OFFICE OF THE
AUDITOR GENERAL
MANITOBA

Department of Innovation, Energy and Mines
Treasury Board Secretariat
Department of Finance
Civil Service Commission

Web Version

3

Information Technology (IT) Security Management Practices

Executive Management
Carol Bellringer
Norm Ricard

Principals
Doug Harold
Fraser McLean

Table of contents

Main points

What we found

Our objective was to determine whether Business Transformation &Technology (BTT) designed and implemented adequate Information Technology (IT) security management practices and controls.

In 2005, work began to consolidate information technology services for all government departments (except Health) into BTT. Consolidation was mostly complete in 2011. The Department of Health continues to manage and secure its own IT services. And the Legislative Building Information Systems unit also continues to manage and secure its own distinct IT services (network, systems, data storage) though it was part of the consolidation.

> **We concluded that BTT needs to significantly improve its IT security management practices and controls to properly secure information. The lack of IT security risk assessments, IT security plans, and a data classification system means that the rationale for the design and implementation of IT security practices and controls is not well supported. As such, we cannot comment on the completeness, relevance and effectiveness of the practices in place to secure systems and network operations.**

We base our conclusion on the findings discussed in our report and summarized below. Many of the findings are longstanding problems, going back over 8 years and persist despite repeated recommendations to remedy the situation. It is important to note that we did not assess whether IT security practices and controls were operating as intended.

BTT not aware of all significant IT security risks: BTT only recently began to assess some common IT security risks. Much more work is needed to identify and assess risks, decide how to mitigate them, assign accountability, and mobilize resources – section 1.

IT security decisions may not support government objectives: BTT has not developed an IT strategic plan or an IT security plan. BTT does not use IT security objectives and performance measures to monitor and improve the IT security program. BTT does not know the full direct costs of the IT security program – section 2.

Many IT security risks not sufficiently mitigated: BTT recently implemented an IT Policy Management Framework. But the Framework does not require that risks drive policy creation or updates. Most existing IT policies need updating; there are many IT security policy gaps – section 3.

Many users unaware of critical IT security expectations: A security awareness program has been in place for several years, but important aspects are missing: attendance by all government employees is not mandatory; workshops are not based on job duties or

associated risks, nor do they refer to all security policies; and some common awareness improvement techniques are not used – section 4.

Information assets not properly safeguarded: An information management framework is not in place even though the government has known, since at least 2004, of weaknesses in the state of information management. Notably, the government has not implemented data classification standards to identify the various sensitivity levels of government information. Specific security procedures tailored to the sensitivity of the information assets and data could then be designed and used. In addition, the risk of unauthorized access to information assets has not been sufficiently mitigated because logical (electronic) and physical control requirements have not been defined – section 5.

Contractor IT security practices may not meet government requirements: BTT has not defined IT security requirements. So each major contractor uses their own security practices. BTT obtains assurance, over the operation of security practices, on only a small portion of these contracted security services – section 6.

Security controls may not protect network and systems: Protecting the network and systems from external threats involves using controls, many of which need to be actively managed and monitored. BTT has implemented preventive and detective controls, but they are not well managed, specifically in the use of high security zones and encryption, and the development of a data loss prevention strategy. In addition, there are several weaknesses with BTT's incident handling practices – section 7.

Previous recommendations not yet resolved: The lack of progress is a problem. Recommendations included in our *January 2012, December 2010* and *December 2007 Reports to the Legislature*, and in our 2008 and 2009 Public Accounts management letters are noted in the following sections of this report as not yet being implemented: IT risk assessments (1.2), IT strategic plans (2.1), IT Security Policy (3.2), updating IT security policies (3.4) and disaster recovery planning (7.6).

In addition, while not discussed in the detailed sections of this report, many recommendations included in either our *March 2004 Report to the Legislature* (the chapter on *Computer Security Incident Response Capability*), or the related internal management letter (issued to the Department) were in response to findings similar to those included in the following sections of this report: IT security risk assessments (1.2), IT strategic planning (2.1), security patch management (7.2), monitoring of IT security events (7.3.6), IT security incident handling (7.5), and disaster recovery planning (7.6).

Previous Information Protection Centre (IPC) strengths no longer in place: Our 2004 audit on *Computer Security Incident Response Capability* found that the IPC had a *Threat Risk Assessment Guideline* (see section 1.2), an interim *IT Security Policy* (section 3.3), and an *Operations Manual* (section 7). These 3 documents are no longer in place, but would have been solid foundations to build current IT security practices on.

Why it matters

The world is increasingly connected through technology, exposing information assets to a wide range of threats. Detecting and responding to attacks against networks and systems cost a lot of time and money. Organizations must know of the IT security risks to their networks and systems. Then they must implement comprehensive IT security risk management practices and controls to effectively mitigate the risks. Otherwise, organizations will have a false sense of security about their IT environment.

BTT provides IT services to more than 13,000 users of the government's network and in 2011/12 had an expenditure budget of $115.5 million. It supports about 500 business systems and protects the information of 18 departments. Many of the consolidated IT services BTT provides are delivered through several large contractors (about $50 million a year).

The government's network and systems contain highly sensitive information. It is critical for the government to properly safeguard this information, which includes witness protection records, child abuse records, pre-release budget information, cabinet minutes and supporting documents, and pre-trial prosecution files on major crimes.

Background

Information security

Information security is the means of protecting **information assets** from unauthorized access, use, disclosure, disruption, modification, review, and destruction. The core principle of information security is to protect the confidentiality, integrity, and availability of information.

In this report, **information assets** refers to all hardware, software, and electronic data.

The government gathers, processes and stores large amounts of data within information systems while also transmitting that data across one or many networks. Threats to the government's systems and data are real. Findings from the *2012 Verizon Data Breach Investigations Report* " … show that target selection is based more on opportunity than on choice. Most victims fell prey because they were found to possess an (often easily) exploitable weakness rather than because they were pre-identified for attack."

Information security over the network and systems used by government departments (except for Health as explained below) is managed by Business Transformation & Technology, a division of the Department of Innovation, Energy and Mines.

Recent history of information technology (IT) management in Manitoba

In 2004, Treasury Board approved an IT restructuring initiative for departments and special operating agencies and created a central shared services IT group named Information and Communication Technology Services Manitoba (ICTSM) within the Department of Energy, Science, & Technology (now the Department of Innovation, Energy, and Mines (IEM)). In 2005, ICTSM was assigned the responsibility of consolidating all IT operations and processes within government departments. In 2009, ICTSM became Business Transformation & Technology (BTT). The consolidation of IT operations was substantially completed in 2011. All departments were included except for the Department of Health. Treasury Board directed IEM to work with the Department of Health to ensure their IT plans, including those of regional health authorities, were consistent with the government's overall IT strategy.

The IT operations of the Department of Health continue to be managed by its Information Systems Branch (ISB). No reporting relationship exists between BTT and ISB. In addition, BTT is not responsible for IT security within the Department of Health.

From here forward in this report, we only refer to BTT and the Department of IEM for the relevant functions.

Business Transformation & Technology

The Assistant Deputy Minister responsible for BTT is the Chief Information Officer (CIO). The Government's website describes BTT's role as follows:

> Provides leadership for service delivery activities, operational transformation activities and the SAP implementation across the Government of Manitoba ensuring the best possible use of the province's existing information and communications technology resources, systems, platforms, applications and skills, while finding new ways to meet service challenges, plan for future needs, and respond to economic opportunities.

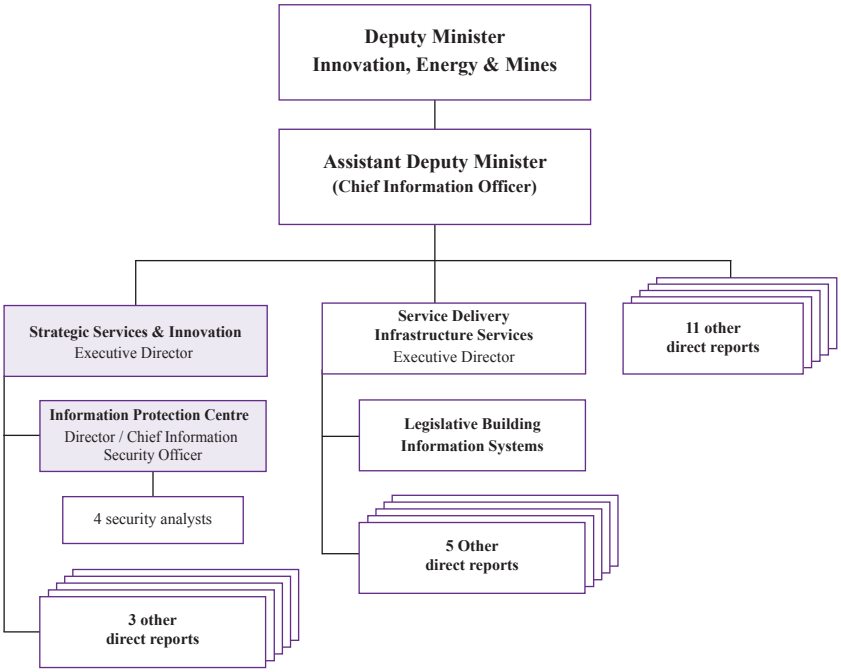
BTT employs about 200 individuals across multiple functional areas, including business transformation, project management, infrastructure support, strategic services, application development, and IT security. BTT provides services to more than 13,000 users of the government's network and in 2011/12 had an expenditure budget (operating and capital) of $115.5 million ($116.1 million in 2010/11). It is responsible for supporting about 500 business systems and for protecting information assets held by 18 government departments (as noted earlier, the Department of Health's IT function was not included in the consolidation of IT services into BTT). Many of the IT services provided by BTT are delivered through several contractors; the major contractors are listed in **Figure 1**.

Figure 1: Major contractors used by BTT

Contractor	Service	Amount Paid in 000s Fiscal 2011	Fiscal 2012
A	Housing and maintenance of systems, including servers and mainframes.	$12,331.4	$12,547.1
B	Housing and maintenance of Managed Environment network services, including user access, email, messaging, and files.	25,989.5	26,995.2
C	Manages the network infrastructure.	11,001.7	11,089.1
D	Intrusion and security event monitoring.	120.1	118.4
	Total	**$49,442.7**	**$50,749.8**

Source: Department of IEM financial records

Figure 2: Business Transformation & Technology organizational structure - June 30, 2012



Our audit examined certain operations within the following branches of BTT (see **Figure 2**).

Strategic Services and Innovation

BTT's website describes the role of this branch as follows:

> Strategic Services and Innovation works closely with the Assistant Deputy Minister and other key stakeholders to: establish and adjust strategic directions for government's information and communication technology (ICT) assets and resources; establish and clarify policies that provide guidance for the management of ICT in government; establish and maintain a business architecture that enables identification of service improvements through technology.

Information Protection Centre (IPC)

The Director of IPC is also the Chief Information Security Officer (CISO). The CISO reports to the Executive Director, Strategic Services and Innovation who reports to the CIO.

BTT's website describes IPC's role as follows:

> The IPC is responsible for protecting the Manitoba government computer networks and safeguarding Manitoba's information and technology assets. The IPC works with business owners to ensure that the information assets of the government are protected and secure while enabling online service delivery.

BTT's internal website provides the following details regarding IPC's role:

> The IPC's mission is guided by the following pledge:
>
> - To enable service delivery by providing balanced, cost effective, security solutions to the government;
> - To protect Manitoba's networks by continuing to find and address vulnerabilities in networked devices;
> - To continually improve the information technology security baseline of the Manitoba government;
> - To detect misuse of, or attacks against, Manitoba's networks and respond to minimize the impact of these security incidents;
> - To provide a single point of contact for network security within Manitoba.
>
> The IPC is responsible for providing a number of services as part of the overall security program that includes:
>
> - **IT Security Policy & Standards**: The IPC provides subject matter expert advice in the creation of technological policies and standards to be followed by all organizations connected to the government network.
> - **Security Architecture**: The IPC assists departments in adopting IT Security solutions based on policy and legislation requirements.
> - **Security Awareness and Education**: Strengthening of Manitoba's security posture through the education of employees by providing organized resources and IT security information to departments through the security awareness program.
> - **Research & Development**: The IPC researches security technologies and processes for their applicability and use within the government's managed environment.
> - **Computer Forensics**: The IPC conducts forensic investigations on behalf of the employing authority.
> - **Intrusion Detection/Perimeter Protection**: Includes network mapping, anti virus, intrusion detection, vulnerability management, and firewall design services.

- **Incident Response**: Provide a coordinated response to incidents as they occur on the network. This includes containment, eradication, monitoring and communications.
- **Risk and Vulnerability Assessment**: The IPC works with departments and business owners to conduct risk and vulnerability assessments.

Legislative Building Information System

The Legislative Building is serviced by a separate and distinct network (with limited connectivity to the provincial network) that is managed and secured by the Legislative Building Information System (LBIS) unit. LBIS reports to the Executive Director of Service Delivery Infrastructure Services of BTT.

The objective of LBIS, as noted in the Department of IEM's annual report, is "To provide a secure technological environment, with highly responsive support services and reliable systems that address business requirements of all staff in the Legislative Building; Government, Legislative Assembly and Caucuses."

LBIS supports the following user groups:

- Legislative Assembly and each of the respective caucuses (NDP, PC and Liberal).
- deputy ministers and their staff.
- other Legislative Building occupants, including – French Language Services, Treasury Division, News Media Services, Legislature Building Security, Tourism, and Legislature Building Maintenance.

LBIS provides the following services to their users - network and security; desktop services; server support and projects; and application services.

Because the Legislative Building information systems are managed independent of the network managed by BTT, it was only included in our audit scope with respect to our examination of BTT's risk management process (section 1).

Audit approach

Our objective was to determine whether Business Transformation & Technology (BTT) designed and implemented adequate IT security management practices and controls. Specifically, we assessed BTT practices and controls against the audit criteria detailed in **Figure 3**.

We did not assess whether IT security practices and controls were operating as intended. For example, we looked for the existence and placement of firewalls, but did not test whether they controlled the flow of information as designed.

Our examination focused on the practices employed primarily by BTT. However, when necessary, practices used by other relevant stakeholders within government were examined.

We examined the design and implementation of practices and controls in place up to June 2012. Our examination took place between February and June 2012.

Our examination was performed in accordance with the value-for-money auditing standards recommended by the Canadian Institute of Chartered Accountants and accordingly, included such tests and other procedures as we considered necessary in the circumstances.

A detailed findings document was presented to BTT for their follow-up.

Figure 3: Audit criteria

Our audit criteria are based on:

- *Control Objectives for Information Technology 4.1* (COBIT) developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
- *ISO/IEC 27002:2005 IT Security Techniques – Code of Practice for Information Security Management* developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

Many organizations use the COBIT framework for the management of their IT environments. COBIT is a set of best practices for information technology management. It provides managers, users, stakeholders and auditors with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the organizational benefits derived from the use of IT and in developing appropriate governance practices and internal controls.

When establishing their security programs, many organizations use *ISO/IEC 27002:2005 IT Security Techniques – Code of Practice for Information Security Management*. Publication of these standards required approval by experts in IT security management.

We reviewed the following **audit criteria** with management, and obtained their concurrence on the suitability of the audit criteria.

Business Transformation & Technology should:

1. **have processes to identify, assess, mitigate, and accept IT security risks.**
2. **have information security strategies that support IT and organizational objectives.**
3. **have policies that address significant IT security risks.**
4. **periodically update and communicate IT security policies.**
5. **classify and safeguard information assets.**
6. **ensure that adequate security controls are in place in outsourced services.**
7. **secure system and network operations to protect against threats and vulnerabilities.**

Findings and recommendations

1. BTT not aware of all significant IT security risks

Organizations face many types of risks that senior management must address as part of their corporate risk management responsibilities. Many of these risks, notably IT security risks, relate to information held in or processed by IT systems.

IT risk management requires that an organization identify risks, assess their impact and likelihood, develop appropriate mitigation strategies, and update their assessments of risk on a periodic basis or, when necessary, by changed circumstances. Integration with entity-wide risk management processes is beneficial.

Ultimately, the responsibility for IT risk management lies with system and data owners. Owners define IT risk tolerances, determine mitigation strategies, and accept residual risks. Without a comprehensive IT risk management framework, an entity may be unaware of certain risks, leaving them unprotected.

We assessed whether:

- BTT developed an IT risk management framework (section 1.1).
- IPC conducted IT security risk assessments (section 1.2).

1.1 ICT Risk Management Model developed, but stakeholders not required to accept residual risks

In January 2011, BTT issued an *Information and Communication Technology (ICT) Risk Governance Model* which defines the risk management roles of the Assistant Deputy Minister (the CIO), the BTT Senior Management Committee, the Risk Office (a role assigned to the Executive Director of Strategic Services and Innovation of BTT), the executive directors and organizational unit managers.

Also in January 2011, BTT issued an *ICT Risk Management Model*. The Model provides guidance on risk identification, analysis, evaluation, and treatment, and includes an inventory of common ICT risks.

While the Model provides useful guidance in managing IT risks, it does not require consultation with system and data owners on their risk tolerance and whether they are prepared to accept any residual risks. As such, if BTT accepts risks on behalf of system and data owners, without due consultation, they are potentially making decisions that are inconsistent with the owners' risk tolerance.

Recommendation 1: We recommend that BTT enhance the *ICT Risk Management Model* by requiring consultation with relevant stakeholders within government on their risk tolerances and their willingness to accept residual IT risks.

1.2 Comprehensive IT security risk assessments not conducted

Organizations depend on information systems and networks to support their operations. Information systems and networks are exposed to serious threats that can negatively impact operations. Through IT security risk management, an organization measures the likelihood and impact of a vulnerability being exploited by a threat. IT security risks can impact the confidentially, integrity, or availability of information assets and operations.

The first step in BTT's *ICT Risk Management Model* is the identification of divisional outcomes. The Model indicates that divisional outcomes "form the basis against which all risks will be identified, assessed and evaluated." Included in the *ICT Risk Management Model* document are 5 BTT outcomes (see **Figure 4**).

Figure 4: BTT outcomes

Outcome	Description
Accessible government	A significantly improved ability for citizens of Manitoba to access government information, programs, and services at times, places, and in formats convenient to citizens.
Cost effective program delivery	Many of the strategies and objectives outlined will result in more cost effective service delivery by BTT and eventually to the citizens of Manitoba.
Safeguard information and assets	We will continue to facilitate legitimate access to information while providing strict control over the collection, management, and security of this information in accordance with freedom of information and privacy legislation.
Support Manitoba communities	BTT will continue to support government's commitment to leverage and coordinate Manitoba's investment in ICT to bring new services and opportunities that support the social and economic development of Manitoba communities.
Enable innovation	BTT will collaborate to create an environment that supports and enables innovation by being flexible and responsive to change and open to new ideas including embarking on a program of Human Resource redevelopment.

Source: BTT's ICT Risk Management Model

In October 2011, 3 of BTT's 12 organizational units held workshops to identify and assess risks. The results are documented in a Risk Register. It is important to note that we did not assess the quality of the IT risk assessments conducted. Nonetheless, we noted that BTT had only begun to identify and assess IT risks (including security risks). The risk assessments in the Risk Register (including those that were IT security related) only dealt with some of the common risks included in the model, and nothing was done to identify IT risks (including security risks) beyond the common risks noted in the model. Much more work is needed to identify and assess risks (including IT security risks), determine mitigation activities, assign accountabilities and mobilize resources.

In addition, the service agreement with Contractor A (see Figure 1 in Background section) indicates that IPC, with the assistance of the Contractor, will perform an analysis to expose and address IT security threats as discovered. At the time of our audit, IPC had not yet taken advantage of this potential assistance from the Contractor.

We are particularly concerned that risk assessments have not been conducted, nor are any planned, around the operations of the Legislative Building Information Systems (LBIS) unit. Adequate strategies or controls may not be in place to mitigate the risks associated with the following conditions:

- The Director of LBIS reports directly to a branch of BTT but the roles and responsibilities of LBIS and BTT are not clearly defined or documented.
- The LBIS unit, with its limited resources, manages a separate and distinct network (from the government network) to provide systems and services to users within the Legislative Building.
- LBIS manages all aspects of the security program over its network, systems and data (including highly sensitive information).
- No performance measures and targets have been defined for LBIS.
- LBIS maintains, communicates and enforces its own policy instruments.

We are also concerned that BTT practices in the area of IT security risk management have not significantly improved despite our previous comments and recommendations. In our *December 2010 Report to the Legislature* and our 2008 Public Accounts management letter, we recommended that BTT implement a comprehensive IT risk assessment process.

In 2004, we conducted an audit of *Computer Security Incident Response Capability*. We noted that the IPC had a *Threat Risk Assessment Guideline* document. The Guideline stated that an IT security threat and risk assessment must be performed on new systems, at least annually, or whenever there is a substantive change in the environment. This Guideline no longer exists. While the Guideline was developed prior to the centralization of departmental IT operations into BTT, it would be a useful starting point in developing and performing IT security risk assessments in today's centralized government IT environment.

Despite their lack of progress, in its 2007 annual report, the Department of IEM stated that BTT implemented an information security risk assessment program for government, overstating the status of IT security risk assessments at the time.

Recommendation 2: We recommend that BTT complete, on a priority basis, a comprehensive IT risk assessment, which would include an assessment of IT security risks.

Recommendation 3: We recommend that BTT complete an assessment of the risks related to the operations of the LBIS.

2. IT security decisions may not support government objectives

Setting the performance goals, objectives and targets of any program is heavily influenced by the strategic direction of the host organization. As such, clear strategic direction is an essential component of program performance management. When planning and assessing program performance, in addition to comparing actual performance levels to targets, it is important to understand whether key risk mitigation controls are in place and operating as expected and whether the financial commitment is sufficient to meet the strategic objectives and performance expectations.

We assessed whether:

- BTT has developed an IT strategic plan (section 2.1).
- BTT uses performance measures to monitor and improve the IT security program (section 2.2).
- independent IT security audits and reviews are performed (section 2.3).
- the full cost of the IT security program is known (section 2.4).

2.1 IT strategic plan not in place, but some planning occurs

An IT strategic plan defines how IT supports the organization's objectives. The plan discusses opportunities and limitations, risks, and resource requirements (both staffing levels and hardware/software). Furthermore, an appropriately developed IT strategic plan guides IT security planning decisions. According to Ernst & Young's *2012 Global Information Security Survey* "developing an integrated information security strategy is critical to gaining

a holistic view of the risk landscape and fully addressing those risks. Leading organizations have recognized this and are working harder to ensure that information security is embedded into both business and IT strategies."

BTT has not yet developed an IT strategic plan, including an IT security strategic plan, despite our previous comments and recommendations. In our *December 2010 Report to the Legislature* and our 2009 Public Accounts IT management letter, we recommended that BTT develop an IT strategic plan, which would include IT security.

We noted that BTT has conducted some strategic planning activities as noted below:

- ***Identified 5 BTT outcomes***: As discussed in section 1.2, BTT's *ICT Risk Management Model*, issued in January 2011, includes 5 BTT outcomes to help focus the risk management processes.
- ***Identified 5 IT initiatives***: In July 2011, BTT identified the following IT initiatives:
  - develop and communicate a policy framework for BTT processes.
  - workplace technology services to continually manage and evolve work-place technology products and services.
  - continue to increase broadband connectivity.
  - improve access to information.
  - information and communication technology prioritization framework.
- ***Developed the "myGovernment 2020" document***: In February 2012, BTT issued *myGovernment 2020*. It provides an overview of the opportunities, vision, approach, driving forces, challenges, recommendations and benefits of information and communication technology within the government of Manitoba from 2010 to 2020. The document lays out, at a high-level, business drivers and strategic focus areas.
- ***Developed a Technology Deployment Roadmap***: In September 2010, BTT created a *Technology Deployment Roadmap* that lists various high level initiatives to be addressed before fiscal year 2012-13.
- ***Commenced Application Portfolio Management Initiative (APMI)***: In October 2011, BTT commenced the APMI. The objectives of this 3 year initiative are to: identify and eliminate application redundancies, assess the condition of each application, and strategically determine application investment decisions. BTT officials told us that applications have been inventoried and that they are now cataloguing the applications to determine which should be eliminated, accepted as is, migrated or innovated.

While these are important steps forward, significant work is needed so BTT can clearly articulate and communicate its strategic plan, and supporting objectives, for IT.

Without adequate planning, IT security practices may not be aligned with government objectives on security. And as such, government resources allocated to protecting information assets may not optimize the value obtained.

Recommendation 4: We recommend that BTT develop an IT strategic plan and a properly aligned IT security plan.

2.2 Performance measures not used to monitor and improve IT security program

Performance measures and established targets help management determine if stated objectives are being achieved and if corrective actions are needed. Relevant, complete, and timely performance measures help management increase accountability, improve program effectiveness, demonstrate compliance with internal and external requirements, and allocate resources. **Detailed** performance measures are used by program managers to improve performance. **Key** performance measures are used by senior entity management to monitor the effectiveness of the program and to allocate resources.

IPC has not implemented performance measures. As noted in section 2.1, IT security strategic plans are not in place to contribute to the identification of measures and the setting of targets. Some statistical information is gathered and some trends are analyzed. These are detailed in **Figure 5**. Some of this information could be useful as performance measures, if compared to preset targets.

Figure 5: Statistical information gathered and analyzed

Type of information	Trends analyzed
Spam (junk email) statistics	Attempted deliveries, actual email deliveries
Virus statistics	Number of viruses detected
Intrusion detection statistics	Number of events
Security awareness training	Background and number of employees trained
Forensic HR investigations	Number of forensic investigations
Application security assessments	Number of security assessments performed on new solution architectures (for example, new applications)
Theft and loss of equipment	Number of computers that were lost or stolen
Security incidents	Varying types of security incidents that occurred
Application server vulnerability statistics (and vulnerability analysis)	Number of operational vulnerabilities in databases and operating systems for the year

For the purposes of managing the IT security program, performance measures could also include the following:

- percentage of systems that meet IPC security requirements.
- percentage of systems with the latest security patches installed.

- results of security assessments performed on new and existing systems.
- number of logins and failed login attempts for privileged users on the network.
- for security incident handling: number of open and closed incidents; events per IPC security analyst hour; and average time spent in open and closed incidents.
- measures of user security awareness.

Without performance measures to track and monitor the performance of IPC's IT security program, BTT senior management cannot be properly informed about the performance of the program and whether it is adequately supporting government objectives. In addition, performance information is not available to senior management when making resource allocation decisions.

Recommendation 5: We recommend that BTT and IPC identify performance measures for the management of IT security operations, and that a specific target be set for each measure. Once an IT security plan is in place, performance measures and targets should align with the noted security goals and objectives.

Recommendation 6: We recommend that BTT and IPC provide senior management with quarterly reports that focus on:

a. key performance measures (as agreed to by senior management).
b. performance in relation to the defined targets.
c. actions to address any performance shortfalls in meeting objectives.

2.3 No recent IT security audits by independent third party

Reviews and audits help assess the overall effectiveness of IT security practices. Those performed by independent parties provide the most value to an IT security program. They must be conducted at regular intervals or when significant changes have occurred within the environment. Deficiencies noted help management take the appropriate corrective actions.

It has been several years since BTT has engaged the services of an independent third party to conduct an audit of its IT security management practices. The latest review occurred in 2005/06 when an external reviewer was hired to examine the IT security practices of BTT's Contractor B (see Figure 1 in Background section). A report was received in March 2006. The report presented multiple deficiencies and recommendations. BTT did not review the recommendations for appropriateness, develop action plans with the Contractor B, and track the implementation of the recommendations.

Between 2008 and 2010, Internal Audit and Consulting Services conducted 5 audits on BTT practices. Three of these reports were released in 2010 including a report on an audit of the handling of sensitive information. The 2 remaining audits were issued in July 2011. We note, however, that the government's Corporate Audit Committee approved 2 BTT requests that additional internal audits not be started, resulting in no new Internal Audit activity between December 2010 and March 2013. In total, 3 audits on BTT practices were deferred. Department specific IT audits, including reviews of security measures at departments, were not impacted.

Through regular independent third party security audits, as well as, internal audits, BTT senior management can be informed in a timely manner of deficiencies within the IT security program.

Recommendation 7: We recommend that BTT obtain, at regular intervals, independent third party audits of its IT security practices, and that progress reports on the implementation of recommendations be provided to senior management.

2.4 Full cost of IT security program unknown

To assess whether good value is being obtained from the IT security program, it is important that the full costs associated with IT security be determined. This can be a difficult task in a large and complex IT environment because IT security practices are often integrated into a number of distinct IT functions and technology domains.

IPC is provided a budget for its own operating needs. However, many IT security practices are embedded within the major Contractor agreements. The cost of these practices is not identified within the total cost of the agreements. As such, a complete representation of the amount spent on the IT security program is not available. Without a complete and detailed understanding of IT security costs (as well as strategic direction, security risks, and performance measures), it is difficult for government to get assurance that good value is being obtained from its expenditures on IT security.

Recommendation 8: We recommend that BTT annually determine the total costs associated with IT security.

3. Many IT security risks not sufficiently mitigated

An organization's IT policy instruments are essential components of its information security program because many IT policy instruments are developed in response to an identified risk. IT policy instruments include policies, standards, guidelines, directives, and procedures.

We assessed whether:

- BTT implemented an IT policy management framework (section 3.1).
- IT policy instruments are complete and up to date (sections 3.2, 3.3, and 3.4).

3.1 Policy Management Framework in place, not risk focused

In June 2011, the Business Transformation Executive Committee (BTEC) approved BTT's *Policy Management Framework* for IT policy instruments. BTEC is a committee comprised primarily of 9 Deputy Ministers (chaired by the Deputy Minister of IEM) that provides direction on the organization and management of government-wide IT and service transformation projects and that reviews and endorses IT policies that have significant government-wide impacts.

Figure 6: Policy Management Framework

Component	Activities
Creation	Identify the need; provide to BTT Senior Management Committee (SMC) for validation by; research & analysis, may include best practices research and consultation with key stakeholders; draft the policy instrument; SMC review and refinement of the draft policy instrument; prepare policy package, including communication and monitoring plans.
Approval	Review and approval by BTEC (at BTEC's discretion may be escalated to Treasury Board for approval).
Communication	Publish in the Corporate BTT Manual and on the BTT intranet site; distribute policy via email; notify service desk; optional activity includes information and awareness sessions.
Monitoring and compliance	Monitor compliance in a manner consistent with the expectation detailed in the policy package.
Sustainment	Review on a regular basis; consult with stakeholders, obtain feedback; refine and update policy instruments as needed, with significant changes treated as a new need; communicate changes.

Source: BTT's *Policy Management Framework*

The major components of the Framework are summarized in **Figure 6**. Of note, the Framework does not require that IT risk assessments or strategic objectives drive the creation of new policy instruments, or the update of existing policy instruments. Linking updated or new policy instruments to significant risks and strategic objectives helps ensure that policies focus on the right areas.

Recommendation 9: We recommend that BTT strengthen its *Policy Management Framework* by requiring that IT risk assessments and strategic objectives support the need for new or updated policy instruments.

3.2 IT Security Policy not in place

An IT Security Policy supports an organization's objectives regarding the security of its information assets. It is an over-arching policy that provides direction for other IT security related policy instruments.

An effective IT Security Policy includes a statement from senior management supporting the goals and principles of information security. It defines roles and responsibilities and outlines the minimum IT security requirements for protecting the confidentiality, integrity, and availability of information assets. An IT Security Policy helps ensure that security practices are consistent with applicable laws and regulations. At a minimum, **security related policies** need to be consistent with an over-arching IT Security Policy.

Security related policies include:

- Data classification
- Operations security
- Access control
- Physical and environmental security Configuration management
- Information systems acquisition, development and maintenance
- Incident handling
- Business continuity
- Media handling
- Compliance
- Network and system usage

BTT has not implemented an IT Security Policy despite our previous comments and recommendations. In our *December 2010 Report to the Legislature* and our 2008 Public Accounts management letter, we recommended that BTT implement an IT Security Policy.

In conducting our 2004 audit of *Computer Security Incident Response Capability* we noted that BTT had published an *Interim IT Security Policy*, however, it is no longer in place.

Without an IT Security Policy, there is an increased risk that IT security practices will not properly align with government objectives on security.

Recommendation 10: We recommend that BTT implement an over-arching IT Security Policy.

3.3 Other significant IT security policy instrument gaps

Because comprehensive IT security risk assessments have not yet been conducted (see section 1.2), BTT cannot ensure the completeness and adequacy of the existing policy instruments to address significant IT security risks present within the environment. For example, IT security policy instruments are not in place for the following activities that have associated IT security risks: virtualization, mobile devices, wireless networking, and physical security.

In January 2003, IPC published a *Standards of Best Practice for Information Security Management*; it has not since been updated. The stated goal of the document is "to provide a framework upon which ICT Security Policy, Standards, Procedures, and Guidelines will be built." This document is based on the *Standards of Good Practices for Information Security* developed by the Information Security Forum, to which IPC continues to be a member. The Forum is "an international association of over 300 leading organizations which fund and co-operate in the development of a practical research programme in information security." Membership entitles the IPC to access all of the Forums guidance documents including the 2012 version of the *Standards of Good Practices for Information Security*. We encourage the IPC to take greater advantage of available Forum resources.

> **Recommendation 11**: Upon the completion of IT security risk assessments, we recommend that BTT implement additional IT policy instruments needed to mitigate IT security risks.

3.4 Most policies need updating

To ensure the ongoing relevance, accuracy and completeness of policy instruments, it is important that they be reviewed on a periodic basis and updated as needed.

The sustainment phase of the BTT *Policy Management Framework* requires that all IT policy instruments be reviewed on a regular basis to ensure that they are relevant and current. However, the Framework does not define the regularity of these reviews, nor does it provide for varying frequencies based on the type of policy instrument. For instance, higher level policies may require less frequent review, while supporting policies, standards, and procedures may need to be reviewed and updated more frequently.

The *Employee Network Usage Policy* (ENUP) was the first IT policy to be updated using the Framework. The ENUP sets standards for access to, and acceptable use of, networks and technologies by government employees; it was updated in December 2010.

No other IT policy instruments have been updated or created using the established Framework and a schedule or plan for the review of IT policy instruments is not in place. This is of concern because existing IT policy instruments require significant improvement as many:

- pre-date the consolidation of IT operations into BTT.
- reference an IT Security Policy that does not exist (see section 3.2).
- are no longer relevant.
- remain in draft form.

In our *January 2012 Report to the Legislature*, we recommended that BTT analyse their IT security policies, standards, guidelines and procedures for completeness and appropriateness.

Recommendation 12: We recommend that BTT strengthen its *Policy Management Framework* by defining the frequency of IT policy instrument review.

Recommendation 13: We recommend that BTT develop a prioritized schedule or plan for the review and update of all existing IT policy instruments and that progress against the plan be actively monitored.

4. Many users unaware of critical IT security expectations

Properly communicating IT security policy instruments involves more than just publishing a document that is accessible and understandable. Organizations need to ensure that employees, contractors and third party users understand and acknowledge IT security requirements and the impact that these requirements have on their use of information assets. Without proper communication of IT security requirements, users may inadvertently place information assets at risk.

We assessed whether:

- BTT has implemented an IT policy communication process (section 4.1).
- employees sign the ENUP to acknowledge their obligation to comply (section 4.2).
- a security awareness program is implemented (section 4.3).

4.1 IT policy communication process in place

The BTT *Policy Management Framework*, as discussed in section 3, includes a communication component. The following mandatory steps are noted:

- publish policy – approved policies are documented in the *Corporate BTT Manual* and BTT's intranet site.
- send email to target audiences – the communication plan included in the policy package identifies targeted audiences for the policy. An email is sent to these groups that discusses the policy requirements and related expectations. BTT's Senior Management Committee and BTEC, are copied on the email communication.
- notify service desk – the service desk is notified of the new or revised policy so they can direct calls to the appropriate person.

Within the Framework, the following steps are optional:

- Information and awareness sessions – depending on the nature of the policy or significance of the change, the policy analyst may choose to have a separate awareness session. The need for such sessions is noted in the communication plan.
- Customer Relationship Managers (CRM) communication campaign – depending on the nature of the policy, there may be a need for the CRMs to actively communicate the details of the policy as part of their customer relationship function.

To date, only an amendment to the ENUP has been communicated using this process. In December 2010, the ENUP was updated primarily to address access to social media. In January 2011, the updated policy followed the communication steps described above.

4.2 Employees not required to sign technology use policy

While IPC requires that users sign the *Virtual Private Network (VPN) Employee Subscriber Policy*, user acknowledgement of the ENUP, either through signature or other digital means, is currently not required. Instead users are provided the option to read the ENUP each time they log into the network. While this makes the ENUP readily accessible to users, it does not ensure that they have read it or that they understand their responsibility to comply with the expectations included in the ENUP. In IPC's March 2012 security awareness survey, 17% of the 839 respondents indicated that they had never read or were not aware of the ENUP.

> **Recommendation 14**: We recommend that BTT amend the ENUP to require new and existing users of the government network, systems, and information assets to acknowledge, either through signature or digital means, their responsibility to comply with the expectations included in the ENUP.

4.3 Security awareness program implemented, but missing important aspects

Security awareness is the human knowledge and behaviour an organization uses to protect its information assets. A security awareness program enhances a user's ability to recognize information security problems and incidents. According to Ernst & Young's *2012 Global Information Security Survey*:

> … 37% of respondents see the threat that has most increased their organization's risk exposure as careless or unaware employees. As well, the number of actual incidents caused by inadvertent employee data loss has risen by 25% in the last year.

Well designed security awareness training sessions present an organization's IT security policies and its expectations when utilizing information assets. Users are informed of IT security incident processes, including the proper channels for initiating contact. Training sessions that focus on a user's job function and its associated risks will enhance the usefulness of the IT security awareness sessions to the user.

IPC has established a security awareness program that includes the following components:

- live training workshops: i) in scheduled classes by Organization and Staff Development, a Special Operating Agency of the Civil Service Commission, and ii) at client locations by IPC staff. Participants are provided with an *Information Security Brochure*, Help Desk tip handouts, and a *Security Quick Reference*.
- security awareness site on the government's intranet providing Frequently Asked Questions, e-Learnings and bi-monthly messages.
- periodic emails containing IT security awareness information are sent to all users.
- annual program review to ensure content currency.
- employee surveys to determine overall awareness (most recently conducted in February 2012 and June 2003).

While IPC has implemented many components of an overall IT security awareness program, the following deficiencies were noted:

Attendance by all government employees is not mandatory: Since 2006, BTT records indicate that approximately 6,000 government employees have taken the live training workshops. Information was not available on how many of these individuals remain government employees. Nonetheless this is a relatively small percentage of government employees with access to the electronic network. In addition, available information indicates that very few employees have taken the on-line e-learning.

Training is not based on job duties or associated risks: Currently, the training is the same for all employees, regardless of the risk associated with their job. Without targeted training, users working with sensitive government information may receive insufficient training, while others working in low-risk positions may receive an excessive amount.

Key information is not used when determining annual updates: Security incident trends are not included in annual updates to the program. In addition, IT security risk assessments and data classification requirements, when they become available, would provide useful information when developing updates.

Workshop does not reference all IT security policies: The current workshop presents the ENUP to employees, but no other IT security policy instruments are referred to. As a result, users may not be aware of the implications of not complying with all other IT security policy instruments.

Additional awareness techniques not used: IPC does not use additional techniques, such as contests, awards, and posters to further promote security awareness among government employees.

Recommendation 15: We recommend that the government make security awareness training mandatory for government employees with access to the electronic network and systems, immediately upon hiring and periodically thereafter.

Recommendation 16: We recommend that IPC enhance the security awareness program by:

a. incorporating the use of IT security incident trends and documented risks.
b. developing additional security awareness training specifically targeting users in higher risk positions.
c. using additional awareness techniques.

5. Information assets not properly safeguarded

Information management involves acquiring, organizing, retrieving, maintaining, and securing all information. Given the rising importance of IT within large and complex organizations, information management has expanded beyond paper-based documents to include electronic data.

We assessed whether:

- the government has developed an information management framework, including data classification standards (sections 5.1 and 5.2).
- BTT has implemented electronic media handling standards and procedures (section 5.3).

- the government has security check requirements (section 5.4).
- security checks have been obtained for IPC staff and contractor staff (section 5.5).
- BTT has processes to mitigate the risk of unauthorized access to information assets (section 5.6).

5.1 Information management framework not developed

Government has been working toward implementing an information management framework for quite some time.

In 2004, the Coordinated Services Unit (a branch of BTT that provided support to the Coordinated Services Committee of Deputy Ministers in the area of innovation in service delivery and technology), formed an Information Management Unit. In December 2004 the Information Management Unit published an *Information Management Framework* (IMF) that was presented to the Coordinated Services Committee of Deputy Ministers. The document included action plans and described the state of information management in the Manitoba government as follows:

> The current information management (IM) environment in the Manitoba government is unsustainable. Ad hoc and inconsistent practices, particularly those related to electronic information, impede collaboration, innovation, and knowledge transfer. There is a weak information culture, IM responsibilities are not well articulated, there is no clear accountability and leadership, and the skill necessary to effectively manage information is not present.

In August 2006 the Coordinated Services Unit established Information Management Manitoba (IMM) as a 2 year pilot. In the Department of IEM's 2006/07 annual report, the role of the IMM was to described as providing "central leadership and effective horizontal coordination to drive and lead the practical implementation of the Information Management Framework."

At the end of the IMM pilot period (August 2008) the Information Management Roundtable was created. Its internal website describes the Roundtable as working "across government departments to establish a disciplined and integrated approach to manage information assets." The Roundtable consists of members with knowledge of and responsibility for the management of government's information assets, including individuals from the Legislative Library, Communications Services, Information and Privacy Policy Secretariat, Archives, and BTT. The roundtable has not met since June 2011.

Despite the longstanding acknowledged need for an information management framework, a department within government has not been assigned this responsibility. As a result, it is unlikely that the state of information management in the Manitoba government has changed much from that identified in 2004 by the Coordinated Services Unit.

Recommendation 17: We recommend that the government:

a. assign responsibility for information management to an appropriate department.
b. develop and implement an information management framework.

5.2 Data classification standards still only in draft

Data classification is a key aspect of information management. Information assets, in either paper or electronic format, vary in importance and sensitivity. To properly protect its information assets, an organization must first classify each information asset in terms of its sensitivity. Information asset sensitivity is typically defined in a range from public information to confidential to highly sensitive.

Determining the sensitivity of information assets is, by necessity, the responsibility of the asset owner. Once data classification standards are defined, organizations implement the needed practices and controls for each level of sensitivity, including media handling procedures, security checks, logical access controls, physical access controls, and processes to remove terminated users.

In August 2011, BTT created a *Proposed Standard for Data Classification* document for review and comment by the Information Management Roundtable, but it has yet to be approved.

As a result, government employees and other users may not be properly protecting sensitive data, including personal and confidential information, and intellectual property. In addition, public disclosure of non-confidential information may be unnecessarily delayed.

Recommendation 18: We recommend that the government implement a data classification standard.

5.3 Electronic media handling standards and procedures not complete

An organization with sensitive information must have an appropriate set of standards and procedures for labeling and handling information, based on defined data classification levels. These are needed for information assets in physical and electronic formats. Handling standards and procedures prevent unauthorized disclosure, modification, removal or destruction of information assets.

Without appropriate handling procedures, information assets may not be handled in accordance with the associated risk and level of sensitivity. High risk and sensitive information assets may not be adequately protected, while scarce resources may be allocated to the protection of lower risk assets.

IPC has published the *Manitoba Government Electronic Media Disposal Standards and Procedures* document for the secure reuse and disposal of **electronic media** containing government information. This document provides procedures and standards for electronic media disposal to help reduce the risk of sensitive information being inappropriately or inadvertently disclosed.

Electronic media refers to different types of data storage options, including hard drives, compact disks, DVDs, flash memory cards and USB drives.

BTT has not, however, developed standards and procedures for handling electronic media during use. In the absence of data classification standards, at a minimum, procedures should be in place for the handling of electronic media that store highly sensitive data (sensitivity determined by the data owner).

> **Recommendation 19**: Upon the implementation of data classification standards, we recommend that BTT develop standards and procedures for properly handling electronic media during use.

5.4 Security checks not obtained periodically

A security check is an important tool to assess the suitability of individuals in positions with access to sensitive information.

The Manitoba Civil Service Commission's (CSC) *Security Checks* policy states that a pre-employment security check is conducted before an individual is appointed to a position for which there is a requirement. The *Security Checks* policy includes several factors for a department to consider when establishing the need for a security check. The factors include: positions having contact with Provincial treasures or sensitive materials; and positions that handle cash and maintain information systems. Once a data classification system is in place, we encourage the CSC to update the risk factors in the *Security Checks* policy to reflect the definition for sensitive data.

The *Security Checks* policy states that the intent of a security check is:

> a highly confidential investigation into a candidate's record of crime or child abuse. It involves a criminal records check or a child abuse registry check conducted before appointing a candidate to a position for which this is a requirement. A security check supplements the reference check.

Each department must provide the CSC with a listing of all positions subject to the security check requirement. Human Resource Consultants of the CSC refer to these listings during the recruitment process.

We are concerned that the *Security Checks* policy does not include periodic security checks for current employees. As noted above, checks are required for certain positions only upon commencement of employment. There is no requirement to obtain periodic security checks during employment. This is particularly important for jobs with access to sensitive information assets.

In addition, under the CSC's *Criminal Charges* policy, employees are required to inform their manager immediately of any criminal charges occurring during employment. We note that the policy does not require periodic declarations from employees. Such declarations would promote employee awareness of their obligations under the policy. CSC noted that they, or Labour Relations Division, do not track and maintain central files regarding criminal charge declarations made to managers.

Without a periodic check, the CSC and government managers may not be aware of an employee's criminal activity subsequent to being appointed, potentially putting sensitive information assets at risk.

Recommendation 20: We recommend that the CSC amend their *Security Check* policy to:

a. require periodic statutory declarations from employees in designated positions, and
b. once a data classification system is in place, require periodic security checks on employees in designated higher risk positions.

5.5 Inadequate security check practices

We assessed whether:

- security checks are on file for IPC employees (section 5.5.1).
- BTT gets assurance that security checks are obtained for contractor staff (section 5.5.2).

5.5.1 Checks not on file for several IPC staff

In January 2012, BTT provided CSC with a listing of employees requiring security checks. While management told us that security checks were obtained for all IPC staff, we could only find a documented security check for one of the 5 permanent IPC staff members. The documented security check was for an employee hired in March 2011. IPC staff members

handle or have access to sensitive security and investigations data. We encourage BTT to obtain documentation of these security checks.

5.5.2 No assurance that security checks obtained for contractor staff

Agreements with Contractors A, B, and C (see Figure 1 in Background) include provisions that require the Contractor to obtain security checks on all of its employees that have access to government of Manitoba information assets (note: Contractor D does not have access to government information assets). BTT has not requested assurance from any of the 3 Contractors that security checks have been obtained for employees that handle government information assets even though many employees of the 3 Contractors have access to sensitive government information assets.

Of note, the 2006 report by an independent third party reviewer of Contractor B (see Section 2.3) noted that the reviewer was unable to determine whether criminal record checks were obtained for 40% of sampled contract support staff. The reviewer recommended the following: "… that the government of Manitoba request (Contractor B) to implement a practice for periodic updates of staff Police record checks to ensure that staff remain compliant with the government of Manitoba's requirements."

> **Recommendation 21**: We recommend that BTT obtain periodic assurance that contractors are obtaining security checks on employees with access to government information assets.

5.6 Risk of unauthorized access to information assets not sufficiently mitigated

Access to information assets needs to be properly controlled. For each user group, access rights and controls must be clearly stated in a policy instrument, including logical (electronic) and physical access controls. Access controls must be established based on data classification requirements and documented IT security risk assessments.

We assessed whether:

- logical access control requirements are defined (section 5.6.1).
- physical security requirements are defined (section 5.6.2).
- processes are in place to restrict and remove access by terminated users (section 5.6.3).

5.6.1 Logical access control requirements not defined

Logical access controls prevent unauthorized access to network and systems and include the following components:

- passwords.
- procedures for creating, maintaining and deactivating access, including privileged users.
- monitoring user activities.

BTT has not defined minimum password requirements. Each Contractor sets specific password controls for the systems or network managed. Weak password controls within the IT environment increase the risk that unauthorized individuals access government information assets.

BTT has not defined minimum requirements for creating, maintaining and deactivating access. System owners are responsible for their own unique processes for creating, maintaining, and deactivating user access to their systems. Weak processes increase the risk that unauthorized individuals access government information assets.

BTT has also not developed requirements for the monitoring of user activities. System owners need to monitor the appropriateness of user access and activities. User activities vary for each system and owners need to determine the high risk activities to be monitored. Ineffective or incomplete monitoring of the government network and information systems increases the risk that unauthorized high risk activities go unnoticed.

Recommendation 22: We recommend that BTT develop logical access control requirements.

5.6.2 Physical security requirements not defined, resulting in deficiencies

Physical access controls prevent unauthorized access to an organization's information assets by restricting access to property, including rooms and data centres. Physical protection must be determined based on identified risk assessments.

Physical security controls include perimeter barriers such as walls, card controlled entry gates or manned reception desks. Entry controls include visitor processes, identification cards, locks, and regular reviews of access rights to secured areas housing sensitive information. Unauthorized physical access can lead to stolen or damaged information assets.

BTT has outsourced the management of its 5 main data centres but has not defined its physical security requirements. As a result, there are distinct differences in the physical controls implemented at the outsourced data centres. The rationale, including risk assessments, for the physical security controls at each outsourced data centre is not documented.

We visited each data center and found that the physical security controls at 2 need strengthening. Detailed findings and recommendations have been provided to BTT in a separate detailed findings document.

Recommendation 23: We recommend that BTT develop and implement minimum physical security requirements for data centres.

5.6.3 Standardized procedures for voluntary staff departures, but not for fired or suspended

Organizations with large and complex environments need to have clear and well-understood termination processes that are based on risk assessments and data classification requirements. Processes include the requirement to return issued software, documents, equipment, mobile computing devices, access cards, manuals, and information stored on electronic media. More importantly, the process needs to include timely removal of user access rights to the network, systems, data, and physical areas. If access is not removed and assets are not obtained in a timely manner, terminated individuals could subsequently obtain unauthorized access to government information assets.

Executive Financial Officers are responsible for termination processes within their departments. We obtained the termination processes from the majority and found that 5 departments did not have documented processes and one did not adequately deal with the removal of user access rights and the return of equipment such as laptops, blackberries, and electronic media.

In May 2012, the Provincial Comptroller's Office developed a standardized *Employee Exit Checklist* (EEC) for use when employees voluntarily leave their division (resign, transfer, retire). The EEC includes: deleting network accounts; removing SAP, email, VPN, network, and internet access; and retrieving laptops, blackberries, cell phones and other peripherals, such as building access cards. However, a checklist for use when employees are suspended or fired has not yet been developed.

Recommendation 24: We recommend that the Provincial Comptroller's Office, in collaboration with BTT, create a standard procedures checklist for use when employees are suspended or fired.

6. Contractor IT security practices may not meet government requirements

When contractors are used to manage a process, it is imperative that service standards and other requirements be detailed in the service agreements. Services provided by contractors need to be monitored to ensure that they are meeting performance requirements. In many instances assessing contractor performance will involve independent reviews or audits.

We assessed whether:

- BTT has defined government IT security requirements (section 6.1).
- BTT obtains assurance that contractor security controls are operating effectively (sections 6.2 and 6.3).

6.1 Government IT security requirements not defined

BTT does not define and maintain its own security requirements. Because significant aspects of the IT environment are managed by 4 major contractors (see Figure 1 in the Background section of this report), it is imperative that BTT be able to clearly indicate to each of its contractors the IT security requirements expected.

We examined the 4 service agreements and noted that many IT security requirements are embedded within the agreements. We were advised that, while government requirements were not developed, at the outset of each service agreement, IPC reviewed the security controls proposed by each contractor and, on a case by case basis, determined the appropriateness of the controls proposed. However, without articulating standard IT security requirements, BTT is not in a position to readily determine the adequacy of the practices proposed by a contractor or the consistency of accepted practices between contractors.

We noted that the IT security practices reflected in each of the service agreements are not consistent. Inconsistent IT security practices within the government's large and complex IT environment, if not monitored, increases IT security risk.

Each agreement also itemizes expectations contractors have of BTT. The agreements show that the contractors expect BTT to implement and provide many of the following IT security processes and requirements (all of which were not met):

- data classification standards as well as identification of systems with highly sensitive information.
- IT security policy and supporting policy instruments, including logical access control policies, mobile messaging policies, and encryption standards.
- establish incident handling coordinators.
- emergency procedures to be executed during a facility shutdown.
- audit history.

Recommendation 25: We recommend that IPC establish standard IT security requirements. Once these are in place, we recommend that IPC assess whether the IT security practices of contractors meet the standard requirements and, if there are gaps, that IPC ensure security practices are strengthened.

6.2 Incomplete assurance that contractor IT security controls operate effectively

BTT monitors the service levels provided by contractors by reviewing monthly reports and attending periodic face to face meetings. However, BTT does not obtain any assurance from 3 of the 4 noted contractors that their practices, including IT security, are operating effectively. For Contractor A, BTT obtains independent quarterly assurance reports on practices employed, including some IT security practices; however, these reports do not provide assurance on some significant IT security practices. For example, no assurance is obtained regarding security patch management and firewall effectiveness.

As also noted in section 2.3, in 2006 BTT obtained the services of an independent reviewer to conduct a security assessment at Contractor B. The objective of the assessment was "to provide IPC with an enhanced understanding of the security considerations" for the government network. A report was received in March 2006. The report presented multiple deficiencies and recommendations. BTT did not review the recommendations for appropriateness, develop action plans with the Contractor, and track the implementation of the recommendations.

The lack of assurance that contractor IT security practices are operating effectively increases IT security risks within the environment.

Recommendation 26: We recommend that BTT periodically obtain independent assurance that the IT security practices used by its contractors are operating effectively.

6.3 No assurance over the adequacy of IT security practices at Health's data centre

As noted in the Background section of this report, the IT operations of the Department of Health were not part of the consolidation of IT services into BTT. As a result, IPC is not responsible for IT security within the Department of Health. Without IPC's involvement, IT security practices employed by IPC and by Health, in similar circumstances, may not be consistent, causing potential security risks.

In 2006, BTT chose to house the government's development systems in the Department of Health's data centre. While BTT conducted an *Internal Data Centre Facilities Analysis* in late 2005, it did not include IT risk assessments, including IT security. No subsequent IT risk assessments on the data center have been performed.

A *Memo of Understanding* (MOU) was signed in 2006 and expired in 2009. BTT and ISB told us that this MOU has continued to be carried on in "spirit". The MOU does not define any roles and responsibilities in regards to IT security at the Department of Health's data centre. The MOU defines monitoring of the physical site, but does not define or outline any other IT security controls and practices to be employed by the Department of Health.

BTT does not obtain periodic assurance that the IT security practices at the Department of Health's data centre are sufficient and operating effectively. Developing standard IT security requirements (as discussed in section 6.1) would help BTT determine the adequacy of the IT security practices used by the Department of Health. It is important that BTT obtain assurance over the effectiveness of Health's practices because, in many instances, copies of live production data are used in the development systems housed in data centre, and because IPC has placed their Security Information & Event Monitoring tool (see section 7.3.6) in the data centre. Unauthorized access to the Department of Health's data centre could negatively impact the confidentiality of sensitive government data residing in development systems and the availability of the event monitoring tool.

Recommendation 27: We recommend that BTT develop a new Memo Of Understanding that clearly defines IT security requirements and the relationship between BTT, ISB and the Department of Health.

Recommendation 28: We recommend that BTT obtain periodic assurance over the operating effectiveness of the IT security practices employed at the Department of Health data centre.

7. Security controls in place may not protect network and systems

Implementing IT security controls and practices, based on IT security risk assessments, is fundamental to an information security program. As threats continue to evolve in large and complex environments, IT security risk management helps organizations implement adequate mitigating controls and practices in a cost effective manner.

Because of the lack of IT security risk assessments, as well as IT strategic and IT security plans, as discussed earlier in this report, the rationale for the design and implementation of IT security practices and controls is not well supported. As a result, we cannot comment on the completeness, relevance and effectiveness of the practices in place to secure systems and network operations.

We assessed whether BTT has implemented:

- configuration management practices (section 7.1).
- vulnerability and security patch management practices (section 7.2).
- preventative and detective controls (section 7.3).
- IT security incident handling practices (section 7.4, 7.5).
- disaster recovery plans (section 7.6).

7.1 Weak configuration management practices

The term configuration refers to the way hardware (for example: desktops, laptops, servers), software (for example: applications and databases), and network components (for example: firewalls and routers) are set up. Configuration decisions must be made in a way that strengthens security.

Because items within an IT environment are so interconnected, inappropriate configuration changes can lead to exploitable vulnerabilities within the environment. How components interact can be complex, increasing the risk that improper configuration changes result in significant negative impacts within the environment. For this reason, configuration changes need to be carefully managed.

We assessed whether:

- BTT has implemented a configuration management database (section 7.1.1).
- BTT has developed configuration standards and management processes (section 7.1.2).
- a configuration control board is in place (section 7.1.3).

7.1.1 Configuration management database does not exist

In large, complex, and interconnected environments, organizations need to maintain documentation describing how configurable items are set up and connected. Documentation includes detailed network and information system diagrams. Versions of configurable items in place are also documented and tracked. To ensure complete, accurate, and up-to-date information, this documentation is maintained in a central inventory called a configuration management database (CMDB).

Central inventories help organizations develop and maintain an understanding of how configuration changes impact the environment. Complete, accurate, and up-to-date documentation allows individuals performing the change to be informed of any potential consequences and impacts to the environment.

BTT does not maintain a CMDB. We obtained both high level and detailed network and information system diagrams; but noted that the network diagrams were outdated, incomplete, and pre-dated current BTT initiatives.

Without a complete, accurate, and up-to-date CMDB, individuals performing configuration changes within the government's IT environment may not be aware of how it impacts the environment. Uncoordinated configuration changes may lead to an increased amount of exploitable vulnerabilities.

> **Recommendation 29**: We recommend that BTT implement a configuration management database with updated network diagrams.

7.1.2 Configuration standards and management processes outdated and incomplete

To ensure that configurable items within the environment are secure, organizations establish baseline configuration standards. To change a configuration within the environment, an organization establishes a specific management process.

In July 2005, IPC published baseline security configuration standards for Windows NT, 2000, and 2003 (*IPC Hardening Guide*); however, it does not provide baseline configuration standards for the newer Windows system technologies in use or any other information systems or network components.

BTT has established a process to manage system changes with one of its contractors, but it is not used for configuration changes. In addition, BTT has not developed any other configuration management processes.

Without stringent change management processes and baseline standards, configuration changes may be inconsistently applied, potentially increasing the amount of vulnerabilities within the government's IT environment.

Recommendation 30: We recommend that BTT implement a configuration management process.

Recommendation 31: We recommend that IPC establish baseline configuration standards for all of its information systems and network components.

7.1.3 Configuration control board does not exist

Configuration changes made in large, complex, and interconnected environments require appropriate oversight to ensure that configuration changes meet organizational objectives.

Organizations need to track configuration changes made within the environment, while ensuring complete and accurate documentation is in place.

A configuration control board or oversight body:

- promotes and maintains configuration standards and baselines, as well as, change management processes.
- approves certain configuration changes.
- tracks configuration changes.
- monitors version control.
- coordinates how configurable items interact.
- ensures complete, accurate, and up-to-date documentation resides in the CMDB.

BTT has not established a configuration control board. Of note is that IPC's 1999 operations manual (although no longer in place) referenced an Architecture Configuration Control Board (ACCB) to oversee configuration changes in the environment.

Without effective oversight, particularly in an environment supported by multiple contractors, incorrect or unauthorized configuration changes could occur, increasing the amount of security vulnerabilities within the environment.

Recommendation 32: We recommend that BTT establish a configuration control board or oversight committee.

7.2 Vulnerability and security patch management practices lacking

A vulnerability is a weakness that a threat can exploit to gain unauthorized access to networks, systems, and data. New vulnerabilities within systems (databases, operating systems, and applications) are frequently discovered and published. Vulnerabilities that are not properly mitigated in a timely manner allow unauthorized individuals to circumvent security controls, negatively impacting the confidentiality, integrity and availability of information assets. Vulnerability assessments are a critical component of IT security risk assessments.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. A key mitigation activity is security patch management. A security patch is software that updates an information system to improve usability or to fix known security vulnerabilities.

The cost of identifying, investigating, containing, correcting, and recovering from unforeseen security incidents, far exceeds the cost associated with implementing effective security patch management.

We assessed whether:

- IPC follows a documented vulnerability management methodology (section 7.2.1).
- BTT has security patch management processes (section 7.2.2).

7.2.1 Few authenticated scans performed

A vulnerability management methodology determines, for each system and network in the environment, the vulnerability assessment frequency and depth based on the risks associated with each system.

A technique used by organizations to identify vulnerabilities in their environments is system and network vulnerability scans. A vulnerability scanner is a computer program that looks for weaknesses. Vulnerability scans are performed in two fashions – authenticated and unauthenticated.

Authenticated scans obtain system login credentials (user name and password), allowing the program to look inside the information system or network zone. These scans are thorough and can identify numerous weaknesses that need to be corrected.

Unauthenticated scans do not obtain login credentials and therefore can only look for basic configuration weaknesses (an outside look).

Organizations routinely perform unauthenticated vulnerability scans against all systems on their network. Authenticated scans are conducted on high risk information systems and network zones (organizations place information assets into zones, based on their associated risks).

IPC does not currently follow a vulnerability management methodology. In conducting our 2004 audit on *Computer Security Incident Response Capabilities*, we noted that IPC's 1999 operations manual included a *Generic Vulnerability Analysis Process* for conducting such assessments, but this manual no longer exists.

IPC routinely performs **unauthenticated** vulnerability scans, but only performs **authenticated** vulnerability scans on new applications. The following event highlights the need to perform authenticated scans on high risk systems. In 2008/09, as part of the server consolidation project, BTT performed authenticated vulnerability scans on various government servers. These scans identified over 1,000 high risk security vulnerabilities and over 15,000 missing server patches. (Note: We did not assess whether these vulnerabilities were mitigated.)

Without performing authenticated scans on high risk systems, IPC may not have a complete and accurate inventory of security vulnerabilities within the government IT environment; impacting its ability to mitigate threats in a timely manner.

Recommendation 33: We recommend that IPC develop and implement a vulnerability assessment methodology.

Recommendation 34: We recommend that IPC conduct authenticated vulnerability scans on high risk components within the environment.

7.2.2 Security patch management processes not in place

BTT has outsourced significant portions of its IT processes, including some security patch management. Contractor agreements require that security patches be implemented.

BTT directly manages databases and applications within the environment; but BTT has only documented security patch management processes for a few of these systems.

IPC does not oversee security patch management by either BTT or its Contractors. Without effective oversight, differences in practices between contractors and BTT can occur (for example, the interpretation of patch criticality and related timing requirements) and security patches may not be implemented in a timely manner. We looked at one Contractor's patch levels and found that it was significantly behind on patching high risk security vulnerabilities, leaving systems and data unnecessarily exposed for a prolonged period of time.

Recommendation 35: We recommend that BTT implement security patch management processes for databases and applications.

Recommendation 36: We recommend that IPC monitor the implementation of security patches within the environment.

7.3 Some preventative and detective controls in place, but not well managed

Organizations layer preventative and detective controls within their environment to protect their network, systems, and data from security threats. Examples of preventative controls include firewalls, anti-virus programs, passwords, network access controls, and encryption. Detection controls include intrusion detection systems, intrusion prevention systems, file integrity checking, and security event monitoring.

IPC has implemented a number preventative and detective IT security controls. We identified opportunities for improvement with respect to:

- firewall management (section 7.3.1).
- the application of network segmentation (sections 7.3.2 and 7.3.3).
- data loss prevention (sections 7.3.4 and 7.3.5).
- IT security event monitoring (sections 7.3.6).

7.3.1 Firewalls in place, but are not recently reviewed or tested

Firewalls provide protection against attackers by shielding systems and networks from malicious Internet traffic. They are designed to block the passage of certain data, while allowing data necessary for operations to go through.

Using its major contractors, IPC has implemented several firewalls within the environment. We cannot comment on the adequacy of the placement of the firewalls because of deficiencies noted in network zoning (7.3.2) and network diagrams (7.1.1).

IPC has not recently reviewed firewall design for continuing consistency with current user needs or tested the firewalls for operating effectiveness. As a result, IPC may not be aware of firewalls that are not up-to-date or not performing as designed, increasing the risk of unauthorized access to the government's network, systems, and data.

Recommendation 37: We recommend that IPC periodically review firewall design and test operating effectiveness.

7.3.2 Network segmentation used, but not consistently applied

Network segmentation is the placement of information assets with similar risk attributes into zones. Each network zone would have its own baseline security standards, based on risk. Network zones are designed to control and restrict access and data communications between one another. Using defined baseline security standards for each zone increases the consistency of security practices. Given that organizations have finite resources, high risk zones would have an increased level of security when compared to lower risk zones.

Network zones were most recently defined in IPC's 2003 *Firewall Standard*, but zones noted in this *Standard* are not consistent with the network diagrams provided to us. Furthermore, network diagrams indicate that the zones provided by 2 contractors are not consistent with one another. This could lead to inadequate security practices employed by BTT and contractors. For instance, high risk information assets may be incorrectly placed in a lower risk zone that has a weaker level of security.

Recommendation 38: We recommend that IPC update their zoning standards and network diagrams.

7.3.3 High security zone not fully used

One of the network zones implemented by IPC is a high security zone. IPC's 2003 *Firewall Standard* states that "A high security zone provides a tightly controlled network environment suitable for mission critical servers or systems processing extremely sensitive information." Only Vital Statistics data and a few financial system components have been placed in this high security zone. Within their published security awareness pamphlet, IPC states that the following information, managed within the environment, is highly sensitive:

- witness protection information.
- child abuse records.
- pre-released budget information.
- cabinet minutes and supporting documents.
- pre-trial prosecution files on major crimes.

We are concerned that the highly sensitive information not placed in the high security zone may be at risk of unauthorized access.

Recommendation 39: We recommend that IPC contact system owners to develop a plan to migrate highly sensitive information assets into the high security zone.

7.3.4 Data loss prevention strategy not developed

Sensitive data breaches are commonplace, causing significant financial and privacy impacts. To mitigate this risk, large and complex organizations implement a data loss prevention strategy. The controls included in the strategy protect data in motion (external to and across the network), data at rest (databases and systems), and data at the end point (laptops, mobile and storage devices). The strategy would be based on IT security risk assessments and data classification standards and may include some or all of the following controls: firewalls, intrusion detection systems, anti-virus programs, and encryption.

BTT has implemented some controls to prevent data loss, such as firewalls and intrusion detection systems, but has not developed a data loss prevention strategy. Given the lack of IT security risk assessments and data classification standards, we could not assess the overall adequacy of BTT's data loss prevention controls.

Recommendation 40: Upon completion of IT security risk assessments and the implementation of data classification standards, we recommend that BTT implement a data loss prevention strategy.

7.3.5 Encryption not fully used

Encryption is an effective control to reduce the risk of data loss. Encryption programs scramble data when transmitted or stored and unscramble the data for authorized users. IPC uses some encryption methods, but we identified 2 areas of concern:

- Emails are not encrypted by the sender, increasing the risk of sensitive data being exposed to unauthorized individuals. This is a particular concern because the network is also not encrypted.
- To protect the information on laptop harddrives, BTT uses an encryption method that, according to the vendor, is reasonable for low risk data, but would not be sufficient for highly sensitive data. IPC reported that 14 laptops were lost or stolen in calendar year 2011, yet IPC did not determine the sensitivity of the data residing on those laptops.

Without adequate encryption, there is a risk that sensitive data can be accessed by unauthorized individuals.

Recommendation 41: We recommend that IPC implement email and laptop harddrive encryption methods that appropriately protect all levels of data sensitivity.

7.3.6 IT security event monitoring incomplete

A Security Information & Event Management (SIEM) system provides tools for effective **security event** monitoring, such as data aggregation and correlation, alerting, and performance dashboards. Large organizations utilize SIEM systems to log security events within their environment, determine trends, and alert IT security professionals accordingly.

A **security event** is said to have occurred when an information system or network has been breached or compromised.

IPC has implemented intrusion detection systems and intrusion prevention systems at key points within the network. The systems are monitored by Contractor D using generic security event filtering and triggering. The Contractor sends IPC high risk security events (called "Intrusion detection major events to be investigated by IPC") for investigation and incident handling.

In the spring of 2009, IPC acquired their current SIEM to log security events within the environment. IPC logs events from several sources, including: its firewalls, intrusion detection systems, and anti-virus programs.

IPC does not fully utilize the features of this SIEM as follows:

- event information is not collected from operating systems, databases, and applications.
- no unique triggers or alerts are used when attempting to identify potential security events.
- it is not proactively used to aggregate, correlate, and detect security events.

Within the agreement between Contractor D and BTT, the contractor has agreed to provide technical reviews of how intrusion detection systems and other security event controls are placed within the government environment. IPC officials told us that the placement of security event monitoring controls is discussed with the Contractor during periodic conference calls. However, IPC has not obtained documented technical reviews from the Contractor.

Without complete and proactive monitoring of IT security events within the government environment, IPC cannot effectively identify trends and anomalies that require follow-up in a timely manner. The longer an incident lasts, the more potential there is for damage and loss to government information assets.

Recommendation 42: We recommend that IPC implement a security event monitoring plan, highlighting SIEM system utilization.

7.4 Incident Management Guide in place, but incomplete

Organizations need to ensure that information security incidents are identified and communicated, allowing for timely response. Information security incident handling processes need to be consistent, reliable, and repeatable.

Information security events, and weaknesses that could lead to events, need to be reported through established and appropriate channels as quickly as possible. To do so, organizations must implement security event reporting procedures. Reporting processes need to clearly define response and escalation procedures. Large and complex organizations need to establish, and clearly communicate to all relevant stakeholders, a point of contact for reporting information security events.

Once information security events and weaknesses have been reported, responsibilities need to be understood and procedures need to be in place to ensure timely, effective and standardized responses. Specific procedures are required to handle different information security incidents, such as:

- information system failures.
- loss or denial of service.
- malicious code.
- breaches in confidentiality or integrity.
- misuse of information assets.

Procedures that can be applied to any information security incident include:

- identifying and analysing the cause of the incident.
- containing the damage done.
- taking corrective actions to eliminate the causes.
- reporting the incident and the actions taken to relevant stakeholders and appropriate authorities.

It is useful to analyse incident information to identify recurring incidents as well as opportunities to improve the information security incident handling process.

In October 2003 IPC published the *Incident Management Guide*, establishing the following processes for information security incident handling:

- incident detection and reporting.
- preliminary investigation.

- formal evidence gathering.
- analysis of evidence.
- dealing with Human Resources.
- risk management.

We identified 2 opportunities to improve the guide as follows:

Detailed procedures and checklists not yet developed: IPC's *Incident Management Guide* includes references to a number of standard operating procedures; however, no such procedures exist. In addition, incident handling checklists and workflows are not used to guide IPC staff when following up on a reported incident. Without supporting procedures, workflows, and checklists, there is a risk that IPC's response to information security incidents will be inadequate, untimely, and inconsistent.

Escalation procedures not defined: IPC is responsible for directly managing information security incidents, but escalation procedures within and beyond BTT are not defined. High impact incidents within the government IT environment may require decisions from BTT senior management or other decision makers in the government, for example the decision to disconnect critical government systems from the network in order to contain any damage.

Without clearly defined escalation procedures, IT security incidents with a significant and pervasive impact to the government network and systems may not be properly dealt with, potentially impacting the availability of key processes and services.

Recommendation 43: We recommend that BTT enhance the *Incident Management Guide* by:

a. developing standard operating procedures and workflows.
b. defining escalation procedures.

7.5 Some incident handling practices need to be improved

We assessed whether:

- IPC provides after hours incident response (section 7.5.1).
- IPC documents the handling of information security incidents (section 7.5.2).
- IPC tests the incident management process (section 7.5.3).

7.5.1 After hours IPC incident response is best efforts only

IPC has outsourced information security event monitoring to Contractor D who provides 24/7 detection reporting back to IPC. There is, however, no on-call function at IPC for after hour responses. IPC advised that best efforts are taken to address after hour incidents.

Without an IPC after hours response program, including on-call schedules and procedures, there is a risk that information security incidents may not be handled in a timely manner.

Timely response to identified information security incidents is critical to minimize the potential impact to organizational processes. The longer an incident lasts, the more potential there is for damage and loss.

Recommendation 44: We recommend that BTT establish an after business hours response program.

7.5.2 Security incident reports not prepared, logged, or analyzed

IPC's *Incident Management Guide* provides the following examples of security incidents:

- unauthorized access, or attempts to access, sensitive government information, government assets, or systems.
- missing documents or computer storage media (i.e., diskettes and removable disks).
- unaccountable changes to data and software.
- computer virus infections.
- theft of assets (e.g., laptop computer or personal digital assistants).
- unacceptable use of Internet or email.
- unauthorized access to files or folders.
- password sharing.
- unauthorized access to the government's data network.
- port scanning.
- inappropriate use of government assets as outlined in the *Network Usage Policy*.

The *Guide* indicates that IPC will generate *Security Incident Reports* (SIRS) for each reported incident and notes that these SIRS may be communicated to senior management, employing authorities, Assistant Deputy Ministers, Deputy Ministers, and Treasury Board.

In the 2011 calendar year, IPC noted the following in its quarterly reports to senior management:

- 2,371 viruses detected.
- 64 intrusion detection major events reported by Contractor D to be investigated by IPC.
- 14 laptops stolen.
- 8 lost or stolen blackberries, cell phones, or printers.
- 5 other events deemed "security incidents".

IPC did not prepare SIRS for any of the above noted 2011 security incidents. IPC noted that the incidents were handled primarily through email exchanges. These emails were not organized in any systematic manner. As such we were unable to examine the quality of incident handling. In addition, IPC did not centrally log, track, and analyze information security events and incidents. Logging and tracking information security events and incidents, would help identify recurring and pervasive security trends. Furthermore, without a log of security events, BTT senior management is not readily able to assess the effectiveness of IPC's performance when managing information security incidents.

Recommendation 45: We recommend that IPC document, track, and analyze all information security events and incidents.

7.5.3 Incident management process not tested

IPC does not test their incident management process against various scenarios such as a denial of service attack or a major virus outbreak. Regular testing would help ensure that IPC incident management processes will operate as intended and are well understood. This is particularly important in the government's large and complex environment supported by multiple contractors.

Recommendation 46: We recommend that IPC routinely test information security incident management processes and make improvements as required.

7.6 Minimal disaster recovery preparedness

To support critical processes, organizations need Disaster Recovery Plans (DRP) for the continuation of technology infrastructure and systems after an unforeseen event. In a large and complex environment, a DRP framework helps ensure consistency across implemented plans for critical systems.

BTT has not implemented a DRP framework for government information systems. In addition, BTT has not developed DRPs for their network and systems, including SAP; however, some recovery services are available through contractors, as follows:

- Contractor B is contractually obligated to provide a remote recovery site for critical network operations, including files and emails.
- Contractor A is contractually required to provide disaster recovery services for one mainframe system. However, in the absence of disaster recovery services and plans, the

agreement states that access to the recovery centre provided by the service provider for mainframes is only on a "first-come-first-serve" basis during a disruption. Recovery services for servers would only be provided on a "best effort" basis.

Of note is that Contractor C is not contractually obligated to provide disaster recovery services for the network infrastructure.

We are concerned that little progress has been made in developing DRPs despite our previous recommendations. In our *January 2012* and *December 2007 Reports to the Legislature* we recommended that government develop disaster recovery plans to ensure the continuation of critical business functions during a disruption.

If unprepared for unforeseen events or disasters, BTT may not be able to recover needed systems in a timely manner, negatively impacting important government processes and services.

Recommendation 47: We recommend that BTT implement a comprehensive DRP framework for critical IT services and systems.

Summary of recommendations

For the Department of IEM

Assessing risk (section 1)

1. We recommend that BTT enhance the *ICT Risk Management Model* by requiring consultation with relevant stakeholders within government on their risk tolerances and their willingness to accept residual IT risks.

2. We recommend that BTT complete, on a priority basis, a comprehensive IT risk assessment, which would include an assessment of IT security risks.

3. We recommend that BTT complete an assessment of the risks related to the operations of the LBIS.

Strategic planning (section 2)

4. We recommend that BTT develop an IT strategic plan and a properly aligned IT security plan.

5. We recommend that BTT and IPC identify performance measures for the management of IT security operations, and that a specific target be set for each measure. Once an IT security plan is in place, performance measures and targets should align with the noted security goals and objectives.

6. We recommend that BTT and IPC provide senior management with quarterly reports that focus on:
   a. key performance measures (as agreed to by senior management).
   b. performance in relation to the defined targets.
   c. actions to address any performance shortfalls in meeting objectives.

7. We recommend that BTT obtain, at regular intervals, independent third party audits of its IT security practices, and that progress reports on the implementation of recommendations be provided to senior management.

Developing policies to deal with security risks (section 3)

8. We recommend that BTT annually determine the total costs associated with IT security.

9. We recommend that BTT strengthen its *Policy Management Framework* by requiring that IT risk assessments and strategic objectives support the need for new or updated policy instruments.

10. We recommend that BTT implement an over-arching IT Security Policy.

11. Upon the completion of IT security risk assessments, we recommend that BTT implement additional IT policy instruments needed to mitigate IT security risks.

12. We recommend that BTT strengthen its *Policy Management Framework* by defining the frequency of IT policy instrument review.

13. We recommend that BTT develop a prioritized schedule or plan for the review and update of all existing IT policy instruments and that progress against the plan be actively monitored.

Communicating security policies (section 4)

14. We recommend that BTT amend the ENUP to require new and existing users of the government network, systems, and information assets to acknowledge, either through signature or digital means, their responsibility to comply with the expectations included in the ENUP.

16. We recommend that IPC enhance the security awareness program by:
    a. incorporating the use of IT security incident trends and documented risks.
    b. developing additional security awareness training specifically targeting users in higher risk positions.
    c. using additional awareness techniques.

Safeguarding information assets (section 5)

19. Upon the implementation of data classification standards, we recommend that BTT develop standards and procedures for properly handling electronic media during use.

21. We recommend that BTT obtain periodic assurance that contractors are obtaining security checks on employees with access to government information assets.

22. We recommend that BTT develop logical access control requirements.

23. We recommend that BTT develop and implement minimum physical security requirements for data centres.

Ensuring contractors use adequate security practices (section 6)

25. We recommend that IPC establish standard IT security requirements. Once these are in place, we recommend that IPC assess whether the security practices of contractors meet the standard requirements and, if there are gaps, that IPC ensure security practices are strengthened.

26. We recommend that BTT periodically obtain independent assurance that the IT security practices used by its contractors are operating effectively.

27. We recommend that BTT develop a new *Memo Of Understanding* that clearly defines IT security requirements and the relationship between BTT, ISB and the Department of Health.

28. We recommend that BTT obtain periodic assurance over the operating effectiveness of the security practices employed at the Department of Health data centre.

Securing system and network operations (section 7)

29. We recommend that BTT implement a configuration management database with updated network diagrams.

30. We recommend that BTT implement a configuration management process.

31. We recommend that IPC establish baseline configuration standards for all of its information systems and network components.

32. We recommend that BTT establish a configuration control board or oversight committee.

33. We recommend that IPC develop and implement a vulnerability assessment methodology.

34. We recommend that BTT implement security patch management processes for databases and applications.

35. We recommend that IPC monitor the implementation of security patches within the environment.

37. We recommend that IPC periodically review firewall design and test operating effectiveness.

38. We recommend that IPC update their zoning standards and network diagrams.

39. We recommend that IPC contact system owners to develop a plan to migrate highly sensitive information assets into the high security zone.

40. Upon completion of IT security risk assessments and the implementation of data classification standards, we recommend that BTT implement a data loss prevention strategy.

41. We recommend that IPC implement email and laptop harddrive encryption methods that appropriately protect all levels of data sensitivity.

42. We recommend that IPC implement a security event monitoring plan, highlighting SIEM system utilization.

43. We recommend that BTT enhance the *Incident Management Guide* by:
    a. developing standard operating procedures and workflows.
    b. defining escalation procedures.

44. We recommend that BTT establish an after business hours response program.

45. We recommend that IPC document, track, and analyze all information security events and incidents.

46. We recommend that IPC routinely test information security incident management processes and make improvements as required.

47. We recommend that BTT implement a comprehensive DRP framework for critical IT services and systems.

For the Government of Manitoba (Treasury Board Secretariat)

Communicating security policies (section 4)

15. We recommend that the government make security awareness training mandatory for government employees with access to the electronic network and systems, the immediately upon hiring and periodically thereafter.

Safeguarding information assets (section 5)

17. We recommend that the government:
    a. assign responsibility for information management to an appropriate department.
    b. develop and implement an information management framework.

18. We recommend that the government implement a data classification standard.

For the Civil Service Commission

Safeguarding information assets (section 5)

20. We recommend that the CSC amend their *Security Check* policy to:
    a. require periodic statutory declarations from employees in designated positions, and
    b. once a data classification system is in place, require periodic security checks on employees in designated higher risk positions.

For the Department of Finance

Safeguarding information assets (section 5)

24. We recommend that the Provincial Comptroller's Office, in collaboration with BTT, create a standard procedures checklist for use when employees are suspended or fired.

Response of officials

Department of IEM

Innovation, Energy and Mines accepts the findings of the Office of the Auditor General (OAG).

A number of supporting initiatives are underway and are in various stages of completion and include:

- A comprehensive IT Security Policy is in the final draft stage and consultations with stakeholders will begin shortly.
- A number of major long term IT service contracts are up for renewal which will provide the opportunity to strengthen security controls in outsourced operations.
- New security event monitoring software is being deployed which will improve security event logging.
- A recovery capability review was undertaken by a Disaster Recovery (DR) planning consultant and will provide a foundation on which to develop DR plans.

We would like to thank the OAG for this comprehensive and thorough report which will help guide our way forward. We welcome the recommendations that deal with strengthening our security program, and have already begun to take action on a number of these recommendations.

Government of Manitoba (Treasury Board Secretariat)

We agree with recommendation 15 and will make any necessary changes in training and orientation material.

We agree with recommendations 17 and 18 to strengthen our approach to information management and data classification standards.

Civil Service Commission

The Civil Service Commission agrees with the recommendation and has started to examine the implications as it relates to the Security Check Policy and related policies and practices.

Department of Finance

The Provincial Comptroller's Office agrees with the OAG's recommendation. On November 15, 2012 the Provincial Comptroller emailed all Executive Finance Officers. The email instructed all departments to adopt the Employee Exit Checklist for all departing employees whether to another department or leaving government altogether.

The departments were also instructed that in the case of fired employees the Employee Exit Checklist be implemented immediately or proactively where possible.