Report 3: July 2012

THE STATUS OF IT CONTROLS IN BRITISH COLUMBIA'S PUBLIC SECTOR: AN ANALYSIS OF AUDIT FINDINGS

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

Library and Archives Canada Cataloguing in Publication

British Columbia. Office of the Auditor General
The status of IT controls in British Columbia's public sector [electronic resource] : an analysis of audit findings.

Includes bibliographical references and index.
Electronic monograph in PDF format.

ISBN 978-0-7726-6591-1

1. Finance, Public--British Columbia--Accounting--Data processing--Evaluation. 2. Administrative agencies--Information technology--British Columbia--Management. I. Title.

HJ9921 Z9 B74 2012 352.4'309711 C2012-980136-4

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

OFFICE OF THE
Auditor General
of British Columbia

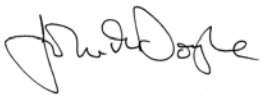
8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250-419-6100
Facsimile: 250-387-1230
Website: www.bcauditor.com

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

Dear Sir:

I have the honour to transmit to the Legislative Assembly of British Columbia my 2012/2013 Report 3: *The Status of IT Controls in British Columbia's Public Sector: an analysis of audit findings.*

Since 2008, my Office has provided a high-level overview of IT control deficiencies in the public sector in our annual report on government's public accounts, *Observations on Financial Reporting*. This year, however, the continued persistence of these deficiencies led us to review the findings more closely, and report our analysis separately in order to highlight both their significance and the pressing need for action to address them. Going forward, we plan to continue to publish IT-related findings from the audit of public accounts as a separate report.



John Doyle, MAcc, CA
Auditor General

Victoria, British Columbia
July 2012

TABLE OF CONTENTS

AUDITOR GENERAL'S COMMENTS

JOHN DOYLE, MAcc, CA
Auditor General

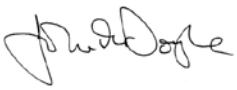
GOVERNMENT INCREASINGLY relies on information technology to conduct operations and deliver services. While technology has the potential for increased efficiency and effectiveness, it is not without its risks. Fraud, theft, service interruption and privacy breaches can be some of the threats to IT systems and information.

We face these risks as individuals in an ever-advancing technological landscape; companies face them as part of doing business and government, too, must prepare for and manage their IT environment to minimize the potential consequences of these threats. However, despite five years of identifying inadequate IT controls, significant problems persist in B.C.'s public sector.

Since 2008, my Office has provided a high-level overview of IT control deficiencies in the public sector in our annual report on government's public accounts, Observations on Financial Reporting. This overview is derived from the detailed letters auditors send to the management of every organization in the government reporting entity as part of our audit, identifying any problems with the preparation of their financial statements. This includes relevant IT systems and processes.

Despite being advised of control issues with IT year after year, IT deficiencies accounted for 30 per cent of the audit issues communicated to the public sector entities for fiscal years ending in 2011. This percentage, and the persistence of these issues, led us to review the findings more closely, and report our analysis separately in order to highlight both the significance of these deficiencies, and the pressing need for action to address them.

Going forward, we plan to continue to publish IT-related findings from the audit of public accounts as a separate report. We will also be tracking government's progress on addressing IT risks, and continue to audit, and report publicly on, the various forms of IT government has adopted.



John Doyle, MAcc, CA
Auditor General
July 2012

PROJECT TEAM

Cornell Dover,
Assistant Auditor General

David Lau,
Director

Raveendran Madappattu,
Manager

BACKGROUND

Information technology in the public sector

THE B.C. PUBLIC SERVICE is increasingly relying on information technology (IT) to gather information and deliver services. The public's expectation for personalized information technology services is also increasing, which is driving the development of more complex IT applications (e.g. i-services, cloud computing, virtualization).

Protecting the accuracy, integrity and confidentiality of IT systems used to collect and store public information and to deliver public services is a serious responsibility for public sector organizations. Information collected from citizens by government organizations must be managed in a safe and ethical manner and protected from misuse.

Threats to IT systems and information can be serious and tied to risks such as: poor data collection and validation (i.e. incorrect information collected and not checked for accuracy), fraud (i.e. individuals providing dishonest or deceitful information, or using information for dishonest or deceitful purposes), IT information and hardware being virtually or physically lost or stolen, and disruption of IT services.

Managing information technology in the public sector

Public sector organizations must ensure they have plans, policies, procedures and resources in place to protect the accuracy, integrity and confidentiality of information technology systems and the data contained in these systems. Frameworks for effective IT governance and control include a number of important elements, including the following:

- Corporate IT governance of information technology
- IT process, control and compliance
- IT change and risk management

A number of business frameworks have been developed to foster and support the harmonization of organizational objectives with IT governance and control. One of the best known frameworks is COBIT (Control Objectives for Business Information Technology). Developed by the Information Technology Governance Institute, COBIT integrates many different good IT practice models into a single guiding framework. We use this guidance in our audits and examinations.

Auditing information technology controls in the public sector

The Canadian Institute of Chartered Accountants (CICA) assurance standards require public sector auditors to obtain an understanding of the entities they audit, including their business environment and their internal controls. The purpose of this work is to identify and assess risks and formulate audit strategies to ensure financial statements do not contain material errors or misstatements.

At the end of every fiscal year, our Office (along with a number of private accounting firms) audits the financial statements of every organization in the provincial government reporting entity (163 organisations in 2010/11.) Audit findings are communicated to government oversight bodies (i.e. ministries, boards and audit committees) and senior management using what is typically called a management letter. Management letters identify problems that need to be addressed, including issues related to information technology and information collection and management.

For more information on management letters and the information they provide, please see our 2010/11 annual observations report, *Observations on Financial Reporting: Summary Financial Statements*.

PURPOSE AND SCOPE

The analysis presented in this report reinforces the importance of the other IT work our Office has undertaken in past several years (click here to read the Office's IT reports), and emphasizes the need for stronger IT governance and control in the public sector.

This report focuses only on management letter points resulting from our assessment of financial applications. It covers off work undertaken during the fiscal years ending March, July and December 2011.

We reviewed the audit findings in 154[1] management letters and found that 30 per cent of audit issues communicated to public sector entities were related to information technology general controls (ITGC) deficiencies. This is a noteworthy percentage; therefore, we reviewed findings more closely, and identified larger, more systemic, issues and risks associated with them. We organized our analysis into the following five categories:

- Information Security Management—ensuring IT Systems and data are protected
- Information Technology Control Environment—organizational IT leadership, tone, and culture
- Available Data Processing—maintaining business operations at all times
- Change Management—updating and replacing IT systems in a controlled and coordinated manner
- Physical Security—protecting IT systems from physical threats

We conducted this work under Section 11.8 of the *Auditor General Act*.

SUMMARY OF OBSERVATIONS

We documented ITGC weaknesses across all sectors of the government reporting entity. The Information Security Management category had the most documented weaknesses, followed by the IT Control Environment category. Table 1 provides a breakdown of the results.

These findings do provide some indication of weak ITGCs within the government reporting entity. However, before drawing conclusions from this analysis, there are some limitations to consider. Management letters are not standardized documents. The contents of these letters depend on what auditors view to be the key risks to organizational financial reporting at the time of their audit. Therefore, even though IT Control Environment issues were not documented in the Health Sector, it does not mean they do not exist – it may not have been an area of focus for auditors as it did not represent a high risk to the overall accuracy of financial statement reporting.

Regardless, while some IT control gaps may seem insignificant, they can leave an organization vulnerable to serious threats of system and application compromise when combined with other control gaps.

Table 1: ITGC management letter issues by government sector

ITGC Categories	Ministries	Crown Corporations	Schools	Universities and Colleges	Health Authorities	Total # of Issues	Per cent of Total
Information Security Management	1	13	19	17	2	52	55%
IT Control Environment	-	2	8	6	-	16	17%
Change Management	1	3	6	4	-	14	15%
Availability of Data Processing	-	3	5	2	-	10	11%
Physical Security	-	-	1	1	-	2	2%
Total	2	21	39	30	2	94	100%
# of entities with issues/total entities in sector	1/18	8/43	12/60	11/25	2/17	34/163	

Source: Government Reporting Entity Audit Management Letters for fiscal years ending in 2011

1 Nine of the 163 organizations looked at did not receive management letters.

DETAILED FINDINGS

Information security management

To effectively manage threats and risks to sensitive information, organizations must have robust information security management to guard against loss of key or sensitive information being stolen or altered.

Public sector organizations should have information security management policies and procedures in place to manage information asset risks and keep information security risks low. This includes: regular reviews of computer systems hardware and software, robust procedures to identify, assess and resolve operational processing errors, and active enforcement of key security policies (e.g. user access management).

We found that 55 per cent of IT-related management letter issues identified problems pertaining to inadequate information security management. For example, we found that:

- account management (to ensure that only appropriate users accessed sensitive information) was poor;
- strong passwords and periodic changes of passwords were not enforced; and
- separation of duties within IT operations (to ensure that no one is in the position to conceal illegal acts or frauds) was inadequate.

Failing to have a strong information security management can increase the likelihood of corporate data or personal information being used for fraudulent purposes.

Information technology control environment

The IT control environment normally consists of a control framework designed to shape the corporate culture or 'tone at the top' and, most importantly, meet business objectives. This includes adequate policies and procedures pertaining to information and information technology. All public sector organizations should have adequate practices and policies for managing IT operations and for assessing and identifying risks that may affect key business objectives.

Our review of management letter points revealed that 17 per cent of IT-related management letter findings documented concerns pertaining to entities' IT control environment. For example, we found that:

- IT strategic plans and policies were neither in place, nor kept up-to-date with business goals and objectives;
- IT staff training was not being kept up-to-date with rapid changes in technology; and
- contract management processes were insufficient to hold contractors or service providers accountable for their deliverables and security measures.

Failing to have a strong IT control environment increases the likelihood that organizations will not be able to identify, assess and resolve threats to IT operations on a timely basis and, furthermore, not be able to meet their business objectives.

Change management

Changes to IT systems are made all the time and have to be carefully managed. Change management ensures that standardized methods and procedures are used for prompt and effective handling of all changes to IT systems or applications.

Public sector organizations should have IT change management plans in place in order to maintain the proper balance between the need for change and the potential negative impact of changes.

We found 15 per cent of IT related management letter points pertained to inadequate change management. For example, in some instances:

- formalized change management policies and procedures to guide testing and implementation of changes/upgrades of software or systems did not exist;
- IT changes were not documented properly with appropriate sign-off by concerned parties; and
- post-implementation reviews were not conducted to ensure changes were implemented correctly.

Inadequate change management increases the risk that systems and applications will not process information as intended, and an organization's operations and services will be disrupted and incorrect information may be produced. There is also a greater chance that information will be lost and that access may be granted to unauthorized persons.

Availability of data processing

Disaster Recovery Plans (DRPs) document the steps necessary to resume normal businesses operations as quickly as possible in the event of disruptions to data processing. Public sector organizations should have DRPs in place and they should be backing up data and system information in a secure location off-site.

We found that 11 per cent of IT-related management letter issues pertain to entities failing to maintain effective, up-to-date DRPs, and back-up data off-site.

Failure to maintain an effective DRP and back-up data in a secure off-site location increases the risk that normal business operations will not be able to be restored efficiently and effectively in the event of human error or natural disaster that disrupt data processing.

Physical security

Good physical security measures are designed to deter and delay attacks from intruders, and detect and respond to intrusions. Public sector organizations should implement good physical security to protect their information assets. Physical security includes strong security practices to prevent unauthorized access to IT infrastructure and the data contained within IT systems.

We found that only 2 per cent of IT-related management letter issues identified a lack of adequate physical security. This finding, however, does not provide assurance that physical security is well managed in the public sector. Physical security has the least immediate impact to the overall accuracy of the financial reporting. Therefore, some auditors may have not reviewed this control category closely.

It is important to note that without good physical security measures, attackers or even accidental intruders may be able to steal equipment or devices that have sensitive and important data stored in them. Public sector organizations must always be vigilant in designing security measures to balance security features and a tolerant amount of personnel access against important and sensitive assets.

LOOKING AHEAD

As government organizations continue to introduce sophisticated IT systems to save costs, share data and capture valuable information about their customers, citizens, employees and suppliers, the overall impact will be a dramatic increase in the need for management of information security to ensure data quality and integrity for financial reporting.

Looking forward, our Office will:

- continue to focus on reviewing the design and existence of general computer controls that are considered significant to credible financial statement audits;
- expand the scope of general computer control reviews to include the assessment of the reliability of certain key application controls for operating effectiveness;
- consider how private sector accounting firms can focus on IT controls within the public sector entities they audit; and
- conduct IT performance audits that will have a positive influence on government and its entities in IT security management practices. By doing this, we will examine different IT management issues including: value delivery, IT security, privacy, governance and project management.

We will be publishing an annual report on IT-related audit findings and tracking government's progress on addressing the risks associated with adopting various forms of IT in their businesses. We are also working on several IT-related audits, which we expect to release later in 2012.