. Some concerns were expressed about the current state of physical security within the Department. However, the possibility that IT assets will be lost or damaged due to the absence of consistent physical security for important infrastructure was considered low because adequate measures were observed at critical sites. CMC/MSC (Dorval) is considered to be a critical site within the Department as well as federally in the Quebec region, as it maintains information and equipment of significant value for delivering weather forecasts. Accordingly, the physical security measures employed at Dorval meet the specifications for a GWMC system.

4. Hardware Security

Issues related to disposal, maintenance, acquisitions, uninterruptible power supplies (UPS) and the associated policies and procedures are the criteria used to assess hardware security.

Hardware Security and ITS Requirements

The audit team found departmental policies and procedures are defined and implemented for hardware security including operational UPS for all MSC locations where they are required.

Hardware acquisition and inventory is not centrally controlled or planned in a uniform manner across the Department. Recording of IT assets in inventory systems is inconsistently applied. Some units, including Ice Services (MSC), Aviation and Defence (MSC), CMC in Dorval (MSC), the National Water Research Institute, the National Hydrology Research Institute, the Atlantic Region, and Policy and Communications (HQ), have standardized equipment within their organizations while others have not. Nevertheless, there are

recommended standard specifications for PCs issued by SID to ensure system compatibility. These issues of non-standardization may affect the ability of management to gain maximum advantage of equipment/hardware. Standardization is also a means to ease the provision of technical support.

Compliance with disposal and maintenance policies is generally good although security certification is not always required for systems repaired externally and internally. However, the potential for problems is considered low since the amount of secure information on equipment is minimal and private sector firms must protect their reputation. In addition, the disposal of hard disk drives using RCMP cleaning software is not universally applied across all regions and programs. Given that alternate software is used, the opportunity to divulge sensitive information appears to be unlikely. Overall the Department can be assessed as being partially in compliance with TBS policy for hardware security.

5. Software Security

The criteria used to review software security includes ensuring virus scanning tools are consistently activated; controls are in place to prevent the installation of unauthorized software; and related policies and procedures are defined and implemented.

Policies and processes for software security are defined and implemented. Processes for acquiring, monitoring, authorizing and installing software at the desktop are lenient in some areas and rigorous in others including Ice Services (MSC), Aviation and Defence (MSC) and Policy and Communication (HQ).

Some concerns were expressed about the current level of software security related to virus protection and the ability of users to install unauthorized software. While virus scanning and antigens are widely available, they are not consistently updated and enforced on all equipment, especially remote systems. It was noted that users do not update their virus software on laptops and home PCs with the same degree of diligence that is applied in the office. There is no departmental polling done on PCs and no systematic tracking of the licenses inventory, with the exception of the National Hydrology Research Institute. In addition, staff in many areas have the ability to download, acquire and install software that has not been previously approved.

Software security for the Department partially meets TBS policy. Yet, unauthorized downloads especially from the Internet can pose concerns in that an individual user has the potential to infect across the network. To reduce the possibility of such an event from happening, the Department currently applies virus detection at the PC as well as network server levels. Greater assurance could be gained by educating users of the risks and/or by better controlling the download capability. Given the increasing likelihood that software available through the Internet may carry brand-new viruses that might by-pass a virus checker, the responsibility for proper use of the system rests with the user community. Remote users who do not update their systems and undertake such downloads are more vulnerable to viruses and in turn may subject the network to an unnecessary level of risk. CMC/MSC does constantly monitor the ECONet but the opportunity for infection from exchange network servers remains.

6. Communications Security

The criteria used to assess compliance with respect to communications security includes an operational secure fax network, the absence of above A level secure information on the network and the use of ACE cards for remote access.

Although not all regions and programs had fully operational secure fax machines at time of the audit, the reviewers were informed that secure fax machines were scheduled to be fully operational by December 15, 2000. With respect to remote access, it was found that ACE cards are used consistently across programs and within the regions.

Approximately 47 percent of interviewees voiced concerns about the Department's communications security. The outstanding issue identified for communications security is the existence of above A level information on the network. Several interviewees reported seeing sensitive information on the network because of the lack of options for pursuing consultation in a timely manner to meet senior management deadlines. The transmission of secret and protected B level information was also reported in the Audit of Security, 2000 conducted by the Review Branch. As sensitive information on the network is an issue, the Department was found to only be partially in compliance with TBS policy. The practice of using the network for secure information increases the likelihood that leaks or interceptions could occur.

7. Operations Security

This section of the audit examines the policies concerning the network, its structure and operational procedures, including monitoring and other safeguards of the system. It is necessary to note that MSC Telecommunications Study currently in progress and due in March 2001 should provide more information on this issue.

Networks and Network Applications

The EcoNet network which supports both MSC programs and the whole Department is operated and managed by MSC. The CMC/MSC facility in Dorval operates a GWMC system and is also designated as a federal mission-critical site in the Quebec Region. MSC supplies the technical and operational expertise to ensure delivery of its weather program on a national basis and overviews network traffic and system irregularities in a 24hour/7day operation. Since regional operations are located in many offices across Canada and provide analysis and delivery of weather data, the network forms the critical infrastructure of MSC operations. The findings revealed that overall, network policies and procedures have been established and are adequate.

Monitoring network logs are a diagnostic and system/network management tool to identify irregularities in system use; it may serve to identify attempted system intrusions, as well as unauthorized system use. Such monitoring is sporadic and varies by service, region and site. There is no comprehensive departmental on-going monitoring which encompasses all system levels (Wide-Area Network, Metropolitan Area Network and Local Area Network). Network log monitoring allows the system administrators to conduct inspections. Inspections imply policing of the departmental Netiquette / Acceptable Use Policy, a task which has not been embraced by nor assigned to them. This type of monitoring is conducted on an exception basis where potential misuse is suspected. Intrusion monitoring at the ECONet level only occurs on a departmental basis at CMC/MSC in Dorval to ensure system safety

and integrity. CMC monitors the network and exercises its authority to take corrective action where threats may be imminent. Similar monitoring is in place at Aviation and Defence operations (MSC).

The audit found other weaknesses. There are some modems installed on networked PCs; this contravenes departmental policies. Some modems are used for legitimate purposes such as communicating with data monitoring equipment and are turned on only for the time of data transfer. The concern is that with an active PC and modem others can potentially tap into the connection and use it as a gateway into the system. In addition, there were instances reported where improper configurations of a PC set-up have occurred and did create holes in the firewall which then provided an open gateway into the network. Fortunately, no incidents of such entry have been reported. The issue is that there is no consistent monitoring for configurations of modems and open ports, as well as lax application of departmental policies. However, there are exceptions such as Research Institutes or Policy and Communication who closely monitor or as in the case of NHRC, control configurations. There certainly is an opportunity to strengthen and add consistency to network operations as they currently do not comply with TBS Policy. However, the active role played by MSC in global network monitoring does provide a reasonable level of safety and security to current departmental operations for the ECONet.

IT Contingency Planning and Departmental Needs

This section of the audit examines the policies and practices concerning business resumption and contingency planning.

The findings revealed that a departmental BRP, focused on EC's important IT systems, was undertaken in advance of Y2K. The results of the effort created a fairly comprehensive BRP, but unfortunately no procedures have been implemented to ensure that its information remains current. Updating such plans using its base of information becomes increasingly more costly as time advances. However, some services/regions have begun efforts to update but only for their individual areas; efforts for a current collective plan are not underway.

In addition, there is no departmental process for monitoring and testing Contingency and BRPs. Most contingency planning is largely MSC program-specific and this is due to its GWMC status. MSC has active contingency plans, and procedures in place. Its operational requirements dictate that it employ appropriate alternate power supplies (UPS), and contingencies for mirror sites if technical problems cause a weather centre to suspend operations. Similar findings were reported in the Audit of Security, 2000 conducted by the Review Branch.

There is an opportunity to maintain currency to business resumption and contingency planning since at present the Department only partially complies with TBS policy. However, the role played by MSC in applying contingency planning as an active element of its daily operations does provide the level of secure operations commensurate with its function. Many regions/services do have less formal contingency procedures and thus are not totally unprotected. Policy and Communications has developed its own operational contingency plans independent of the Department.

Based on the earlier findings and the management response contained in the Audit of Security, 2000, the Departmental Security Officer will appoint a central point of contact

responsible for the monitoring and updating of business continuity and resumption plans on an annual basis. Such actions should lower the level of risk by ensuring a consistent effort across the Department.

Other Issues

During the conduct of the audit, information was obtained about the Department's effort with respect to **GOL**. Interestingly, security was a frequently raised issue.

> *The need for e-government is now broadly accepted. Governments are wrestling with practicalities, such as priorities, costs, speed, who does what, organizational and HR impact, and public profile* .[3]

Interviews noted that increasing and maintaining security was important because certain departmental business information will require increased safeguards. A balance between security and client access will have to be sought. As well some level of authentication of data will have to be featured to provide assurance of its source and validity. The question of resourcing will need attention with respect to increased client contacts and system connections. This will necessitate greater investments in both staff and infrastructure. Other commentary noted that currently GOL was still very conceptual and lacked clear operational connections and implications. The roles of both public and private sectors will need clarification and central agency policies such as those of Treasury Board, will have to be amended to ensure compatibility with this the "new way of doing business". Scientists will also have to undergo a paradigm shift in adjusting their view and ownership of data.

Compliance with **official languages** requirements is part of all audits or reviews. Although many services/regions reported no major problems, some issues were raised. One weakness was the lack of French in internal communication with the Quebec region. For example, some of the departmental virus announcements are not bilingual when distributed to the Quebec region; some e-mails with the Quebec region arrive only in English noting that the French version is to follow but this does not always happen.

The Internet is increasing the pressure for entire reports to be bilingual, a capability that cannot be easily supported by researchers and results in costly translations and associated delays. This situation was noted whether the originator's language was English or French.

Other potential concerns in this area include: the number of bilingual staff in the Atlantic region (only the director position); and, the demand for the provision of MSC services in French to Iqaluit is likely to increase demands to the PNR since this site was previously serviced from the Montreal office.

The audit found that electronic technologies and increased pace in communications result in English becoming more and more the predominant language. This is not due to the technology itself (i.e. the software) but to the way communications are conducted by the user community. The observation that was made in the Review of Office Technology, completed

---

[3] David Prime , Auditing and risk in a e-business world, IIA Ottawa Chapter Internal Auditors in Government Conference, October 16, 2000

in April 1999, still holds true today that *"Consideration should be given to ensure that both official languages are used in greater frequency by the businesses and programs using the technology, where appropriate."*

Recommendations

EC operates successfully a GWMC system in MSC and has built its network on this system, thus providing a level of ITS commensurate with the operational requirements of this type of system. Although the Department generally meets partially most of the objectives of the TBS Policy, the improvements recommended below would bring the level of compliance more in line with the TBS Policy and would better support EC's objectives. The overall findings and the analysis led the audit to submit the following recommendations under the categories of management, communication and training and tools.

Management

Recommendation #1

The Department has in place the decision-making infrastructure, namely the business tables and ITAC, to improve the management and administration of ITS as well as to ensure consistency in policy and procedures application and monitoring across the Department. The business tables are the key decision points of the Department and ITAC is composed of the most senior informatics advisors, experts and managers. However, currently ITAC is not currently aligned with reporting to Management, Administration and Policy (MAP) table. Given that CMC/MSC plays an important role network's structure, a realignment of its role on ITAC should be considered. The adjustment of the reporting relationship has already been noted in the Review of Office Technology conducted by the Review Branch in 1999.

It is recommended that the ADM of Corporate Services in consultation with the ADM of MSC review the role of ITAC. This review should include: a revised mandate for the committee and its sub-committees; a change in the reporting relationship of the committee; and an examination of membership and roles to ensure all stakeholders are appropriately represented.

This recommendation should be implemented in 2000-2001 with minimal costs.

Recommendation #2

Although roles and responsibilities between SID and MSC are defined and being updated, the dispersion of responsibilities across the Department has led to fragmentation in the management and administration of ITS across the Department and as a result departmental policies and procedures are inconsistently applied. A review and redefinition of roles and detailed responsibilities would be beneficial to increase policy compliance and improve efficiency. The accountability structure between the following positions and organizations should be included in this review:

- ITS Headquarters and the Regions;
- Business lines within Headquarters,
- SID and the Regions;
- Government On-Line secretariat; and

- SID and the Departmental Security Officer (DSO).

It was found that some programs or regions employ excellent practices while others partially meet policy requirements. If all the best practices currently employed in parts of the department (outlined in Annex 2) were to be come universal, there would be much progress to improving ITS as well as increase departmental compliance with TB Policy.

It is recommended that the DG of SID undertake to strengthen the management framework for ITS in the department. This would include: greater clarification of roles and responsibilities of ITS; improved coordination and consistency in policy application and procedures; enhanced ITS planning; and, reporting.

This recommendation should be implemented in 2000-2001 with minimal costs.

Communication and Training

Recommendation #3

Within the Department one key to achieving good ITS practices is the user community. With the exception of a few select areas, user awareness was identified as a key factor in improving ITS. Users tend to have little or no ITS training and awareness about potential threats is also generally low. In addition, the existing policies and procedures have, in many instances, a low impact on the user community. This is mainly due to a lack of communication/marketing strategy of ITS.

A comprehensive Department-wide IT awareness program tied to a communication/marketing strategy should include the following attributes:

- one website with all ITS policies & procedures;
- improved information packaging and messaging to increase the impact on users and ensure a consistent message across the Department (e.g., periodic refreshers; regular updates to cover new technology done in conjunction with other training; and potential for computer-based module on on-line training); and
- mandatory training for all employees; (e.g., a specialized package for visiting scientist/students; an orientation session).

Any actions should be linked to the development of the existing commitment for the DSO launch of a department-wide security awareness program at EC. Given the wide range of responsibilities, it would be prudent that all appropriate parties be consulted in the preparation stages.

It is recommended that the DG of SID, in consultation with the Director of Informatics at MSC, the DG, HR and the Departmental Security Office (DSO), develop an ITS awareness/ communication/ marketing strategy.

This recommendation should be implemented in 2000-2001; the cost should be assessed by SID DG including the DSO.

Tools

Recommendation #4

Monitoring is required in order to ensure processes and procedures are adhered to and implemented consistently on a departmental level in order to facilitate the detection of ITS breaches. To achieve an increased degree of assurance, stronger monitoring is required in the following areas:

- ITS logs
- built-in mechanisms related to the implementation of policies and procedures such as sign off sheets for Threat and Risk assessments.

The need for external audits (RCMP) should be assessed by ITAC and the decision made at the MAP table.

It is recommended that the DG of SID, in consultation with ITAC members, review options to implement appropriate software to monitor ITS logs on a departmental level.

This assessment should be conducted every two years, starting in 2002-2003, thus giving sufficient time to implement the recommendations of this audit. The costs should be evaluated by the DG of SID.

Recommendation #5

The Department lacks efficient and effective digital tools for handling sensitive information. Personnel handling sensitive information may not be aware of alternate communications methods available and may not have adequate information to make an informed decision when electronically transmitting sensitive information. Additionally, alternate communication tools, such as secure fax machines have only recently been made operational. This has led to a situation where sensitive information is not consistently transmitted in a secure manner. Staff need secure and efficient tools to consult rapidly their colleagues across the Department and meet the short deadlines of senior management. Staff should have tools to allow them to communicate sensitive information as efficiently as they do with regular documents. The pilot project to implement secure messaging by 2001 using PKI is certainly one step to a longer term solution. However, steps towards improved security by examining OGDs as well as educating users of risk avoidance options may, in shorter term, result in tangible improvements.

It is recommended that the DG of SID, in consultation with the Director of Informatics at MSC and the Departmental Security Office, identify and make available improved electronic tools to facilitate the transmission of secure communication.

This recommendation should be implemented in 2000-2001; the cost should be assessed by the DG, SID and the DSO.

Management Response **(See Executive Summary)**

Conclusion

Overall Environment Canada partially meets most of the objectives outlined in the TBS ITS Audit Policy (1995). For EC, IT is an integral part of its operations but focus and profile of its attendant ITS has not received commensurate attention. The Department has been applying security measures but not as consistently and comprehensively as stated in policies. Some areas fall short while others exceed policy requirements. Security awareness at all levels as well as clear accountabilities cloud effectively addressing many of the ITS issues.

As dependence on the electronic environment increases through growth of WEB sites and GOL, it is important to address current weaknesses or inconsistencies for the network and its users. The network can only be as strong as the weakest link and the key element is the user. For this reason, addressing the identified areas for improvement in a timely fashion is of great consequence. The effort should focus on the following:

- improving the Department's ITS - effectively reducing the current identified weaknesses before they become increasingly costly to adjust;
- bringing the Department into greater compliance with the TBS Security Policy; and
- placing the Department in an improved position to move forward safely and securely with GOL initiatives.

Annex 1 List of Supplementary Documents for IT Security Audit

Note: Supplementary documents may not be available in both official languages.

1. Methodology of ITS Audit
2. Bibliography of ITS Audit
3. List of Interviewees for ITS Audit
4. Results of Focus Group - Risk Statements

Annex 2 List of Best Practices

Roles and Responsibilities

Security management responsibilities are clearly established, defined and assigned in structure and in function to the network managers.

ITS is assigned to a staff member who is responsible for developing a consistent set of policies and procedures that will be applied across the regions and for developing an implementation plan. These responsibilities are reflected in the IT Security Officer's job description.

IT Security Awareness

IT security awareness sessions are held several times a year with periodic mailings and a central location outlines security policies.

IT staff participate in the program management teams which is also conducive to communicating security issues.

A written user introduction kit is available to new system users.

A comprehensive information kit (video and CD ROM) outlining all IT security aspects has been assembled and tabled at the November, 2000 meeting of ITAC.

Planning

Policy information is currently being collected from all the region in order to create a uniform plan that is kept updated. The staff member responsible for ITS develops this plan.

IT and ITS is coordinated and planned as a central service common to the user community and reports to a management committee for direction/control.

For all new projects, a project charter is developed, which includes IT security requirements. A project may not proceed until the project charter has been completed.

Contingency and Business Resumption Planning

A full contingency plan has been developed and is tested and kept up-to-date

Risk Management

A mandatory risk management assessment is done for all systems. A life cycle approach is always utilized and followed by the development group

Physical Security

Servers and systems of value are maintained in a secured computer room with temperature and humidity control with access controlled by magnetic pass card, which registers the

owner of the pass card and the time of entrance to the room. The computer room has a UPS system for power fluctuations or outages. Commensurate fire protection (sprinklers, extinguishers) are supplies current and in place.

Software and Network Security

The use of software is limited to the configurations of the system. This process ensures that unauthorized software cannot be installed on the system. This procedure also safeguards the network.

Monitoring

Periodic security sweeps are performed. When issues are identified (e.g., computers are found left on, documents unsecured or cell phones in the open) the individual responsible is given additional training.

ITS inspections by the RCMP or by a private firm were arranged to verify computer and network set-ups with subsequent adjustments.

Periodic reviews are undertaken to monitor the server logs for suspicious activity.

Repair and Disposal of Hardware

Secure information is only stored on the system and not on PCs or lap tops.

Property tag system is used and, should an attempt be made to modify the hardware (e.g. ram chip is removed), an alert is activated.

External repair technicians are brought in and supervised until they finish their work. They are not provided with passwords or pin numbers.