January 2014

INFORMATION TECHNOLOGY COMPENDIUM

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250-419-6100
Facsimile: 250-387-1230
Website: www.bcauditor.com

The Honourable Linda Reid
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Madame Speaker:

I have the honour to transmit to the Legislative Assembly of British Columbia my *Information Technology Compendium* Report.

This report contains three separate reports regarding Information Technology (IT). The first report, *An Overview of the BC Government's Capital Spending in Information Technology,* reveals how investing in IT is an essential part of the Government of British Columbia's fiscal plan. The second body of work, *The Status of General Information Technology Controls in the Government of British Columbia*, examines the health of general IT controls across government entities. The third report, *Web Application Security Audit*, assesses the security of government's web applications and if they are protected and managed effectively to minimize security threats.

Since web technologies are constantly evolving, government must develop its websites and online services in accordance with leading security practices and, as much as possible, initiate practices that are one step ahead of potential security threats.

I would like to thank the staff of the Office of the Chief Information Officer, Crown corporations and government entities for their cooperation and assistance during our work on this report.

Russ Jones, MBA, CA
Auditor General
Victoria, British Columbia
January 2014

TABLE OF CONTENTS

AUDITOR GENERAL'S COMMENTS

RUSS JONES, MBA, CA
Auditor General

GOVERNMENT RELIES on Information Technology and the Internet to conduct its daily operations and deliver online services. Whether it's an online application form, license renewal or health record, British Columbians expect that any personal information that government collects from them is protected and secure. They also expect that online services are available 24/7 and provide reliable information.

This report contains three separate reports regarding Information Technology. The first report, *An Overview of the BC Government's Capital Spending in Information Technology*, reveals how investing in IT is an essential part of the Government of British Columbia's fiscal plan. About $500 million is spent annually on IT infrastructure and systems. Large IT projects that have affected most British Columbians in recent years include the e-Health initiative, the Integrated Case Management system, the Gaming Management System, and a new Student Information System. These projects are summarized in this report.

The second body of work, *The Status of General Information Technology Controls in the Government of British Columbia*, examines the health of general IT controls across government entities. General IT controls are a key component in protecting the confidential information that government manages; ensuring the integrity of processed transactions; and verifying that critical government services are available consistently. These controls are expressed as a maturity level that each entity in the B.C. government feels it has attained.

While technology has the potential for increased efficiency and effectiveness, it is not without risks. Fraud, theft, service interruption and privacy breaches are some of the threats to IT systems. The third report, *Web Application Security Audit*, assesses the security of government's web applications and if they are protected and managed effectively to minimize security threats. The audit indicated that government needs to be more vigilant in monitoring the design and implementation of web applications. The audit also includes recommendations for how government entities, through the direction of the Office of the Chief Information Officer, can establish a process to assess, address and continually monitor the threats against government web applications embedded in their websites.

Since web technologies are constantly evolving, government must develop its websites and online services in accordance with leading security practices and, as much as possible, initiate practices that are one step ahead of potential security threats.

I would like to thank the staff of the Office of the Chief Information Officer, Crown corporations and government entities for their cooperation and assistance during our work on this report.

Russ Jones, MBA, CA
Auditor General
January 2014

AUDIT TEAM

IT Capital Spending

Cornell Dover
Ada Chiang
Joji Fortin
Laura Bridgeman

Status of General IT Controls

Cornell Dover
David Lau
Joji Fortin
Kenny Cham
Lillian Kuo
Chelsea Jade Ritchie
Artem Valeev
Mark Vinnish

Web Application Security

Cornell Dover
David Lau
Stan Andersen
Gabriel Botel

RESPONSE TO THE INFORMATION TECHNOLOGY COMPENDIUM REPORT OF THE OFFICE OF THE AUDITOR GENERAL

The Office of the Chief information Officer (OCIO) appreciates the Information Technology (IT) Compendium report recently conducted by your office. The audits that form the basis of the report: The B.C. Government's Capital Spending in Information Technology; The Status of General Information Technology Controls in the Government of British Columbia; and the Web Application Security Audit address important control areas as the B.C. Government offers a greater number of its services via the Internet and faces increasing demand for its financial resources. This timely report has provided valuable information to inform our ongoing efforts to strengthen information security and highlights the significant investment in information technology that is required to support government programs. The protection of information and thoughtful allocation of financial resources are responsibilities and obligations that the B.C. Government takes very seriously.

The report identifies that government spends almost ten per cent of its capital budget on IT systems and infrastructure projects that tend to be very complex in nature. In addition to improving its procurement practices to increase return on investment by seeking joint partnerships with the private sector, the B.C. Government has implemented an IT project assessment process that requires all requests for capital funding for IT projects to be submitted to my office for review. The projects are evaluated and prioritized based on their overall potential value to government programs and to ensure duplicate and low value projects are avoided. The recommended projects are then reviewed by the Deputy Minister's Committee for Technology and Transformation to ensure that government's capital spending for IT projects is focused on the B.C. Government's highest priorities and remains within the approved budget.

The information provided by the General Information Technology Controls review has provided valuable information regarding the maturity of the management of the controls and will assist in prioritizing improvements. My office will continue to urge Ministry Chief Information Officers to improve management of controls to ensure adequate, measurable protection.

The OCIO has developed Security Standards for Application and Web Development and Deployment which were published in December 2012.

RESPONSE FROM GOVERNMENT

In February 2013, the Chief Information Security Officer communicated with all Ministry Chief Information Officers on the need to ensure that the vulnerabilities identified in the audit be properly mitigated. Ministries have reviewed the vulnerabilities of their applications, developed their mitigation plans, and are working to complete implementation. The OCIO is also working to make vulnerability scanning available as a service.

The OCIO accepts the valuable recommendations of the Office of the Auditor General, which are well-aligned with the direction of the government security policy and standards. My office is also appreciative of time provided to mitigate the identified vulnerabilities prior to publication of the audit.

The OCIO continues to improve the protection of government information and responsible allocation of financial resources.

Bette-Jo Hughes
Associate Deputy Minister and Government Chief Information Officer

BACKGROUND

Information Technology (IT) is a significant driver for delivering government programs and services. IT is integrated in almost every aspect of government's business, and crucial to effective, efficient delivery of its services. Technology helps government improve its performance, responsiveness, and accessibility.

Investing in IT infrastructure and systems is recognized as an essential element of capital spending in the Government of British Columbia's fiscal plan. In this overview, we present a summary of government's capital spending in IT. The intent of this information piece is to highlight the significance of the amount of public money spent on IT, and our intention to maintain a focus on this important area in future work that we plan.

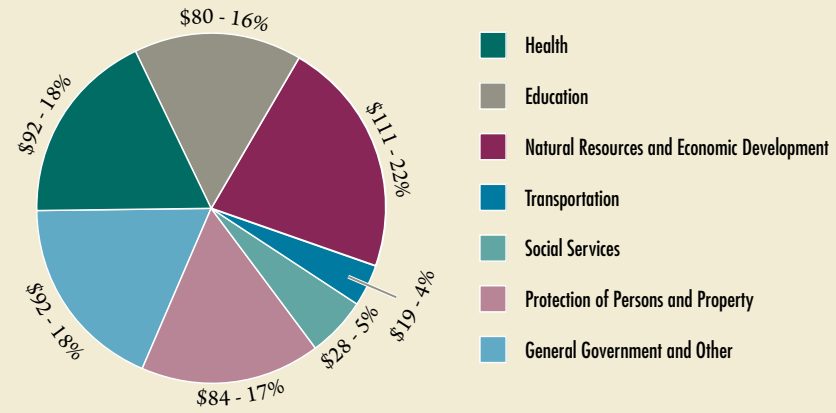
The summary of IT capital spending information presented in this overview is a snapshot of the financial information reported by ministries and organizations that make up the government reporting entity. This includes ministries, Crown corporations, and other public sector organizations such as universities, colleges, school districts, health authorities, and similar organization that are controlled by, or accountable to, the provincial government. We compiled the information primarily from the Summary Financial Statements included in government's Public Accounts and other publicly available information.

IT CAPITAL SPENDING

The government spends approximately $6 billion annually on capital infrastructure projects such as for school additions, hospital expansions, highway improvements, bridge replacements, power generation and transmission, and information systems upgrades across the province. Of that, approximately $500 million is spent on IT infrastructure and systems.

In 2012/13, government spent $506 million on IT capital infrastructure and system additions. Refer to Exhibit 1 for a breakdown of dollars spent by sector.

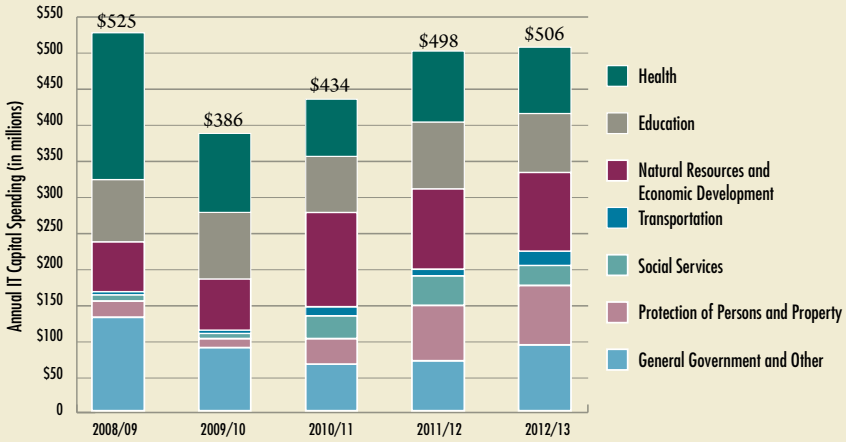
Exhibit 1: 2012/13 IT Capital Spending by Sector (dollars in millions)



Source: 2012/13 Public Accounts and information supplied by certain Crown corporations

Exhibit 2 shows the total amount of IT capital spending, by sector, over the last five years. IT capital spending has decreased from $525 million in 2008/09 to $506 million in 2012/13, representing a slight reduction of about 5%.

Exhibit 2: IT Capital Spending by Sector per Year from 2008/09 – 2012/13



Source: 2008/09 to 2012/13 Public Accounts and information supplied by certain Crown corporations

According to government's 2013 *British Columbia Financial and Economic Review*, the IT capital projects with the greatest cost, more than $50 million, include the:

- e-Health Initiative;
- Integrated Case Management System; and
- Gaming Management System.

e-Health Initiative

The e-Health initiative is a large, multi-year, multi-project initiative that began in 2004. It focuses on the implementation of a province-wide Electronic Health Record system. The aim is to establish an electronic health record for every citizen of British Columbia. E-Health enables healthcare service providers to access quickly patients' health records, health history and care within the health system.

The government is completing the provincial e-Health initiative in 2013 for a total expected capital cost of $262 million.

Integrated Case Management System

The Integrated Case Management (ICM) project was launched in 2008 to replace outdated legacy systems used to deliver social programs such as the Employment and Income Assistance program, the Child Care Subsidy program, and the Child Protection Services program. The project is a partnership of three ministries: Social Development and Social Innovations; Children & Family Development; and Technology, Innovation and Citizens' Services, with changes in service delivery happening at the two social sector ministries.

The ICM system is being implemented over a six-year period with a capital budget of $182 million. The Ministry of Social Development and Social Innovation, the lead Ministry accountable for the project implementation, is looking at completing the project by the end of 2014.

Gaming Management System

In 2012, the BC Lottery Corporation began replacing its existing casino Gaming Management System. This system is used for operating slot machines and monitoring table games in casinos and community gaming centres across B.C. Completion is expected in 2015 for a total capital budget of $104 million.

ALTERNATE IT PROCUREMENT ARRANGEMENT

Implementing new IT systems is complex and costly. Government traditionally invests in IT infrastructure and systems through capital spending. Since early 2000, government shifted its procurement approach for large IT projects to one that undertakes a joint solution approach with the private sector. The current procurement of a student information service for all students in Kindergarten through Grade 12 to replace the existing British Columbia Enterprise Student Information System (BCeSIS) is one example.

Ministry of Education: Procuring the Student Information System as a Service

In the spring of 2011, the Ministry of Education commenced its planning for a new student information system to replace the current BCeSIS. The procurement approach is to provide schools with a student information system that is hosted by a private vendor. The vendor would provide, maintain and operate the platform that runs the new system and provide users with secure access to the information service. With this approach, government would not own the software license or require upfront capital investment for the implementation of the system. Instead, the system would be financed through the Ministry's annual operating budget for the term of the vendor contract.

The Ministry has completed its vendor selection for the contract service. It is anticipated that school districts will begin transitioning to the new service in 2014 and BCeSIS will be decommissioned in early 2016.

LOOKING AHEAD

In recent years, the Government of British Columbia has invested a significant amount of its capital spending in large IT system projects. Our Office plans to conduct audit work that examines the effective management of these projects in achieving benefits and value.

BACKGROUND

Information Technology (IT) is critical to government's day-to-day functions. From delivering services such as healthcare and education to processing billions of dollars in transactions, the Government of British Columbia's IT systems handle sensitive and significant information that impact the daily lives of everyone in our province.

Citizens expect government to have controls in place that ensure sensitive information is protected, transactions are processed correctly and systems are free from lengthy interruption. This includes, among other things, assessing and managing physical risks (such as theft or natural disasters) and digital risks (such as hacking and other unauthorized access). With the fast pace at which technology changes, IT requires constant vigilance and sustained commitment to implement, monitor and adjust controls as necessary.

General IT controls, also referred to as general computer controls, are controls relating to the environment within which systems are developed, maintained and operated. They help ensure proper development and implementation of systems, and help maintain the integrity of systems, data and operations.

This report will inform British Columbians about the health of government's general IT controls.

PURPOSE, SCOPE AND APPROACH

The purpose of this project was to determine the health of general IT controls expressed in terms of maturity level that each entity in the B.C. government has attained with respect to the general controls used for their computing systems and IT environment, particularly regarding:

- protecting the information they manage (*confidentiality*);
- ensuring that transactions are processed correctly (*integrity*); and
- ensuring critical government services can continue (*availability*).

The entities covered in this project include ministries, Crown corporations, universities, colleges, school districts, health authorities and similar organizations that are controlled by or accountable to the provincial government. Trust funds and entities without separate IT functions were excluded.

The project was carried out under Section 12 of the *Auditor General Act*. This is not an audit and we did not provide an opinion on the fairness of the information published. We conducted the project in accordance with the Office's internal quality standards and processes.

We asked 138 B.C. government entities to complete a self-assessment form. The form was designed using the maturity model (see Exhibit 3) defined in the COBIT 4.1[1] framework developed by the IT Governance Institute.[2]

This model is a globally accepted leading practice for measuring how well developed an entity's controls are and in identifying improvements.

We focused on nine general IT controls areas in COBIT 4.1 which are critical to maintaining confidentiality, integrity and availability of information and systems:

1. ***Assessing and managing IT risks:*** analyzing and communicating IT risks and their potential impact on business processes and goals.
2. ***Managing changes:*** responding to business requirements in alignment with the business strategy, while reducing solution and service delivery defects and rework.
3. ***Installing and accrediting solutions and changes:*** implementing new or changed systems that work without major problems after installation.
4. ***Managing third-party services:*** providing satisfactory third-party services while being transparent about benefits, costs and risks.
5. ***Ensuring continuous service:*** ensuring minimal business impact in the event of an IT service interruption.
6. ***Ensuring systems security:*** maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents.
7. ***Managing the physical environment:*** protecting computer assets and business data and minimizing the risk of business disruption.
8. ***Managing operations:*** maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures.
9. ***Monitoring and evaluating IT performance:*** transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements.

Once we received the completed self-assessment forms (with a 100 percent response rate), we reviewed them for completion and compiled the results. As this is not an audit, we did not validate the results of the self-assessments.

A management report was sent to the head of each entity detailing their results compared to similar entities. We also sent a report to the government's Chief Information Officer (CIO), informing her about the report we sent to each entity and providing her the

1 COBIT 4.1 and earlier versions are formally known as Control Objectives for Information and related Technology (COBIT). It is an internationally accepted framework for IT governance, management, control and assurance.

2 IT Governance Institute was formed by ISACA - an independent, non-profit, global association, which engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.

summary results by general IT controls area and type of entity. The government's CIO is mandated with governance authority for standards setting, oversight and approvals for the Province's information and communications technology.

Exhibit 3: COBIT 4.1 Maturity Model Rating Definitions

0 - Non-existent	Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed.
1 - Initial/ad hoc	There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
2 - Repeatable but intuitive	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
3 - Defined process	Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices.
4 - Managed and measurable	Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 - Optimized	Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Source: COBIT 4.1 Framework complimentary download, figure 13, page 19

OBSERVATIONS

Self-assessment results

Exhibit 4 shows the number of entities that assessed themselves at each level per general IT control area.

Exhibit 4: Summary Chart of Maturity Levels for each General IT Control Area

IT Control Areas	Maturity Levels						Average Maturity Rating
	5 Optimized	4 Managed & Measurable	3 Defined	2 Repeatable but Intuitive	1 Initial/ Ad Hoc	0 Non-Existent	
Assess and Manage IT Risks	0	39	28	50	21	0	2.6
Manage Changes	2	50	32	42	12	0	2.9
Install and Accredit Solutions and Changes	7	45	38	33	14	1	3.0
Manage Third-Party Services	5	42	48	28	13	2	3.0
Ensure Continuous Service (BCP/DR)	3	31	45	51	8	0	2.8
Ensure Systems Security	4	33	47	39	15	0	2.8
Manage the Physical Environment	8	38	65	18	8	1	3.1
Manage Operations	10	55	46	25	2	0	3.4
Monitor and Evaluate IT Performance	1	18	31	50	32	6	2.2

Source: Compiled by the Office of the Auditor General of British Columbia

We observed that the average maturity rating for all nine IT control areas is 2.9:

- average maturity levels between 2.2 and 2.9 were assessed for IT control areas such as Assessing and Managing IT Risks, Managing Changes, Ensuring Continuous Service, Ensuring Systems Security and Monitoring and Evaluating IT Performance; and
- average maturity levels between 3 and 3.4 were assessed for IT control areas such as Installing and Accrediting Solutions and Changes, Managing Third-party Services, Managing Physical Environment and Managing Operations.

The ideal maturity level that an entity should operate at for each general IT control area will depend on their business objectives, complexity of their computing systems and IT environment, and the value of the information that they manage. For some entities where the risk factors in these areas are low, it may be acceptable to operate at a maturity level of three. Conversely, where the risks are high, a maturity level of four or five may be more appropriate.

COMPARING SELF-ASSESSMENT RESULTS WITH IT-RELATED FINDINGS FROM FINANCIAL AUDITS

Background

Each year, our Office (along with a number of private accounting firms) audits the financial statements of every entity in the provincial government. The Canadian auditing standards require public sector auditors to obtain an understanding of the entities' business environment and their internal controls for the purpose of formulating audit strategies to ensure financial statements do not contain material errors or misstatements.

At the end of these financial statements audits, internal control weaknesses, including general IT controls, are communicated in a management letter to each government entity through senior management, boards and audit committees. The detailed findings contained in the management letter are cleared with management of each entity and then summarized at a very high level in our Office`s annual *Observations on Financial Reporting* report.

Last year we analyzed the findings related to general IT controls and published them in a separate report entitled *The Status of IT Controls in British Columbia's Public Sector: An Analysis of Audit Findings*. Our intent was to raise awareness of the importance and responsibility of IT controls within the Government of British Columbia.

We mentioned in the report that we would publish an annual report on IT-related audit findings and track government's progress on addressing the risks associated with adopting various forms of IT. This year, because of this general IT controls self-assessment project, we performed a high-level analysis of these findings and relate the results with the self-assessments results for consistency purposes.

Analysis of IT-related findings from financial audits

This analysis includes IT-related findings from audits of financial statements with fiscal periods ending June 30, 2012 (school districts), December 31, 2012 (certain Crown corporations) and March 31, 2013 (all other entities in the B.C. Government).

The analysis indicated that 57 (70%) IT-related findings relate to *Ensuring Systems Security*. This is consistent with the result of self-assessments in Exhibit 4, which shows that the same general IT control area has below average maturity rating (2.8). These findings pertain to:

- weaknesses in access control and password management;
- lack of documented security policy; and
- lack of separation of duties for IT staff or users' functions.

It is understandable that the majority of the IT-related findings were related to *Ensuring Systems Security* as the focus of assessing general IT controls in financial statement audits is on the security of data and integrity of financial information.

The other 24 (30%) IT-related findings pertain to general IT control areas such as Managing Changes, Managing Third-Party Services, Ensuring Continuous Services and others.

WHAT ENTITIES SHOULD DO

Given our knowledge of the structure and complexity of certain entities from our annual financial and IT audit work, we noted that certain government entities rated themselves too high or too low in certain areas. We plan to conduct further work in this area.

We encourage each entity to:

1. review the results of its self-assessment;
2. establish a process to determine the target maturity level for each IT control area;
3. assess the gaps between the current and target maturity level;
4. develop an action plan to address the gaps;
5. implement and monitor the action plan; and
6. perform steps one to five above on a periodic basis.

We also encourage the Office of the Chief Information Officer of the Government of British Columbia to continue assisting government entities in achieving and/or improving the maturity levels for their general IT controls.

LOOKING AHEAD

We look forward to conducting this assessment project annually to keep British Columbians informed about the health of government's IT controls. The information in this report will serve as a foundation for our work in the succeeding years.

Starting next year, we will selectively review and validate completed self-assessment forms. This will involve examining supporting documents and processes to corroborate the self-assessed maturity levels.

BACKGROUND

Websites have been embraced by millions of businesses to communicate and exchange information with their customers and clients. The government of British Columbia uses its websites to interact with its citizens, provide program information and offer online services. Online services include, but are not limited to, applying for a medical service plan, social assistance, permits and licences, legal services, completing a land title search and researching property assessments.

What is a Web Application?

There are two important components of a modern website: 1) web applications and 2) web browsers. Web applications are programs embedded in a website designed to perform specific tasks. From a technical viewpoint, a website is an environment that allows customization through the deployment of a large, diverse range of web applications.

There are many web browsers available with the most popular being Internet Explorer, Firefox, and Google Chrome. Web browsers allow users to retrieve data and interact with content located on web pages within a website.

Features such as webmail, login pages, support, product requests, registration forms, social media, search functions and shopping carts are common web applications used to communicate between the site owner and the user. Web applications are popular due to web browsers which can be updated and maintained without distributing and installing software on web users' computers.

Citizens visiting government websites may be asked to subscribe to newsletters, submit application forms or make an online payment. In these instances, browsing habits are often tracked to enhance future browsing experiences. As well, the data must be captured, stored, processed and transmitted to be used immediately or at a later date. This is done through web applications via a web browser.

Significance of Web Application Security

In the past, cybercriminals used spam emails (or emails sent to numerous recipients) with attached computer viruses or malicious software (called malware) to infect the recipients' computers and steal confidential information. Currently, most cybercriminals exploit a flaw or weakness in the web application's design, implementation, or operation. Exploitation tools are freely available online, can be downloaded by anyone and can be used from anywhere in the world.

Because web applications can capture confidential and sensitive user information, it is imperative that government have appropriate security measures to protect web applications from cybercriminal threats. For instance, government's main website

(www.gov.bc.ca) is a web application portal that provides online access to many services in a wide variety of areas. These online services are public-facing web applications.

Public-facing web applications such as these increase risk to an organization. IT departments tend to focus on building strong network perimeter protection (e.g. firewalls or Intrusion Detection Systems). However, securing the network perimeter is not the only way to stop or detect attacks. For government organizations to stay ahead of attackers, they need to ensure their web applications are securely designed, and have properly managed network security.

Governing Authority and Responsibilities

The Office of the Chief Information Officer (OCIO) promotes and guides the implementation of corporate-wide Information Management and IT policies. The policies provide overall strategic direction for securing government's information technology infrastructure and electronic records and information. The OCIO also ensures that measures are established to assess compliance with security policies, procedures and standards.

Under this mandate, the OCIO established an Information Security Policy framework to guide ministries in the development and security of applications. In December 2012, the OCIO introduced a *Security Standard for Application and Web Development and Deployment*. This new standard is incorporated into the Information Security Policy framework, which all government ministries are required to follow.

PURPOSE, SCOPE AND APPROACH

The purpose of this audit is to determine whether government is effectively managing and securing public-facing web applications from cyber security threats. We assessed whether the OCIO has:

- ensured that government's websites are developed in accordance with leading web application security practices;
- evaluated reported security threats and incidents in a timely manner to continuously improve website security; and
- ensured that ministries have minimized web application vulnerabilities against cyber security threats.

Scope

This audit was carried out under Section 11(8) (b) of the *Auditor General Act*.

This audit focused on the overall governance function of the OCIO and to some extent, the operational relationships between the OCIO and ministries. It also included vulnerability scans on selected public-facing web applications.

We carried out our work between September 2012 and July 2013.

Our Approach

We conducted this audit in accordance with the assurance standards recommended by the Canadian Institute of Chartered Accountants and included tests and procedures necessary to obtain sufficient evidence to support our conclusions. We used traditional audit techniques for assessing the overall IT governance and management areas.

The BC government has approximately 1,500 web applications of which 437 are public-facing. The majority of these are hosted within the Shared Services BC government network. From those, we selected a sample of public-facing web applications for assessment of vulnerability using industry standard scanning tools and methods. We selected public-facing web applications hosted within the government network that were identified as:

- business and mission critical;
- had a high or moderate impact risk to the health, safety, security, or economic well-being of British Columbians, and
- had a high or moderate impact risk of disruption to a department's service levels, contractual obligations with third parties, obligation to obey the law, regulatory obligations, and their obligations to other government departments, other levels of government, and/or foreign governments.

What We Did Not Look At

We excluded the Ministry of Justice because a similar audit of the government's computerized criminal justice application was conducted and reported by our office in 2012: *Securing the Justin System: Access and Security Audit at the Ministry of Justice*.

Vulnerability scans such as those which we conducted can sometimes inadvertently and negatively affect a web application's service. Because of this, and to avoid public safety risks, we excluded applications that provide travel and recreational safety warning information.

We did not include non-core government organizations, such as Crown corporations, agencies, schools, colleges, universities and health authorities. These entities may be considered for future audits.

OVERALL OBSERVATION AND CONCLUSION

The OCIO developed and implemented policies and standards for the development of web applications in late 2012. Although the OCIO has taken some actions in addressing the security of web applications, we concluded that they are not enough to protect web applications from cyber security threats.

We found that the OCIO has not:

- incorporated the compliance review of web application development policies and standards as part of its annual review of ministries' self-assessment;
- verified the accuracy and completeness of ministries' application inventories;
- fully implemented a process for evaluating vulnerabilities of public-facing web applications; and
- established a formal process to investigate and follow-up on results of vulnerability scans for all public-facing web applications.

KEY FINDINGS AND RECOMMENDATIONS

Website Development Using Leading Security Practices

In the area of security leading practices, we assessed:

1. whether policies and standards are in place for web application development and if so, whether they are in accordance with security leading practices;
2. whether roles and responsibilities for web application security are clear between the OCIO and ministries; and
3. how well the OCIO monitors ministries' compliance with web application development policies and standards.

Effectiveness of the Web Application Development Standard

As previously mentioned, in December 2012, the OCIO released the *Security Standard for Application and Web Development and Deployment.* We compared this standard with standards and practices from leading security organizations and found that it addresses key risks related to the secure development of web applications.

Roles and Responsibility

The OCIO has the overall responsibility for ensuring web applications are developed and maintained in accordance with security leading practices. The office also provides strategic advice and sets the overall direction and standards for IM/IT relating to government's entire IT environment.

Conversely, ministries are responsible for developing and maintaining ministry information and business applications, including web applications in accordance with the OCIO standards. Responsibility for compliance with standards and policies falls to the Ministry Chief Information Officer (MCIO). The MCIO deals with day-to-day information security issues within his/her ministry and helps ensure compliance with policies and standards. He/she reports directly to the respective Deputy Minister, and has a functional reporting relationship with the OCIO through various committees.

We found that roles and responsibilities between the OCIO and MCIO are clearly defined and communicated.

Compliance with Policies and Standards

Government's current policies and standards provide ministries with guidance for developing and maintaining web applications. Ministries conduct annual self-assessments of their IT security, which the OCIO reviews to ensure there is adequate support for the assertions. However, OCIO's review does not look to see if ministries are in compliance with the web application development policies and standards.

RECOMMENDATION 1: ***We recommend that the Office of the Chief Information Officer (OCIO) incorporate a compliance review of web application development policies and standards as part of its annual review of ministries' self-assessments.***

Evaluation of Reported Security Breaches/Incidents

We assessed the effectiveness of current policies and processes for tracking and resolving web application security incidents. We also reviewed how well cyber threats are monitored and investigated, and steps for improving web application security.

Tracking and Resolving Security Incidents

Security incidents are unwanted events that threaten privacy or information security. Web application security incidents include the accidental or deliberate unauthorized use of, disclosure of, or access to data.

The OCIO's *Information Security Policy* clearly identifies roles and responsibilities for affected personnel in reporting and mitigating security events for prompt resolution. Other guides designed to assist personnel with reporting, logging and resolving information security incidents include:

- *Information Incident Management Process*
- *Easy Guide for Responding to Information Incidents*
- *Information Incident Checklist*
- *Process for Responding to Privacy Breaches*
- *Information Incident Report Form*

The existing policies and procedures are effective in providing guidance for tracking and resolving web application security incidents.

Monitoring and Investigating Threats and Incidents

Staying ahead of security threats and incidents can be a daunting task. New vulnerabilities are reported daily and where a web application was once considered secure, it could be vulnerable the next day. Therefore, the OCIO should have a process for staying abreast of security threats and incidents, and informing ministries so they can mitigate the risk of web applications being exploited.

To accomplish this, the OCIO has established a special investigations unit to identify and track information cyber threats and incidents (both external and internal) to government. This unit works closely with the federal government's Canadian Cyber Incident Response Centre and other partners inside and outside of Canada to mitigate cyber threats to vital networks.

Information security incidents within government, regardless of priority, are immediately logged and forwarded to the OCIO's investigation unit. After review, they are assigned to an Incident Action Team to determine overall response strategy and work assignments.

We found that the process established by the OCIO is reasonable for monitoring and investigating web application security threats and incidents. However, due to the evolving threats, the OCIO should continuously review the sufficiency of the process for monitoring cyber security threats.

Improving Security

The OCIO's investigations into web application threats and incidents have resulted in a number of corporate-wide initiatives including a comprehensive *Information Security Program and Security Assurance Process*.

The *Information Security Program* addresses the need for improving information governance and the protection of government information assets at a corporate-wide level. Initiatives include action items for addressing cyber attacks and development standards for applications and web security.

The *Security Assurance Process* aims to develop and maintain standards and tools for ministries to test for possible web application security deficiencies and is expected to include an audit program for assessing ministry compliance with the standards. Ministries will be able to draw from a list of web application vulnerability scanning services once it is fully implemented.

The OCIO is taking appropriate measures to improve overall web application security.

Awareness of the Extent of Website Vulnerabilities

As part of our work, we first reviewed the OCIO's process for maintaining an accurate inventory of all government applications including public-facing web applications. We then performed our own vulnerability scans on selected public-facing web applications. Lastly, we examined the OCIO's process for investigating and following-up on the results of their vulnerability assessments.

Inventory of Applications

Businesses often depend on an accurate and detailed record of their assets to operate and maintain competitiveness. Therefore, up-to-date inventory records should provide management with essential information on how many assets they have in inventory, what the assets are, and where they are stored or located. This information can then be used to properly plan, budget, and safeguard the assets.

In the case of government IT assets, it is equally important to know what IT assets are owned, their purpose, and where they are installed. Without this detailed knowledge, it would be difficult for management to assess their criticality and security status.

In 2011, the OCIO implemented a formal applications record management process requiring each ministry to collect and maintain a list of applications on a spreadsheet for which it is responsible.

The collection included a detailed description of each application's:

- hardware,
- software,
- purpose,
- cost,
- age,
- hosting environment,
- risk classification,
- criticality, and
- impact on government if it failed.

This information is uploaded to the OCIO and compiled into a master inventory list. We found that the master inventory spreadsheet of web applications was inaccurate and missing information. Over 22% were missing one or more key data fields such as information security classification, criticality, impact on British Columbians and government operations, web application internet address, and the status of the most recent *Security Threat Risk Assessment*.

As a result, the OCIO may be relying on an inaccurate and incomplete inventory, which could negatively affect decisions regarding safeguarding of government's web applications.

RECOMMENDATION 2: ***We recommend that the Office of the Chief Information Officer (OCIO) establish a process to ensure the accuracy and completeness of its web applications master inventory list.***

Vulnerability Scans

To determine the vulnerability status of public-facing web applications, we conducted vulnerability scans on 80 public-facing web applications using industry standard scanning tools and methods.

We conducted vulnerability scans between December 2012 and February 2013.

Vulnerability Severity Levels

Vulnerabilities are defined according to the risk level they pose to the application. We chose to use vulnerability rankings as determined by HP WebInspect. HP assigns severity levels based on whether the vulnerability allows the attacker to execute commands, retrieve or modify private information, view source code, or access system files and other sensitive information.

For reporting purposes, we focused on critical, high and medium vulnerability severity levels (see Exhibit 5).

Exhibit 5: HP WebInspect Rankings

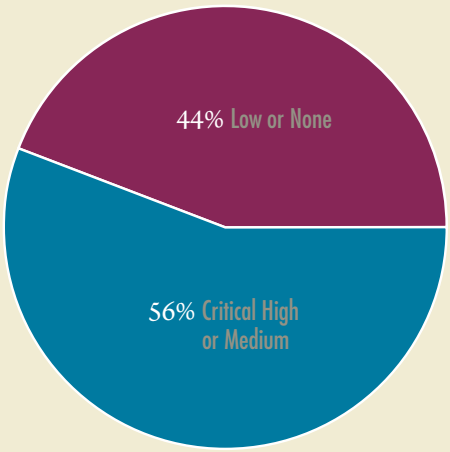
Severity	Description
Critical	A vulnerability that could let an attacker execute commands on the server, or retrieve and modify private information
High	A vulnerability that could let an attacker view source code, access system files, and view sensitive error mesages
Medium	Other errors or issues that could be sensitive
Low	Interesting issues that could potentially become higher issues

Source: Compiled by the Office of the Auditor General of British Columbia

Results

Of the 80 public-facing web applications scanned, 56% had one or more critical, high or medium vulnerabilities (see Exhibit 6). These vulnerabilities could allow cyber criminals to access confidential information or cause malicious activity.

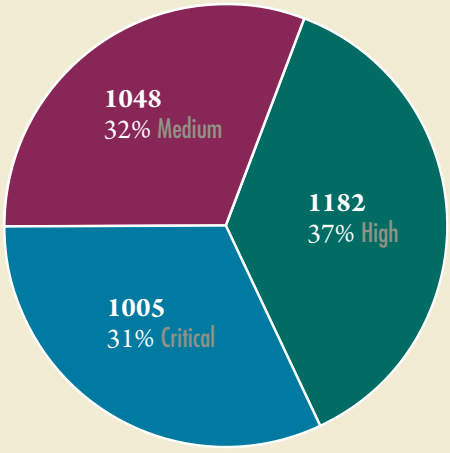
Exhibit 6: Percentage of public-facing web applications scanned by vulnerability severity level



Source: Compiled by the Office of the Auditor General of British Columbia

Of the critical, high and medium vulnerabilities found, we identified over 1000 vulnerabilities for each of the severity levels (see Exhibit 7).

Exhibit 7: Number of vulnerabilities identified and grouped by severity



Source: Compiled by the Office of the Auditor General of British Columbia

Based on the high number of critical, high and medium vulnerabilities found per web application, we determined that public-facing web applications are not adequately protected from cyber security threats. As a result, there is a high risk for loss of confidential information and service availability.

RECOMMENDATION 3: ***We recommend that the Office of the Chief Information Officer (OCIO) work with ministries to facilitate regular vulnerability scans for all public-facing web applications.***

Following-up on Vulnerability Scans

During our audit, we reported the results of our scans to the OCIO and commended the office for taking immediate corrective action to address the vulnerabilities.

However, the OCIO has not established a formal process to assess and follow-up on the vulnerability status for all public-facing web applications. Without knowing the status of all public-facing web applications, the OCIO would not know whether government website vulnerabilities are minimized against cyber security threats.

RECOMMENDATION 4: ***We recommend that the Office of the Chief Information Officer (OCIO) work with the ministries to establish a formal process to promptly investigate and follow-up on the results of vulnerability scans for all public-facing web applications.***

Summary of Recommendations

We recommend that the Office of the Chief Information Officer (OCIO):

1. incorporate a compliance review of web application development policies and standards as part of its annual review of ministries' self-assessments.
2. establish a process to ensure the accuracy and completeness of its web application master inventory list.
3. work with ministries to facilitate regular vulnerability scans for all public-facing web applications
4. work with ministries to establish a formal process to promptly investigate and follow-up on the results of vulnerability scans for all public-facing web applications.

LOOKING AHEAD

As government organizations continue to increase reliance on websites to communicate and deliver services, it is imperative that the web applications used be designed and implemented with strong controls. This will inhibit fraudulent users from accessing information through cyber attacks.

Looking forward, the Office of the Auditor General will:

- continue to monitor government's effort in securing public-facing web applications; and
- extend our review of web applications security to other government entities such as Crown agencies, schools, universities, colleges and health authorities.

OFFICE OF THE
Auditor General
of British Columbia

Location:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

Office Hours:
Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll free through Enquiry BC at: 1-800-663-7867
In Vancouver dial 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website:
This report and others are available at our website, which also contains further information about the office: www.bcauditor.com