Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Security Audit - June 2002

Published: 2002-00-01

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-28/2002E-PDF
ISBN: 978-0-660-25354-1

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Vérification de sécurité - juin 2002

Security Audit - June 2002

Security Audit
June 2002

Table of Contents

1.0 Executive Summary

The purpose of this audit was to express an opinion on the compliance of the Treasury Board Secretariat (TBS) in implementing the security standards of the Government Security Policy (GSP) and its operational standards, and to assess the efficiency and effectiveness of TBS' security program. The scope of this audit included an assessment of the policies, procedures, processes, systems and controls included in TBS' security program. The Department of Finance was not included in the scope of this audit even though many corporate services are shared between TBS and Finance.

The audit approach for this audit was based on the Audit Guides developed for the GSP and the Information Technology Security (ITS) operational standard. The audit guides were developed as guidance to the internal audit community in conducting audits of the implementation of the GSP and the ITS operational standard. The GSP was reissued in February 2002, however as the accompanying operational standards and audit guides will not be completely updated in the near future it was decided to audit the TBS against the July 1994 GSP. We reviewed the new GSP and believe that all of our findings and recommendations are still relevant under its provisions.

During our interviews and testing, we identified that TBS' security program is in full compliance with seven (7) of the thirty-two (32) audited control objectives, and are partially compliant with an additional twenty four (24) control objectives, however, for nine (9) of these, the department has appropriate procedures in place but they were not adequately documented. There was one control area where TBS was found to be non-compliant. We have identified the need for remedial actions to improve the efficiency and effectiveness of TBS' security program. On the basis of the deficiencies, it is our opinion that TBS's security program is not in full compliance with the GSP and its operational standards.

We have provided recommendations in section 4.0 to address the areas of partial or non-compliance to the GSP and its operational standards identified during our audit. Our findings are difficult to categorize, as many of them are high-level issues that affect all elements of TBS's security program. However, prevailing themes found throughout our audit was a lack of formal procedures, infrequent performance of internal security reviews and investigations, and inadequate documentation. As a result, we believe that TBS' ability to understand and address its varied security weaknesses and vulnerabilities may be compromised. We recommend that the following areas be dealt with immediately - timely investigations of security incidents, judicious preparation of threat and risk assessments, and the development of a formal self-assessment process. In developing responses to these issues, management should take into consideration that resource constraints was a common reason provided by our interviewees for TBS' non-compliance to the GSP.

Management Response:

We accept the findings and recommendations of the Internal Audit on compliance with the Government Security Policy (GSP), and on the whole, we view it as a useful management tool for improvement. While the audit found that there were areas of partial non-compliance, in most of those areas the department has lived up to the spirit of the policy requirements, but has not documented formal procedures in the manner required by the GSP.

In some areas the recommendations can be easily implemented and indeed, work has already begun to address many of the issues identified in the audit. For example, the Security Services Division has already instituted a new process to formalize the process of investigating security breaches and violations, and discussions have begun regarding the development of a self-assessment program. TBS will continue to incorporate a risk-based methodology in the deployment of threat and risk assessments (TRA), and maintain the focus on higher risks areas. However, the department will strive to bring more rigour to this process in the future.

TBS is committed to bringing itself into full compliance with the new GSP and we will adjust our policies and practices as the revised operational standards become available. While we do not feel that any area of TBS is unduly exposed to risk, we are committed to rectifying the weaknesses identified by the audit. All the recommendations will be implemented by the end of 2002-03.

2.0 Introduction

2.1 Background

The Treasury Board Secretariat (TBS) approved the Government Security Policy (GSP) and Standards document in December 1989. The GSP was initially designed to provide security standards for departments' organizational, physical, personnel and information technology programs. In June 1994, the GSP was updated to reflect recent changes in the Canadian and global economies, and to address policy and operational standards governing contract and contingency management. The GSP was recently reissued in February 2002, however as the

accompanying operational standards will not be finalized in the near future it was decided to audit the TBS to the new GSP.

To assist departments in performing internal audits to assess their compliance with the GSP and its standards, the TBS developed the following audit guides:

- *Guide to the Audit of Security (GAS), 1990 (revised June 1996), and*
- *Audit Guide on Information Technology Security (ITS), September 1995.*

The purpose of the audit guides is to provide guidance to the internal audit community in conducting audits of the implementation of the GSP and the information technology security (ITS) operational standards. Specifically, the guides are designed to assist organizations in assessing:

- departmental *compliance* with the GSP and *ITS* operational standards;
- the *effectiveness* of implementation of the GSP and ITS operational standards; and
- the *efficiency* of implementation of the GSP and ITS operational standards.

The last security audit for the TBS was conducted in March 1994.

2.2 Audit Purpose

The purpose of this audit is to express an opinion on the compliance of the TBS in implementing the security standards of the GSP and the ITS operational standards, and the efficiency and effectiveness of TBS' security program. In areas where non-compliance or security weaknesses were identified we have provided recommendations for minimizing security vulnerabilities and increasing the efficiency and effectiveness of TBS' security program.

2.3 Audit Scope

The scope of this audit included an assessment of the policies, procedures, processes, systems and controls included in TBS' security program. The Department of Finance was not included in the scope of this audit even though many corporate services are shared between TBS and Finance.

Our audit comprised the totality of TBS' security program, which encompasses the following divisions or groups:

- Security Services;
- Informatics;
- Records Management;
- Facilities;
- Telecommunications;
- Contracting; and
- Orientation / Human Resources.

2.4 Audit Approach / Methodology

The audit approach for this audit was based on the Audit Guides developed for the GSP and the ITS operational standard.

Our audit approach and methodology included the following audit procedures:

- Review of documented security policies and procedures and other documentation supporting TBS' security program;
- Interviews with key personnel responsible for managing security;
- Review current processes for administering and monitoring security;
- Where appropriate, perform sample testing to determine whether security activities were performed as intended;
- Assess the current security processes against the security objectives to identify gaps; and
- Provide recommendations for activities to address the gaps.

A listing has been provided in Annex A of the TBS employees we interviewed, or performed testing with, as part of our audit.

2.5 The Government Security Model

Security is often described as the protection of people, sensitive information, and material assets from threats using safeguards designed to ensure their *confidentiality, integrity*, *availability* and *well-being.*

The GSP and operational standards were designed with the expectation that departments would develop a departmental security program model with the following components:

- Organizational structure;
- Administrative procedures; and
- Five sub-systems:
- Physical security,
- Information technology security,
- Personnel security,
- Security and contingency management, and
- Security and contracting management.

The efficiency and effectiveness of the security program depends upon the performance of each of these elements independently and together with each other. Therefore, where responsibility for the various sub-systems is assigned to different organizational units or where it is decentralized, the sub-systems should be structured to provide for a coordinated approach to planning, management and administration.

The Assistant Deputy Minister, Corporate Services Branch, has been named as the senior official to coordinate and direct the ongoing implementation of the GSP and its operational standards for TBS. Management of the security program is the responsibility of the Director, Security Services Division (SSD).

3.0 Audit Results

The audit has been designed to provide senior management with an assessment of the current compliance, effectiveness and efficiency of the TBS security program in relation to the GSP and its operational standards. Provided below is our overall assessment of TBS' compliance with each audit objective provided in the audit guides. As we identified a number of areas requiring improvement, it is our opinion that TBS's security program is not in full compliance with the GSP and its operational standards. TBS' partial or non-compliance with some of the audit objectives identifies the need for remedial actions to improve the efficiency and effectiveness of their security program. Specific details on the security vulnerabilities and weaknesses identified, and our recommendations, are provided in section 4.0.

3.1 Guide to the Audit of Security - Audit Objectives

Audit Objective	Was Objective met?			Recommendations	
	Yes	Partially	No	P&P(1)	Other
Security Organization					
1. Ensure that a security management structure is in place which encompasses responsibility for the overall management of the department's security program, including administrative, physical, information technology and personnel security and security and contingency and contracting management, and that it meets the needs of the department.	X				
Security Administration					
2. Ensure that the DSO [Departmental Security Officer] has implemented an effective security program that is an integral part of the overall departmental program and that meets the requirements of the GSP and Operational Standards.		X		4.1	
3. Ensure that effective security education and training programs are in place.		X		4.1	4.2
4. Ensure that sensitive information and assets are classified and designated according to the GSP and Operational Standards and that classifications and designations are downgraded or removed when the information and assets are less, or no longer, sensitive.		X			4.3, 4.4
5. Ensure that safeguards applied for the protection of sensitive		X		4.1	4.5, 4.6

information, assets and employees are based on mandatory standards and a risk management methodology.					
6. Ensure that possible breaches of security, security violations and other security incidents are investigated, that action is taken to minimize loss and that appropriate administrative or disciplinary action is taken, if warranted.		X		4.1	4.6
7. Ensure that appropriate safeguards are applied to sensitive information shared with, or received from, official sources outside the department.	X				
Physical Security					
8. Ensure that consideration is given to locating and designing facilities to reduce or eliminate the threats and risks to which sensitive information and assets and employees in the facilities will be exposed.		X		4.1	4.7
9. Ensure that appropriate physical safeguards are in place at facilities to provide for the safeguarding of sensitive information and assets.		X		4.1	4.7
10. Ensure that appropriate physical safeguards are in place at facilities to provide for the safety and security of employees.	X				
11. Ensure that physical safeguards are reviewed and tested periodically.			X		4.7
Personnel Security					
12. Ensure that the security screening of individuals is carried out according to the GSP and Personnel Security Standard.		X		4.1	
13 Ensure that required screening levels are authorized, denied and revoked according to the GSP and Personnel Security Standard and that this is done in a fair and unbiased way.		X		4.1	
14. Ensure that, when it is decided to terminate [discharge or transfer] an individual's employment, it is done in a way that reduces or eliminates any risk to the department's sensitive information and assets and essential systems.		X		4.1	4.8
Security and Contingency Management					
15. Ensure that managers of facilities throughout the department have taken the necessary action to protect sensitive information and assets and employees during all types of emergencies.		X		4.1	4.9
16. Ensure that department-wide plans are developed to provide for the resumption of essential business operations following an unplanned interruption.		X		4.1	4.9
Security and Contracting Management					
17. Ensure that security requirements are included with other requirements in contracts when they involve access to sensitive information and assets.		X		4.1	

3.2 Audit Guide on Information Technology Standard - Audit Objectives

Audit Objective	Was Objective met?	Recommendations

	Yes	Partially	No	P&P(2)	Other
Organizing and Administering ITS					
1. Ensure that an ITS management structure is in place and meets the needs of the department.		X		4.1	
2. Ensure that ITS safeguards are implemented, maintained, monitored and adjusted, within a risk management environment.		X			4.2, 4.10
3. Ensure that the information technology (IT) resources are appropriately managed.		X			4.7
4. Ensure that ITS equipment is appropriately managed, repaired, maintained and disposed.		X		4.1	4.7, 4.10
5. Ensure that cryptographic materiel is appropriately managed, repaired, maintained and disposed.	X				
6. Ensure that departmental ITS undergoes regular monitoring and review.		X			4.7
Personnel Security					
7. Ensure that personnel having access to IT systems/networks/ applications that process, transmit or store sensitive information are appropriately screened before being given access and are aware of their security-related responsibilities.		X		4.1	4.2
Physical Security					
8. Ensure that IT is developed and maintained with consideration given to its physical and environmental security requirements.		X			4.7
Hardware Security					
9. Ensure that IT is developed and maintained with consideration given to its hardware security requirements.		X		4.1	
Software Security					
10. Ensure that IT is developed and maintained with consideration given to its software security requirements.		X		4.1	
Communications Security					
11. Ensure that IT is developed and maintained with consideration given to its general communications security requirements.	X				
12. Ensure that networks and network applications are developed and maintained with consideration given to their security requirements.		X		4.1	
13. Ensure that IT is developed and maintained with consideration given to electronic authorization and authentication (EAA) security requirements.	X				
14. Ensure that IT is developed and maintained with consideration given to emanations security requirements.	X				
Operations Security					

15. Ensure that ITS operations are in place and meet the needs of the department.		X		4.1	

4.0 Recommendations

The following recommendations were developed to address the security weaknesses and vulnerabilities identified during our audit of TBS' security program. Throughout our audit, we found that resource constraints was a common reason provided for TBS' non-compliance to several aspects of the GSP.

4.1 Departmental Policies and Procedures

The GSP and its operational standards were developed as a general guide, and were designed with the expectation that each department would develop detailed policies and procedures for each area in their security program. The TBS security program utilizes the GSP and its operational standards, however in many areas they have not developed departmental specific policies and procedures, or the current policies and procedures are outdated. Provided below is a list of some of the areas in which departmental policies and procedures need to be developed:

Guide to the Audit of Security:

- Risk Management and the Preparation of Threat and Risk Assessments
- Reporting, Investigating and Resolving Security Breaches, Violations and Threats
- Assessing Security Requirements for New or Renovated Sites and Preparing Security Briefs
- Managing and Monitoring Operation of Physical Security Elements
- Granting, Denying and Revoking Security Clearances
- Retrieving and Protecting Corporate Assets from Discharged Employees
- Updating and Testing Business Resumption Plans
- Refining Security Requirements for External Contracts and Monitoring Compliance

Audit Guide on Information Technology Standard:

- Planning, Implementing and Maintaining Information Management and IT
- Management, Repair, Maintenance and Disposal of IT equipment
- Maintenance and Monitoring of System Access
- IT Security - Policies and Operational Procedures

We would recommend that a project be initiated to develop departmental policies and procedures for all security elements identified within the GSP and its operational standards. The development of these policies and procedures should include all related divisions within TBS. Once completed, the policies and procedures should be made easily accessible to applicable personnel, and accountability should be assigned for maintaining the policies and procedures.

Management Response:

SSD will continue to use the Government Security Policy as a general guide and will develop detailed policies and procedures on an as required basis to meet specific needs (i.e. Policy on the Use of Electronic Networks) or when it is determined through a Threat and Risk Assessment that more detailed policies and procedures are required. All new policies and procedures will be made available electronically to employees using TBS' Intranet (InfoSite).

4.2 Security Awareness and Training Program

The GSP requires departments to ensure that individuals who have specific security duties receive appropriate, up to date training. In addition, a security awareness program should be established to inform and regularly remind individuals of their continuing security responsibilities, make them aware of recent threats to sensitive information and assets, and inform them of changes to security policy and procedures. SSD does not have a formal security awareness or training program. Specific training requirements are determined through each individual's annual performance evaluation, however these requirements are not necessarily linked back to the direct needs and requirements of the security program. Security awareness is partially provided through security briefs to new employees, and irregular security bulletins, however a formal strategy has not been developed and no subsequent training is provided, except in isolated cases (i.e. Internet Acceptable Use Policy).

We recommend that SSD implement a formal security awareness and training program. The program should be designed to support SSD' strategic vision, and address current security needs and requirements. In addition, a repository of security bulletins and alerts should be created on the intranet and be accessible to all security

personnel. Establishment of a formal security awareness and training program would help to educate employees, including security personnel, on the division of responsibilities within the security program and current vulnerabilities and threats faced by TBS.

Management Response:

SSD will implement a Security Awareness and training program to support current security needs and requirements by the Fall/Winter 2002. The Security Awareness and training program will be expanded upon as the revised GSP operational standards become available. Security bulletins and alerts will be posted on the Intranet (InfoSite) that is accessible to all employees.

4.3 Records Management - Multiple Volume Dockets

TBS' Records Management group utilize multiple volume dockets, in which the whole set of volumes is classified according to the highest classified document in the dockets. This practice, although common practice at one time, is now in contravention with the GSP, as it results in the over classification of information.

We recommend that the Records Management personnel discontinue use of multiple volume dockets and store documents based on their original classification.

Management Response:

The use of multiple volume dockets will cease immediately. All new material will be stored based on their original classification.

4.4 Records Management - Downgrading or Declassification of Information

The Documentation Classification and Designation Guide clearly specifies that classified and designated matter should be kept under constant review and downgraded or declassified by authorized persons as soon as such action is warranted. Although TBS has developed a declassification schedule for a number of documents, the declassification has not been performed.

We would recommend that the declassification schedules in the Document Classification and Designation Guide be reviewed and approved by the authorized person(s), and appropriate actions be taken to downgrade documents as determined in the schedule.

Management Response:

Originators or designated authorities are responsible for the declassification and downgrading of documents. Therefore, we will advise originators about the requirement to follow the practice for classification, declassification and downgrading outlined in the Document Classification and Designation Guide. Future Information Management practices will include consultation with clients to establish declassification dates for new classified material.

A review is expected to commence in the fall of 2002 to update the existing Classification and Designation guide. The guide, which currently exists in paper format only, will be made available on the Intranet in electronic format so that all employees may have access.

4.5 Preparation of Threat Risk Assessments

A requirement of the GSP is that departments must conduct ongoing assessments of threats and risks to determine the necessity of additional safeguards. This would involve updating the assessment for any changes in the threat environment such as a breach of security or other serious security incident, or a change in the sensitive information and assets being protected. Although SSD supports the preparation of Threat Risk Assessments (TRA), there are several instances where resource and time constraints have impeded their preparation of a full TRA and heavier reliance was placed on less-rigorous vulnerability assessments. In addition, TBS is still placing reliance on outdated TRAs that should be updated. For example, the network TRA was prepared in September 1995. Although the network configuration may not have changed considerably since 1995, the threat environment has changed and therefore additional risk areas may need to be considered by TBS.

We recommend that a project be initiated by SSD to ensure that complete and updated TRAs are completed for all operational activities affecting the safeguarding of employees and/or assets, including facility renovations, the introduction of new or modified systems, networks and applications, and any additional changes in the threat environment. The preparation of TRAs should be included in the security awareness program, to ensure that all personnel, including those in the Informatics, Telecommunications, and Facilities divisions, are

appropriately educated on the requirements for a TRA, and can involve SSD in development projects, as appropriate.

Management Response:

In the past, SSD has completed threat and risk assessments for those issues that present the greatest risk to TBS and performed high-level reviews for those issues that present a lesser risk. SSD will review its current practices and make adjustments as soon as practical.

In addition, SSD will be actively involved in the Integrated Risk Management process for TBS to ensure that SSD has a true appreciation of the risks facing TBS. Full TRAs will be completed for all high-medium risks faced by TBS. High-level reviews will continue to be completed for low risks.

4.6 Investigation of Security Breaches and Violations

An important element of a department's security program is the investigation and resolution of all security breaches and violations. It is through these follow-up activities that the department can better understand changes in their threat environment, and react quickly to mitigate security threats and vulnerabilities. Although TBS has experienced very few security breaches or violations, we observed that comprehensive investigations are not being conducted on a timely basis, and detailed security reports are not consistently prepared, for those incidents, which do occur. As a result, security threats and vulnerabilities may persist undetected.

We recommend that a process be developed for tracking, investigating and resolving security breaches and violations. A procedural manual should be developed which outlines the required steps for each reported item, and includes standard templates for documenting the initial notification and resolution of the security breach or violation. This process should include the preparation of a threat and risk assessment, if deemed necessary. Senior Management should be involved in reviewing and approving the actions taken to ensure they are appropriate for the case under review.

Management Response:

SSD has already addressed the issue of tracking, investigating and resolving security violations and breaches by developing the required templates. Senior management will continue to become involved in the review of serious security incidents.

4.7 Physical Security Requirements

Physical security was defined in the GSP as an integral part of a department's security program. Physical security involves the proper layout and design of facilities and the use of measures to delay and prevent unauthorized access to government assets. During our audit, we identified a number of areas in TBS' physical security program that should be addressed.

(a) Facility Design:

The GSP specifies that departments must ensure that security is fully integrated in the process of planning, selecting, designing and modifying their facilities. This process should include the preparation of security site and design briefs, continued involvement during the design stage, and physical inspections prior to site occupation. Currently, the SSD has minimal involvement in determining security requirements of facility designs. They are usually not involved until the end of the design process, and do not prepare security briefs, or perform physical inspections of completed sites. During our interviews, we found that the roles and responsibilities between SSD and the Facilities Division were unclear, and that increased involvement of SSD in facility design was needed.

We recommend that the roles and responsibilities between SSD and Facilities be clearly defined and agreed upon by both Divisions. Specifically, responsibilities should be defined for determining security requirements for facilities designs, identifying physical safeguards of remote locations, and approving site designs. To foster a collaborative relationship between these two divisions, regular status meetings should be held to discuss upcoming projects, identify priorities and develop action plans. As a solution to the current resource constraints, a Physical Security Officer should be appointed within SSD. This individual should act as the SSD representative on all facility projects, and be responsible for reviewing facility designs, creating security briefs and inspecting facility sites. As required, the Emergency Preparedness Office and Occupational Health and Safety Officers should be involved in facility projects in order to provide guidance on health and safety issues related to facilities, and knowledge of all related codes, policies and standards.

Management Response:

ASD and SSD will work more collaboratively to define roles and responsibilities for determining security requirements for facility design, identifying security safeguards and approving site designs. Regular meetings between SSD and Facilities have been occurring since the fall of 2001. SSD will review the requirement for a dedicated Physical Security officer.

(b) Key Management:

A number of TBS' restricted zones are protected using non-approved key sets that utilize replicable keys. As a result, the keys can be easily replicated and the appropriate safeguarding of the grandfather or root key cannot be assured. In addition, many of the facility keys are stored in a weakly secured area. These vulnerabilities increase the risk of sensitive assets and information being compromised.

We recommend that one group perform management of all facilities' keys. The keys should be secured in an appropriate container, and access restricted to a few individuals. An authorization table and sign-out log should be used to manage the distribution of all keys. The facilities' door locks for restricted areas should be changed to approved key sets that utilize non-replicable keys.

Management Response:

SSD will complete a review of keyways used for restricted areas to ensure that they are appropriate for the area being protected. It should be noted, however, that all sensitive restricted areas within TBS are alarmed after hours, minimizing the need for high-security locksets. SSD will also work with ASD on key handling procedures for offices.

(c) Combination Mechanical Locksets:

Access to several of TBS' restricted areas, including the data centre, cable closets and server rooms, is controlled through the use of combination locksets. There are no policies or procedures outlining the security controls for combination locksets, including a specification of the duration that a combination can be active. As a result, the combinations are changed infrequently, and are not always changed when employees leave the department. This increases the risk of sensitive assets and information being compromised.

We recommend that a formal policy be developed that requires the combinations for locksets be changed on a periodic basis (i.e. six months). As a precautionary measure, we would also recommend that the combinations be immediately changed following the departure of an employee with knowledge of the combination or upon occurrence of a security breach.

Management Response:

The issue of changing the combination on Unican/mechanical type locksets will be addressed in the Security Awareness program. Again, sensitive restricted areas are protected by an intrusion alarm system after hours which mitigates much of the risk identified in the audit report.

(d) Internal Reviews of Physical Safeguards:

The GSP identified that continuous review of physical security safeguards is essential to reflect changes in the threat environment and take advantage of new cost-effective technologies. Due to resource constraints, there have been no recent internal tests or reviews of the physical security plans, procedures or systems by SSD. The last security audit was conducted in March 1994, and SSD management was not aware of any recent external agency audits (i.e. RCMP, CSIS), excluding the annual COMSEC audit by CSE.

We recommend that SSD and Internal Audit co-develop a self-assessment program to ensure a periodic review of the various elements of the security program, including the physical safeguards. The audit program should be developed from a risk perspective, taking into consideration the current threats and vulnerabilities of the TBS, and consist of internal self-assessments and reviews, and periodic independent audits.

Management Response:

SSD will consult with Internal Audit and they will jointly develop a self-assessment program by the end of 2002-03.

4.8 Retrieving Corporate Assets from Discharged Employees

During the last year, the Orientation Centre and SSD have prepared an employee discharge checklist. The checklist was designed to ensure that all corporate assets, including access cards, communication equipment, lap top computers, and keys are collected from employees leaving the department. During our interviews, it was identified that this checklist is not being used consistently for all employees leaving the department. The

Orientation Centre completes the checklist for all employees administered through their office, however there are a number of employees whose leave is administered within their branch, and do not have contact with the Orientation Centre before their departure. As a result, valuable corporate assets may be lost and physical security of the facilities could become compromised.

We recommend that the Departure Process currently being developed by the Orientation Centre be put into practice as soon as possible. To ensure all corporate assets are returned, Managers or Administration Assistants should be held accountable for ensuring an employee's departure form includes all privileges and assets assigned to them, and that a signed copy has been provided to the Orientation Centre prior to the employee's departure. The checklist should specify the assets to be collected under different scenarios, including permanent leave, temporary transfer, leave of absence and contractor / temporary employment.

Management Response:

The Departure Process is currently being finalized and should be ready for implementation by the end of the first quarter by the Orientation Centre.

4.9 Business Resumption Plan

In December 1999, TBS finalized a comprehensive business resumption plan (BRP) to ensure the continued availability of critical services and assets in the event of a disaster. TBS has not reviewed or tested its BRP since its inception in December 1999. In addition, as the BRP was designed to specifically address the Year 2000 problem, it may be less relevant in today's environment. To address this problem, SSD has initiated a project to update the BRP and expect the revised version to be available in May 2002.

We recommend that SSD continue its efforts to update the BRP. A schedule should be developed to review and test the BRP on an annual basis. Testing of the BRP should involve all components of the plan, and be developed to test its applicability and appropriateness for a number of test scenarios. Senior Management should ensure that the job descriptions of all personnel clearly identify their role in the Emergency Preparedness program, including administrative and Commissioner staff.

Management Response:

SSD is working closely with the TBS BRP Committee to update the BRP. Testing of the plan will be discussed with senior management when the plan is presented for approval in the fall of 2002.

4.10 System Development Methodology

TBS does not currently use a standard methodology or approach in performing system development or maintenance of system, network or application software. In many cases, key decisions and approvals are communicated informally through e-mails and are not appropriately maintained as support for system modifications. Lack of a formalized method of system development may result in programs, reports, customizations and application systems that are not properly authorized, tested, and approved before being put into the production environment.

We believe the current process does not contain adequate controls to prevent unauthorized or incorrect changes being implemented. Below are some of the recommendations we suggest be considered:

- ***The process for changing software, generating reports or customization should be formalized and documented.*** A System Development Methodology will help ensure a consistent and appropriate level of quality and control in the software change process. This methodology should require formal documentation of the nature and extent of changes, development of back-out procedures, and the identification of individuals responsible to perform and review that the changes were appropriate. To ensure ongoing proper system processing, the process for modifying and upgrading software should include procedures to ensure that only authorized and properly tested changes are made to production programs. The System Development Methodology should also contain directions for developing and maintaining security, and include guidance for the development of applicable security related deliverables including a system security plan and requirements document, statement of sensitivity, threat and risk assessment and security accreditation.

- ***Users requesting the software should be required to sign off and accept the software prior to it being placed into production.*** While current procedures involve informal approval of software changes through e-mails, consideration should be given to formal written sign off of acceptance. Requiring users to sign off on software prior to placing it in production, not only helps to ensure that only authorized changes are implemented but it also reinforces the responsibility users have to ensure that software changes meet their requirements.

Management Response:

The Informatics Services Division (ISD) has adopted a set of procedures and processes to manage the development and maintenance of system, network and application software for which it is responsible. For example, each group in the division prepares change management plans for all planned changes to systems, network and applications. The tables of content for these plans include sections on: goal definition, justification/benefits analysis, impact/risk analysis and detailed project tasks description and schedule (initiation, first level testing, second level testing, implementation, measurement and post-implementation analysis). These plans are discussed and approved at divisional management meetings being held twice a week. ISD also uses extensive e-mail correspondence as the underlying communication and decision support vehicle with clients. The use of electronic mail to conduct internal business functions, such as receiving sign offs from clients when approving software changes or business process changes for internal departmental operation, forms an integral part of our system development methodology. This approach has allowed us to significantly streamline the delivery of services and to meet the rapid development requirements associated with most applications.

ISD recognizes the need to better document and to strengthen its system development methodology. A project to formally document our system development methodology will be undertaken in 2002-2003 to address the recommendations of the report and to ensure that security related deliverables (Statement of Sensitivity and Threat and Risk Assessment) are included in change management plans.

Since other areas of the department are also responsible for application development and maintenance, there is a need to extend the system development methodology for department-wide adoption. This will be done in close collaboration with the departmental IM/IT Advisory Committee. This issue should also be reviewed as part of the development of the departmental IM/IT Strategy that is planned for 2002-2003.

Annex A

Provided below is a list of TBS employees that we interviewed and/or performed testing with, as part of our audit.

Len MacPherson, Director of Security	Security Services
Mike Pellerin, Manager Security Operations	Security Services
Lillian Noel, Manager, IT Security & ITS Coordinator	Security Services
Pat Johnston, IT Security Officer	Security Services
Linda Marchard, Security Officer	Security Services
John Evans, Occupational Health & Safety Officer	Security Services
Karen Koster, Manager	Facilities
Mark Marion, Accommodation Officer	Facilities
Raymond Boutlier, Accommodation Officer	Facilities
Gregory Howes, Chief, Network Management Group	Informatics
Maureen Lamb, Systems Development Group	Informatics
Sue Arsenault, Manager	Orientation Centre

Mike Giles, Senior Contracting Officer	Contracting
Clarence Smith, Manager	Mailroom
Bernadette Provost, Manager	Records Management
Simone Lauriault, Supervisor	Records Management
Marianne Pelletier, Systems Analyst	Records Management
Sylvie Cloutier, Staff Relations Officer	Human Resources

Endnotes

(1) As a number of control objectives have not been met due to the lack of documented policies and procedures ("P&P") at the departmental level, we have isolated this recommendation within the table above.

(2) As a number of control objectives have not been met due to the lack of documented policies and procedures ("P&P") at the departmental level, we have isolated this recommendation within the table above.