



December 2015

THE STATUS OF GOVERNMENT'S
GENERAL COMPUTING CONTROLS: 2014

www.bcauditor.com

CONTENTS

<i>Auditor General's Comments</i>	3
<i>Report Highlights</i>	5
<i>Response from The Ministry of Technology, Innovation and Citizens' Services</i>	6
<i>Background</i>	7
<i>What we did</i>	8
<i>What we observed</i>	10
<i>What organizations should do</i>	17
<i>Appendix A: Maturity level by IT process and type of organization</i>	18
<i>Appendix B: Summary of IT audit recommendations over the last 10 years</i>	23

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1
P: 250.419.6100
F: 250.387.1230
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 report, *The Status of Government's General Computing Controls: 2014*.

We conducted this audit under the authority of sections 10 and 11 (8) (b) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Canada Handbook – Assurance, and in accordance with Value-for-Money Auditing in the Public Sector.



Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
December, 2015

AUDITOR GENERAL'S COMMENTS

INFORMATION TECHNOLOGY (IT) systems are vulnerable to threats like hacking, theft, and systems disruption due to physical damage or sabotage. For government IT systems, there's even more at stake because these systems contain substantial – and sensitive – information. We rely on IT systems for essential services like healthcare, education and transportation, and for millions of financial transactions across all government organizations.

Strong general computing controls are government's first line of defence against potential threats. They control who can access the systems (confidentiality), how to make changes to the systems (integrity), and backup and recovery of systems (availability).

We've seen issues with general computing controls in previous audits of IT systems, including PARIS, CORNET, JUSTIN, ICM, and wireless networks in government. Over the last 10 years, 78% of the recommendations in our IT audit reports have been about improving general computing controls, thus illustrating their importance.

For this report, we looked at how good government's general computing controls are, and how good government organizations think they are. To do this, we asked 148 government organizations (ministries, Crown corporations, health authorities, universities, colleges, schools and more) to self-assess how well-developed and capable their general computing controls are. This is known as the maturity level. We then validated 13 self-assessments from across all types of organizations.

The majority of organizations self-assessed at maturity level 3 and above. However, in our validation, we found that 69% of organizations over-rated their self-assessments. They didn't have sufficient evidence to support their self-assessments. And most of the organizations lacked documentation of policies and procedures – both hallmarks of mature



CAROL BELLRINGER, FCPA, FCA
Auditor General

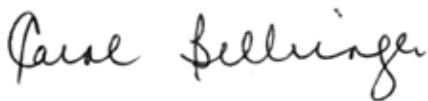
AUDITOR GENERAL'S COMMENTS

general computing controls. We encourage all organizations to take a critical look at their IT processes and be realistic about their level of maturity.

We believe that each organization should aim for at least maturity level 3 as their baseline. That said, some organizations should have a higher target maturity level, especially those that have complex computing needs or handle sensitive information.

The findings and recommendations from this audit should be of interest to all IT professionals in government organizations. Senior management needs to fully understand the importance of general computing controls and how they can mitigate threats to their IT systems. We are recommending that organizations review their business and IT goals, and determine which maturity level is best suited for their needs, and then, ensure that maturity level is achieved and maintained.

We are grateful to all 148 organizations for completing their self-assessments. We had a 100% response rate, which helps to make our job easier. And thank you to the 13 organizations whose results we validated – we appreciate your cooperation.



Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
December, 2015

REPORT HIGHLIGHTS

USE OF IT COMES WITH RISKS:

**FRAUD
ERRORS
SYSTEM
DISRUPTION**



Strong general computing controls can reduce the impact of risks.

78%

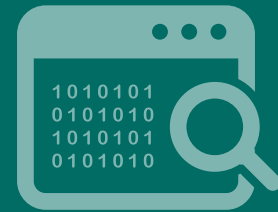
of our previous **IT audit** recommendations were about **general computing controls**

BC government organizations **SELF-ASSESSED A HIGHER AVERAGE MATURITY LEVEL THAN 2013**

Majority of organizations self-assessed at



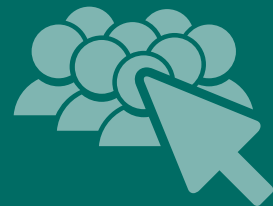
69% of audited organizations lacked sufficient evidence to support their self-assessed levels



IT is critical

to government's service delivery – from healthcare to education

Over **600** **IT services** are **outsourced** to external parties



RESPONSE FROM THE MINISTRY OF TECHNOLOGY, INNOVATION AND CITIZENS' SERVICES

THE OFFICE OF the Chief Information Officer (OCIO) would like to thank the Auditor General for reviewing the status of Government's General Computing controls. Government takes very seriously the importance of general computing controls as the first line of defense against potential threats, and is committed to ensuring ongoing confidentiality, integrity and availability of systems and data under its mandate.

I accept the Auditor General's recommendation pertaining to the Government Chief Information Officer's role in promoting strong controls and assisting organizations with implementing them, and will continue to carry out this role within my mandate. I have taken prompt and appropriate action and have planned future improvements, to the extent that my office is empowered to do so under the government Core Policies.

To date, we have completed our Annual Information Security Review and created a Vulnerability and Risk Management Team to respond to relevant incidents, integrated formal security requirements into vendor service procurements, implemented advanced cybersecurity and vulnerability scanning tools, published new standards for Critical Systems and Enterprise Business Architecture to be applied by all ministries, formalized the Terms of Reference and processes for OCIO's Change Advisory Board, and completed government's annual Business Continuity Plan exercise and developed plans to address the identified gaps.

In the coming months, we plan to undertake a comprehensive data classification standards review, continue our work on developing a Cloud security standard, continue to implement critical security infrastructure into government's data centres, implement a government-wide proactive issues management process and continue our efforts to ensure compliance with relevant government standards and policies.

We appreciate the efforts of the Office of the Auditor General (OAG) of British Columbia in their assessment of government's computing general controls with the ultimate objective of reducing overall risk to government. The information provided by "The Status of Government's General Computing Controls: 2014" has provided valuable information regarding the maturity of the management of the controls and will assist in prioritizing improvements.

My office will continue to work with Ministry Chief Information Officers to improve management of controls to achieve their targeted maturity level. We look forward to future years' assessment by the Auditor General staff.

BACKGROUND

THE IMPORTANCE OF GENERAL COMPUTING CONTROLS

INFORMATION TECHNOLOGY (IT) is critical to government's day-to-day operations. From delivering services like healthcare and education, to processing billions of dollars in transactions, B.C.'s government IT systems handle substantial and sensitive information. This impacts the daily lives of everyone in our province.

More and more, government is relying on third parties to develop their IT systems and provide IT services. There are currently over 600 outsourced IT systems and services across government.

All these come with risks, such as:

- ◆ fraud: intentional access to systems and data for personal gain
- ◆ human errors: unintentional changes to systems and data
- ◆ down time: inability to resume critical services quickly after an unexpected disruption (power outages, disasters or malicious activities)

To reduce the impact of these risks, government needs strong controls.

General computing controls ensure that IT systems and services can help organizations fulfill their needs (the business objectives) through the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations.

They play an important role in detecting and preventing fraud and errors, protecting organizations' IT assets, and ensuring that critical business operations could continue. As such, 78% of the

recommendations in our IT audit reports over the last 10 years focused on improving general computing controls. See [Appendix B](#) for a summary of these 104 IT audit recommendations.

RESPONSIBILITY FOR GENERAL COMPUTING CONTROLS

The B.C. Office of the Government Chief Information Officer is mandated with governance authority for standards setting, oversight and approvals for the province's information and communications technology.

B.C. government organizations are responsible for following the spirit and intent of this policy in designing and implementing the general computing controls best suited for their IT environment – regardless of whether IT systems or services are in-house or outsourced.

B.C. government organizations include ministries, Crown corporations, universities, colleges, school districts, health authorities and other organizations controlled by, or accountable to, the provincial government. Collectively, they are called the *Government Reporting Entity* (GRE).

WHAT WE DID

2013

IN 2013, WE asked 138 organizations in the GRE to complete a self-assessment of their sophistication regarding use of general computing controls. We reported the results in terms of a maturity level that each B.C. government organization had attained.

The self-assessment was designed using the maturity model defined in the COBIT 4.1 framework (see Exhibit 1). The maturity model is a way to assess how well developed and capable the established IT controls are.

COBIT 4.1 is a globally accepted framework developed by the IT Governance Institute. The institute was formed by ISACA – an independent, non-profit, global association that engages in the development, adoption and use of globally accepted,

industry-leading knowledge and practices for information systems.

The self-assessment focused on *nine critical IT processes* defined in COBIT 4.1 as essential for maintaining:

- ♦ *confidentiality*: protecting the information they manage
- ♦ *integrity*: ensuring that transactions are processed correctly
- ♦ *availability*: ensuring critical government services are always up and running

Exhibit 1: 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 control framework for IT governance (www.isaca.org)

WHAT WE DID

See [Table 1](#) for the description of each of the nine areas.

In 2013, we received 100% of the organizations' self-assessments. We did not validate the results of their self-assessments, but we sent reports to the heads of each organization. The reports showed their results compared to similar organizations and provided recommendations on how they can achieve or improve their target maturity levels. We also sent a summary report to the B.C. Government Chief Information Officer.

In January 2014, we published a high-level report summarizing our findings and intent for future years as part of our [IT compendium report](#).

2014

In August 2014, we asked the same 137¹ organizations, plus nine Independent Offices of the Legislative Assembly and two new organizations (in total, 148 organizations), to complete the same self-assessment.

This year though, we selected 13 organizations and validated their self-assessments. This sample included a ministry, a health authority, two Crown corporations, three universities, two colleges and four school districts. The validation process included:

- ◆ reviewing the completed self-assessment form
- ◆ interviewing key IT personnel from each organization
- ◆ examining supporting evidence for the self-assessed levels

Again, we sent detailed reports to the heads of all 148 organizations, comparing their results to similar organizations, as well as their 2013 results. These reports provided recommendations on how they can achieve or improve on their target maturity levels. We also sent a summary report to the B.C. Government Chief Information Officer.

We conducted this project under sections 10 and 11 (8) (b) of the *Auditor General Act* from August 2014 to June 2015.

DETERMINING THE BENCHMARK

The COBIT 4.1 model states that maturity levels may be different for each organization, depending on the organizations' business objectives, complexity of their computing systems and IT environment, and the value of the information they manage. For example, a government organization that has the personal information of every person in British Columbia, or that provides critical services, should have higher maturity levels.

We believe that each organization should aim for at least *maturity level 3: Defined Process*, as their baseline. At this level, organizations have standardized and documented their procedures, mandated that they be followed, and trained staff accordingly.

¹ One of the 138 organizations in 2013 was dissolved in 2014.

WHAT WE OBSERVED

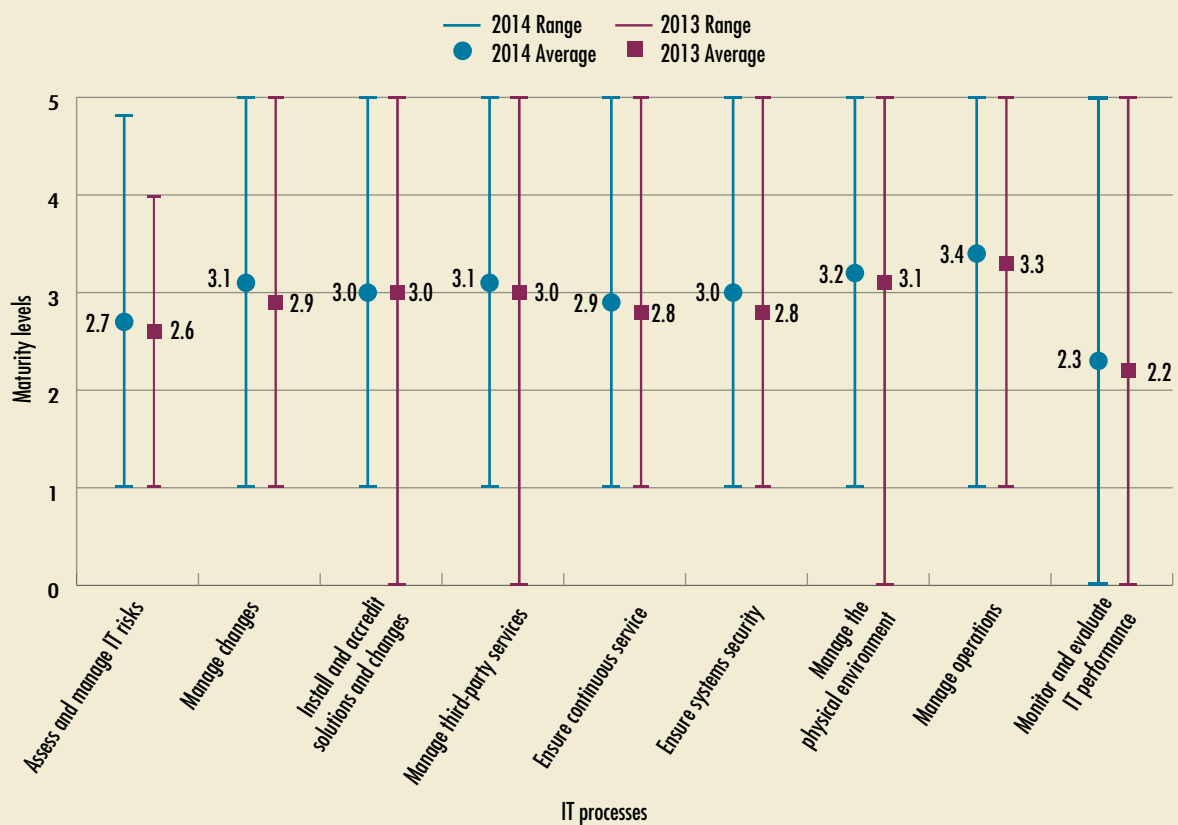
ORGANIZATIONS SELF-ASSESSED A HIGHER AVERAGE MATURITY LEVEL THAN 2013

Overall, the average self-assessed maturity level across all the organizations in the B.C. GRE and the nine IT processes was between 2.3 and 3.4. This is slightly higher than the 2013 results, which were between maturity levels 2.2 and 3.3 (See Exhibit 2).

Health authorities, ministries and Crown corporations had consistently higher average maturity levels than universities, colleges and school districts.

See [Appendix A](#) for maturity levels by the nine IT processes and type of organization.

Exhibit 2: Range and average self-assessed maturity level for each IT process



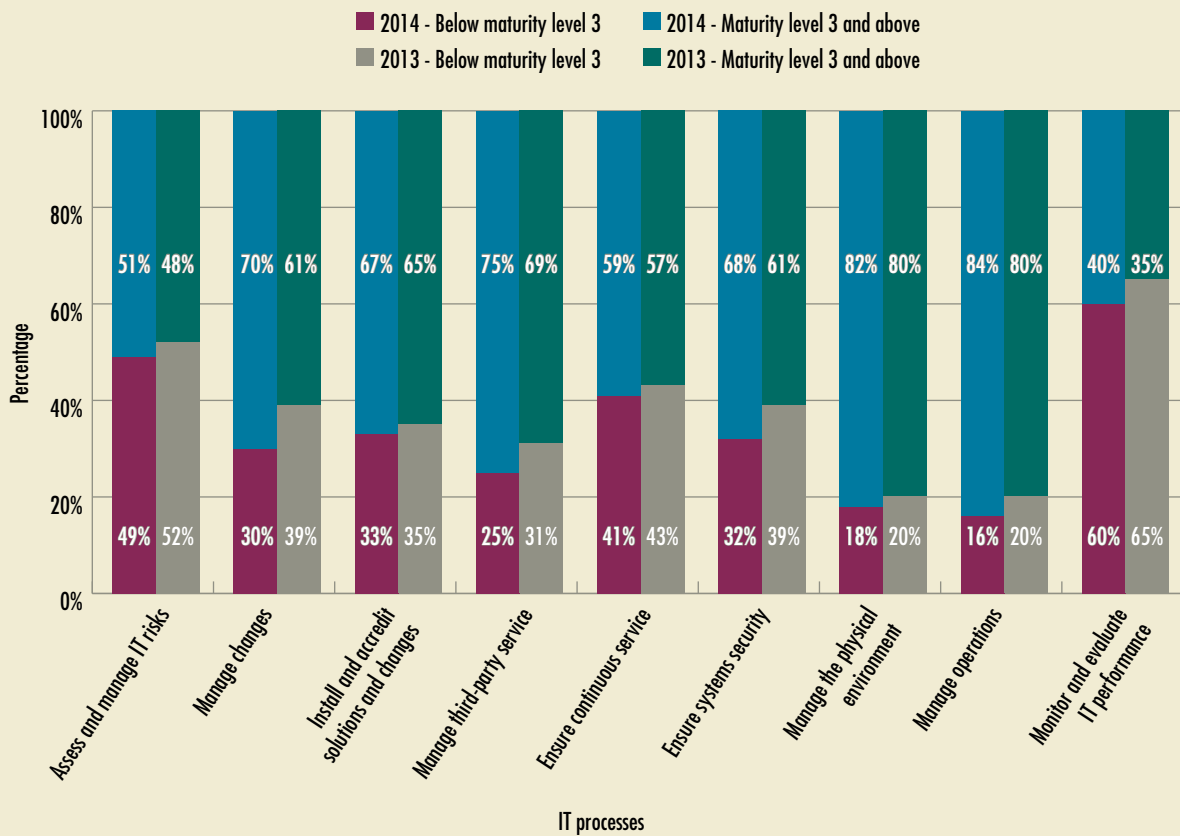
Source: Office of the Auditor General of British Columbia

WHAT WE OBSERVED

THE MAJORITY OF ORGANIZATIONS SELF-ASSESSED AT MATURITY LEVEL 3 AND ABOVE

Between 51% and 84% of the organizations self-assessed at maturity level 3 and above in eight of the nine IT processes (See Exhibit 3).

Exhibit 3: Percentage of organizations that self-assessed at maturity level 3 and above for each IT process



Source: Office of the Auditor General of British Columbia

WHAT WE OBSERVED

MOST ORGANIZATIONS LACKED SUFFICIENT EVIDENCE TO SUPPORT THEIR SELF-ASSESSED MATURITY LEVEL

In our validation, we found that nine of the 13 organizations (69%) did not have sufficient evidence to support their self-assessed maturity level, in one or as many as all nine IT processes.

For organizations that had insufficient evidence to support their self-assessments, we discussed our

findings with those organizations and adjusted their maturity levels accordingly.

Validation findings for the nine IT processes

The table below summarizes our validation results for each of the nine IT processes we looked at.

Table 1: Validation findings for each IT process

1. Assess and manage IT risks

All organizations should define a risk management framework for identifying, assessing and treating risks that affect key business areas. The framework helps gather information on IT operations risks so that senior management can make informed decisions about the risks they are willing to accept.

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Four organizations lacked sufficient evidence to support self-assessed maturity levels 3 and 4	<ul style="list-style-type: none">◆ Risk management processes and activities were:<ul style="list-style-type: none">◆ not formally documented◆ in the process of being documented◆ in the early stage of implementation◆ Risk management processes were not consistently applied to all activities in IT operations

WHAT WE OBSERVED

2. Manage changes

Organizations should manage changes to systems to prevent inaccurate data processing, disruption or delay of services, or cause loss of information. Prior to implementation, organizations should define policies, standards, procedures, and roles and responsibilities for monitoring, assessing and authorizing changes.

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Three organizations lacked sufficient evidence to support self-assessed maturity levels 3, 4 or 5	<ul style="list-style-type: none"> ◆ Change management processes were: <ul style="list-style-type: none"> ◆ not established ◆ not formally documented ◆ in the process of being developed ◆ in the early stage of implementation ◆ Lack of management's periodic monitoring of compliance with established policies, standards and procedures

3. Install and accredit solutions and changes

In conjunction with the policies and procedures for managing changes to systems, organizations need to have proper planning, testing and implementation of changes and carry out a post-implementation review. This will help ensure that systems are operational and are in-line with the agreed-upon expectations and outcomes.

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Four organizations lacked sufficient evidence to support self-assessed maturity levels 3 or 4	<ul style="list-style-type: none"> ◆ Procedures were: <ul style="list-style-type: none"> ◆ ad hoc ◆ informally documented ◆ still being developed

4. Manage third-party services

Organizations should ensure that third-party service providers are meeting business requirements. This is accomplished by clearly defining the roles, responsibilities and expectations of all parties, together with effective monitoring of compliance with service agreements. These processes help organizations mitigate the risk of third-party providers failing to perform in accordance with agreements.

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Two organizations lacked sufficient evidence to support self-assessed maturity levels of 3 or 4.5	<ul style="list-style-type: none"> ◆ Lack of formal documentation in selecting and managing third-party providers ◆ Did not follow its IT purchasing policy and the policy was out-dated

WHAT WE OBSERVED

5. Ensure continuous service

The provision of continuous, uninterrupted service requires defining roles and responsibilities for all involved parties; developing, maintaining and periodic testing of IT continuity plans; using off-site backup storage for systems and data; and, periodic IT continuity training. These processes help minimize the impact of a major IT service interruption on key business functions and processes.

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Four organizations lacked sufficient evidence to support self-assessed maturity levels of 3, 3.5 or 4	<ul style="list-style-type: none"> ◆ Roles and responsibilities were not defined ◆ Lack of training and monitoring for continuous service ◆ IT continuity plans were: <ul style="list-style-type: none"> ◆ non-existent ◆ in the process of being developed ◆ in existence, but neither updated nor regularly tested ◆ Backup facility was close to the main data centre and was exposed to the same physical risks (earthquake, storm, flood, fire, etc.)

6. Ensure systems security

To maintain the integrity of critical information and protect their IT assets, organizations should define a security management process which typically includes:

- ◆ establishing and maintaining IT security, policies, standards, procedures, plans, roles and responsibilities
- ◆ monitoring and testing security plans periodically to identify security weaknesses or incidents
- ◆ developing and carrying out corrective actions in order to minimize their business impact

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Five organizations lacked sufficient evidence to support self-assessed maturity levels of 3 to 4.5	<ul style="list-style-type: none"> ◆ IT security policies, procedures and plans were: <ul style="list-style-type: none"> ◆ not defined or formally documented ◆ in the process of being developed ◆ not current ◆ IT security procedures were not aligned with IT security policies ◆ Responsibility for systems security was neither clearly assigned nor independent from IT operations ◆ Security awareness and training was limited ◆ Risk and impact analysis, testing, monitoring and reporting on security were rarely carried out or was not aligned with business objectives

WHAT WE OBSERVED

7. Manage the physical environment

To protect computing facilities and staff from intentional or unintentional harm, organizations should:

- ◆ define the roles and responsibilities for managing the physical environment
- ◆ establish appropriate physical site requirements
- ◆ monitor environmental factors
- ◆ manage physical access

Number of organizations with insufficient evidence	Deficiencies in general computing controls
<p>Seven organizations lacked sufficient evidence to support self-assessed maturity levels between 2 and 5</p>	<ul style="list-style-type: none"> ◆ Lack of formal documentation of defined: <ul style="list-style-type: none"> ◆ roles and responsibilities ◆ environmental and physical security requirements ◆ Physical access to computing facilities was neither monitored nor reviewed ◆ Some organizations had not implemented preventive measures; where they had, the monitoring was weak ◆ Not all staff were trained in health, safety and emergency procedures

WHAT WE OBSERVED

8. Manage operations

To ensure complete and accurate processing of data and minimize delays in business operations, organizations need to have effective management of data processing procedures and diligent maintenance of computing hardware. This includes:

- ◆ defining roles and responsibilities for managing IT operations
- ◆ establishing operating policies and procedures for data processing
- ◆ protecting sensitive reports
- ◆ monitoring IT infrastructure performance
- ◆ ensuring preventive maintenance of computing hardware

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Five organizations lacked sufficient evidence to support self-assessed maturity levels of 3.75, 4 or 4.5	<ul style="list-style-type: none"> ◆ Lack of formal or up-to-date documentation of: <ul style="list-style-type: none"> ◆ IT standards and operating procedures ◆ clearly defined responsibilities ◆ Lack of: <ul style="list-style-type: none"> ◆ ongoing training ◆ monitoring against IT standards ◆ High degree of reliance on the knowledge of individuals managing IT operations ◆ Processes for monitoring the IT infrastructure were not sufficiently addressing the root causes of operational errors and failures

9. Monitor and evaluate IT performance

Monitoring is essential for effective management of IT performance, and ensures that things are done in line with the set directions and policies. This process includes defining and reporting on relevant performance indicators, and addressing deviations promptly.

Number of organizations with insufficient evidence	Deficiencies in general computing controls
Five organizations lacked sufficient evidence to support self-assessed maturity levels of 2 to 4	<ul style="list-style-type: none"> ◆ Organizations used ad hoc and informal approaches in monitoring and evaluating IT performance ◆ High degree of reliance on the knowledge of individuals monitoring activities ◆ Procedures and indicators for managing IT performance were still in development ◆ Where monitoring processes exist, the indicators were output-based, rather than outcome-based

Source: Office of the Auditor General of British Columbia

WHAT ORGANIZATIONS SHOULD DO

WE RECOMMEND THAT with regard to the general computing controls,* organizations in the B.C. Government Reporting Entity, periodically:

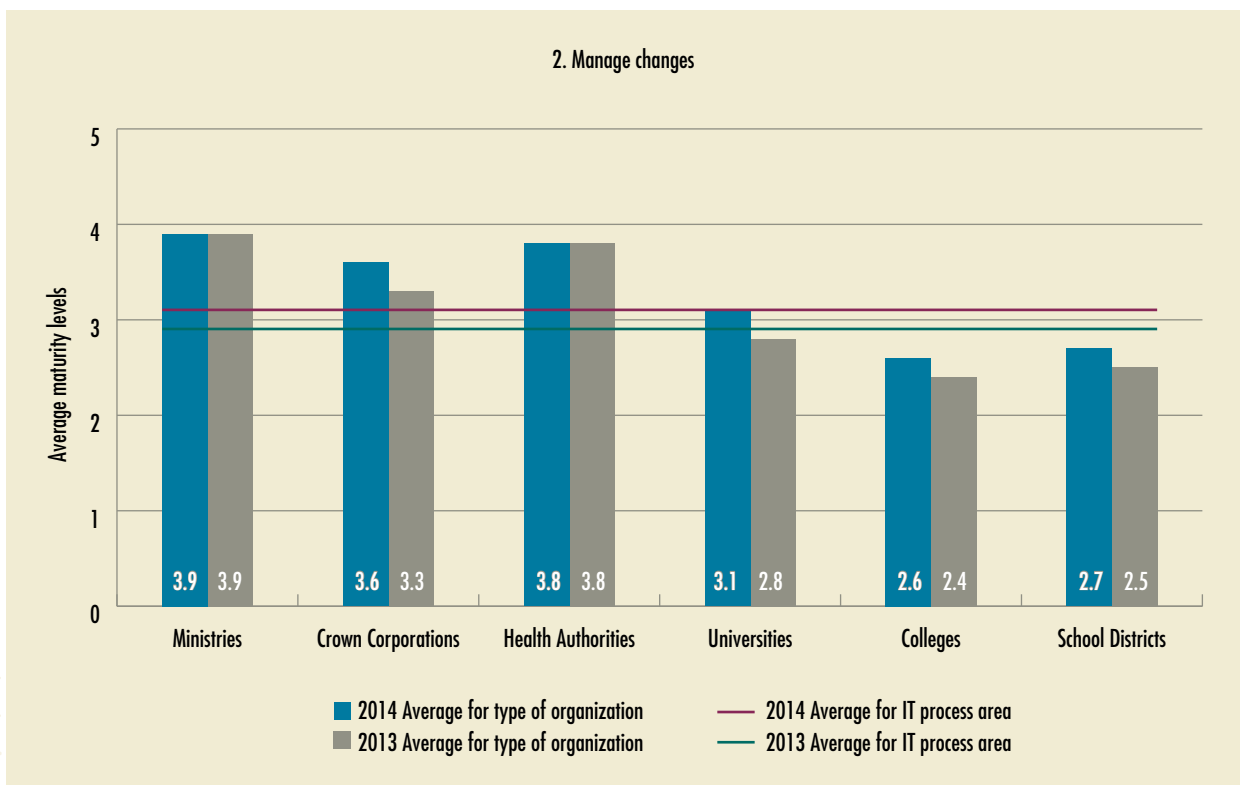
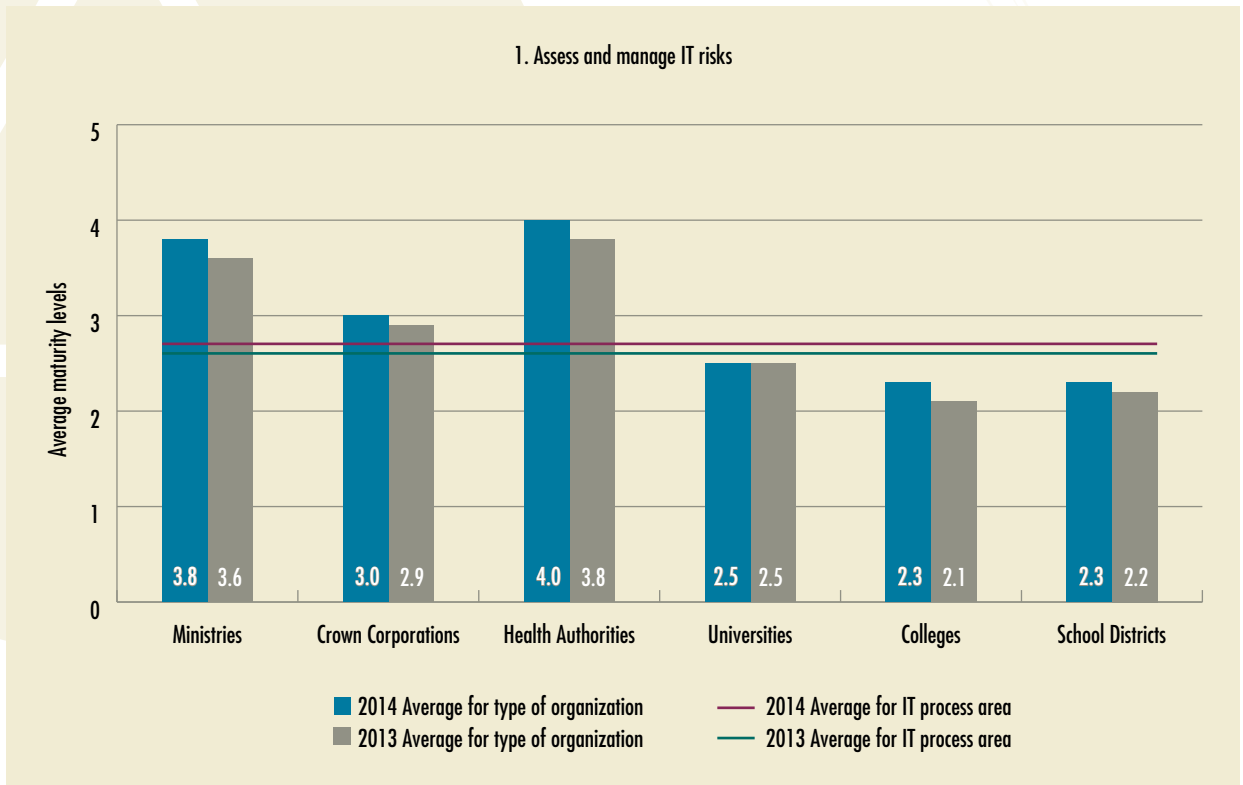
1. review their business and IT goals, and determine the target maturity level
2. analyze the controls necessary for meeting the target maturity level
3. determine what needs to be done to achieve the target maturity level
4. monitor the progress in achieving the target maturity level

*in accordance with the COBIT 4.1 maturity model

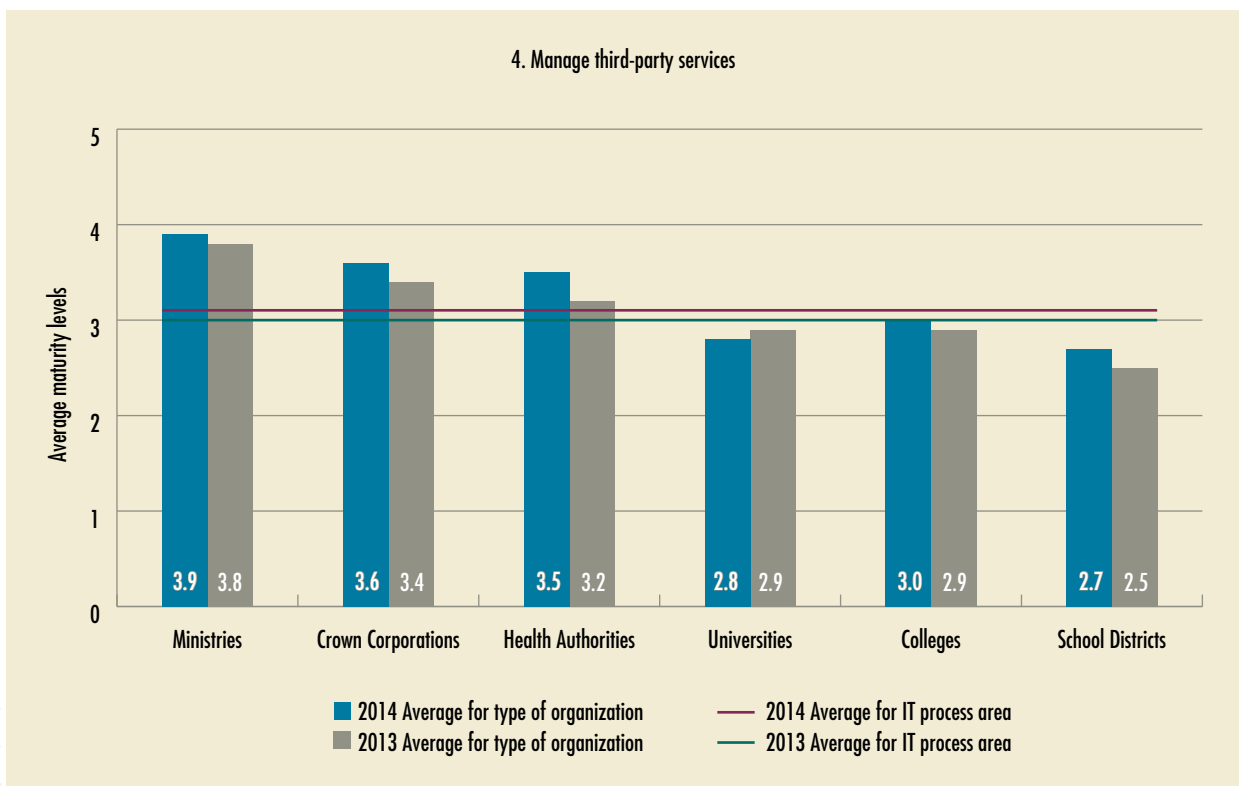
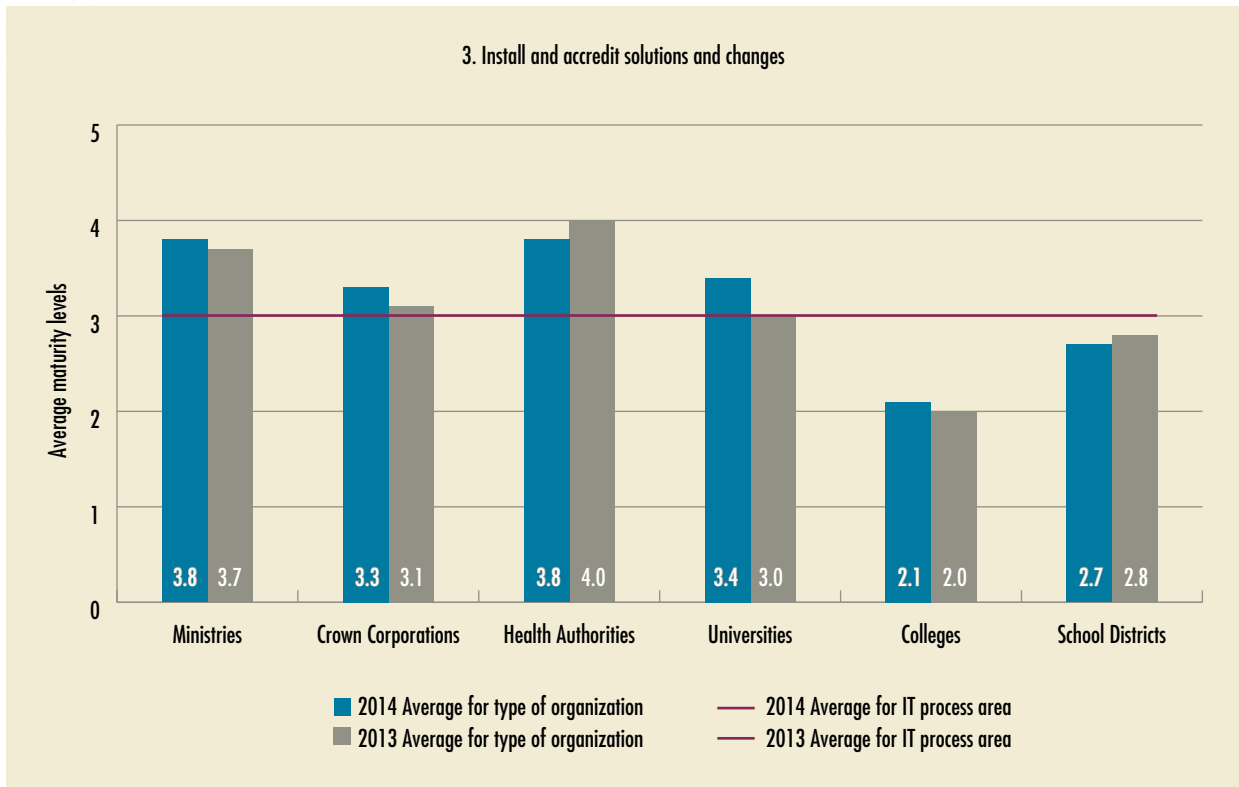
We also recommend that the B.C. Office of the Government Chief Information Officer continue to promote strong general computing controls and assist government organizations in achieving and improving their target maturity level.

APPENDIX A:

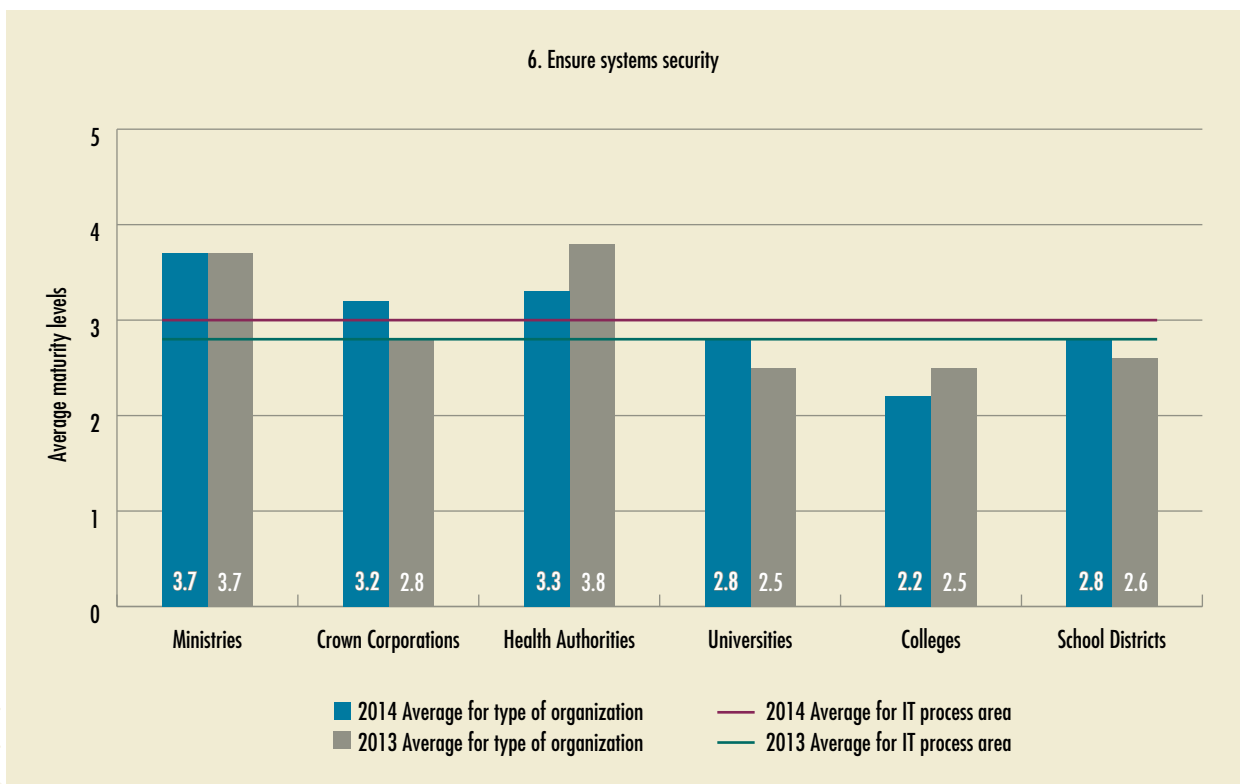
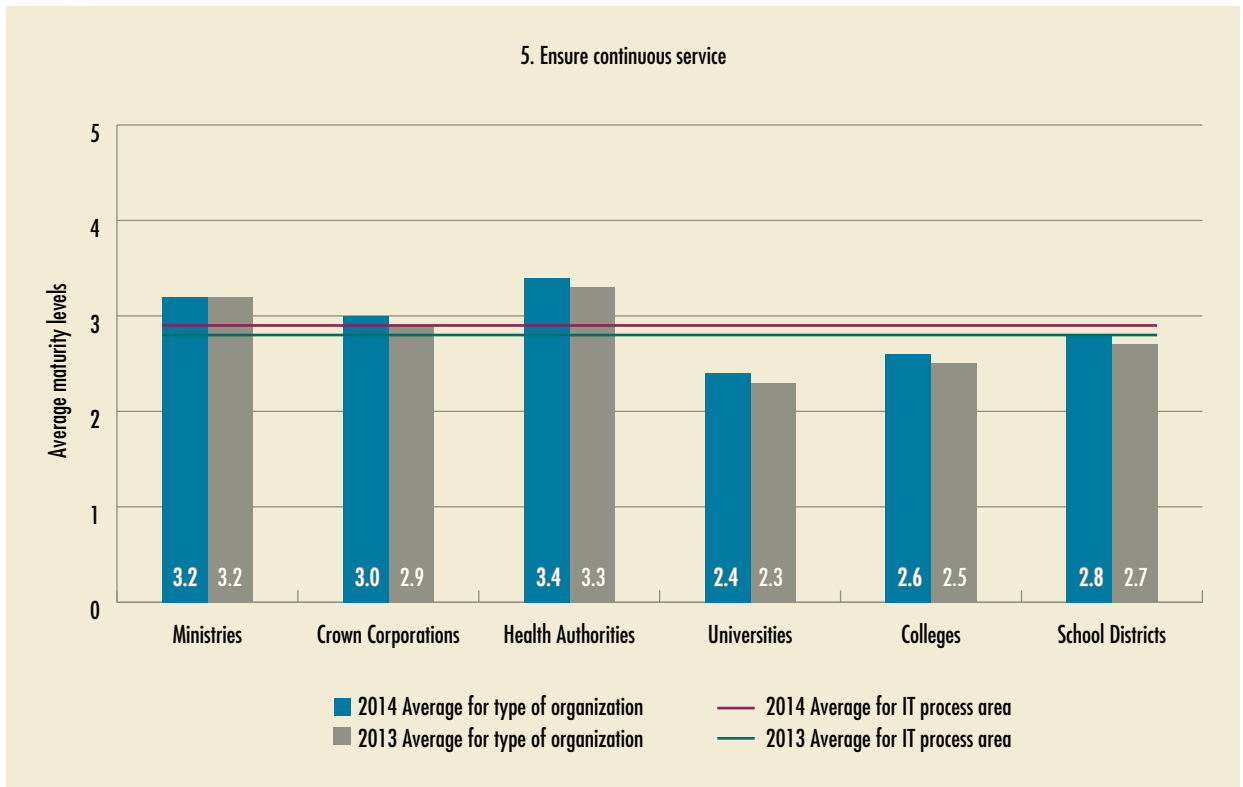
MATURITY LEVEL BY IT PROCESS AND TYPE OF ORGANIZATION



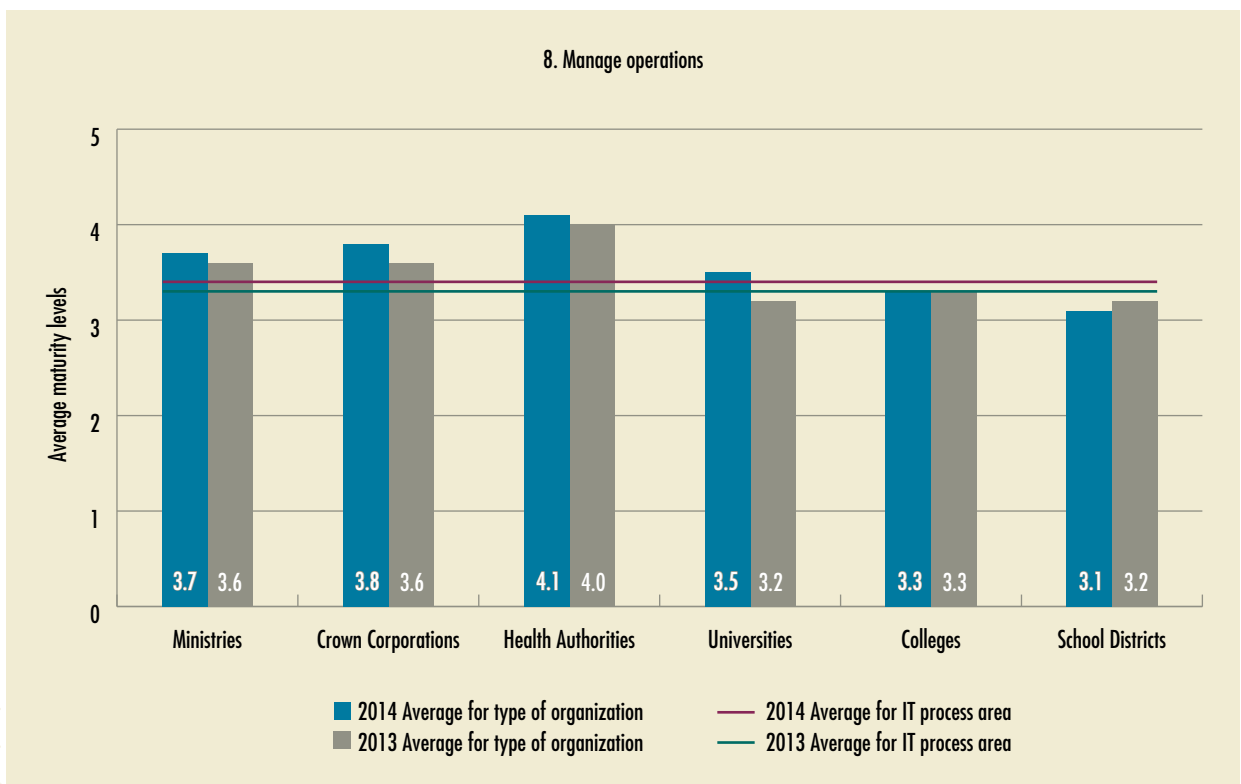
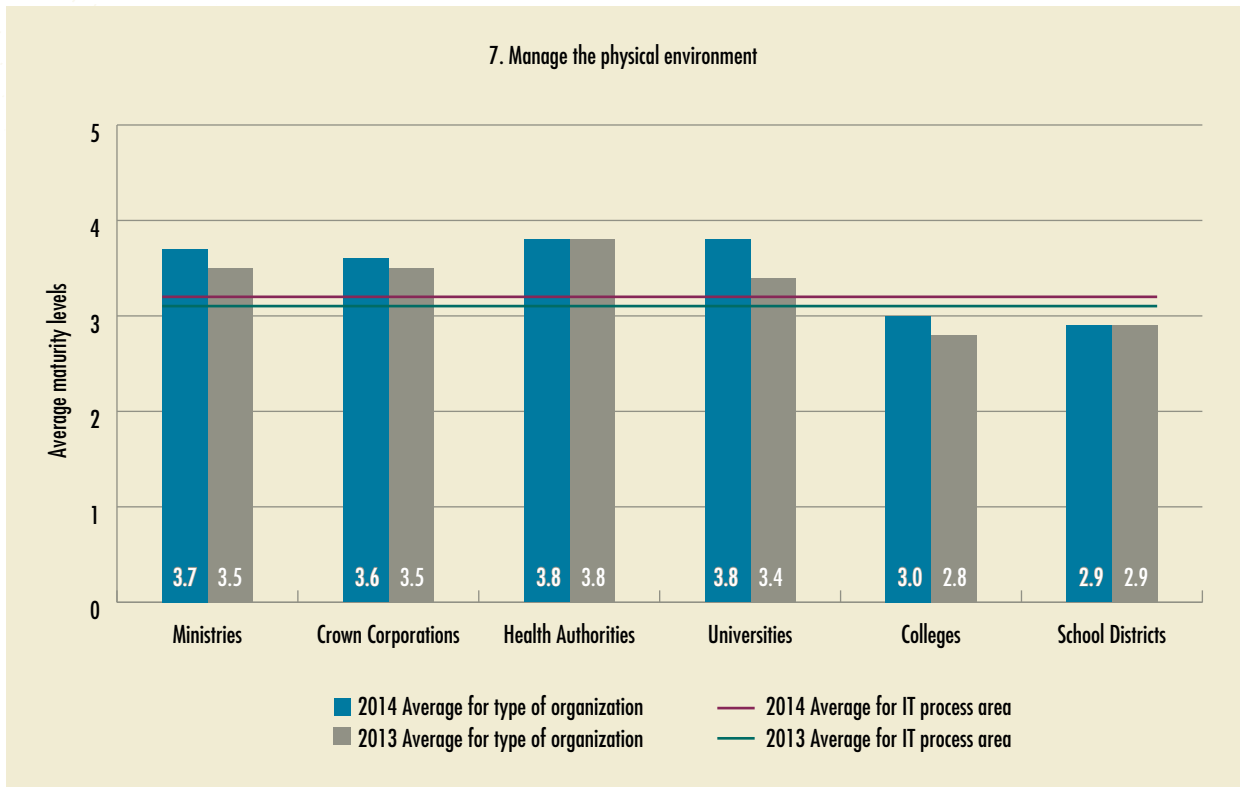
APPENDIX A: MATURITY LEVEL BY IT PROCESS AND TYPE OF ORGANIZATION



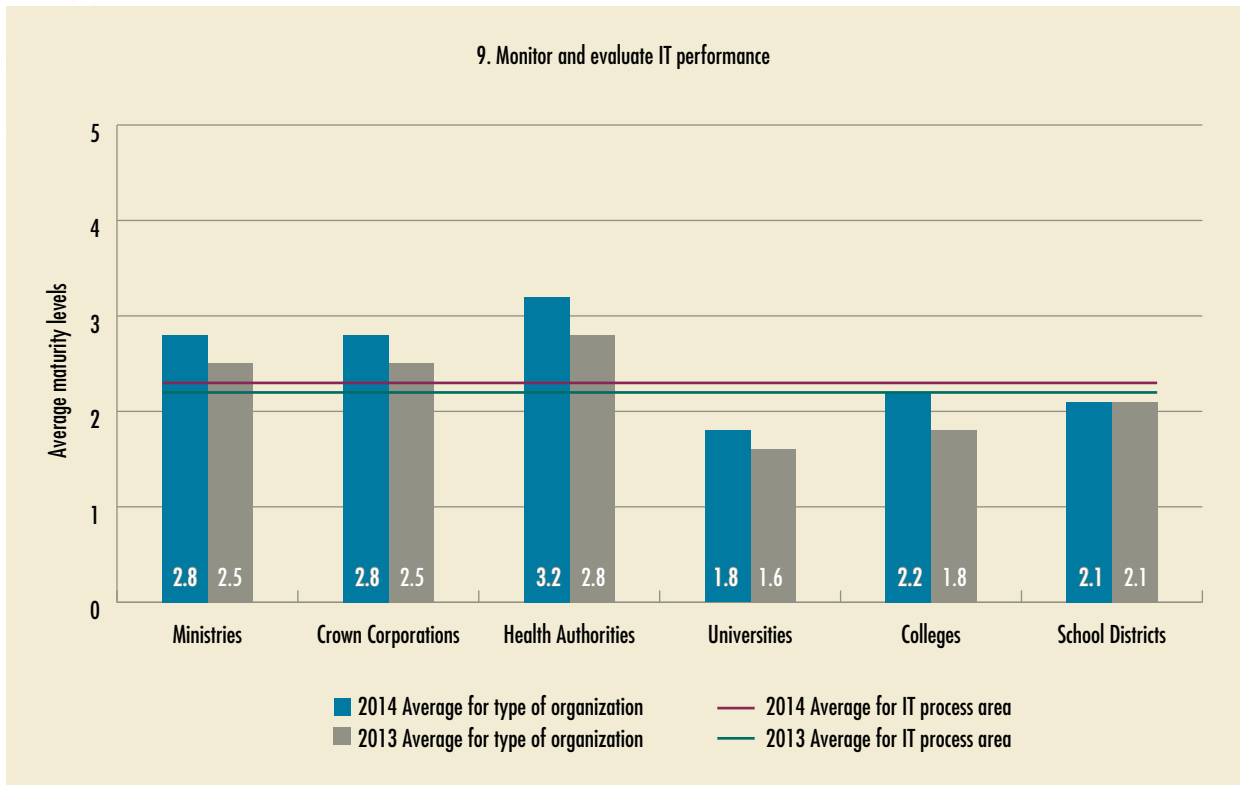
APPENDIX A: MATURITY LEVEL BY IT PROCESS AND TYPE OF ORGANIZATION



APPENDIX A: MATURITY LEVEL BY IT PROCESS AND TYPE OF ORGANIZATION



APPENDIX A: MATURITY LEVEL BY IT PROCESS AND TYPE OF ORGANIZATION



APPENDIX B:

SUMMARY OF IT AUDIT RECOMMENDATIONS OVER THE LAST 10 YEARS

IT audit report title	Total number of recommendations	Number of recommendations within the nine IT processes	Percentage of recommendations within the nine IT processes
Audit of the Government's Corporate Accounting System: Part 1	14	12	86%
Audit of the Government's Corporate Accounting System: Part 2	13	5	38%
Electronic Health Record Implementation in British Columbia	3	2	67%
Information Technology Compendium - Web Application Security Audit	4	4	100%
Integrated Case Management System	7	5	71%
IT Continuity Planning in Government	9	9	100%
Managing Access to the Corrections Case Management System	9	9	100%
Managing Government's Payment Processing	6	3	50%
Securing the Justin System: Access and Security Audit at The Ministry of Justice	5	5	100%
Summary Report: Results of Completed Projects - Info Security Management: An Audit on How Well Government is Identifying and Assessing its Risks	6	6	100%
Summary Report: Results of Completed Projects - Wireless Networking Security Phase 3	22	16	73%
The PARIS System for Community Care Services: Access and Security	10	9	90%
Wireless Networking Security in Government Phase 2	21	15	71%
Wireless Networking Security in Victoria Government Offices: Gaps in the Defensive Line	4	4	100%
Total	133	104	78%



OFFICE OF THE
Auditor General
of British Columbia

Location

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

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: www.bcauditor.com

This report and others are available at our website, which also contains further information about the Office.

Reproducing

Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our Office with authorship when any information, results or recommendations are used.



AUDIT TEAM

Cornell Dover
*Assistant Auditor General,
Corporate Services*

David Lau
Director, IT Audit

Joji Fortin
Manager, IT Audit

Joyce Mak
Senior Auditor, Financial Audit

Helen Li- Hennessey
Senior Auditor, Financial Audit

Nijjy Potikanon
Auditor, IT Audit

Wendy Lee
*Senior Audit Associate,
Financial Audit*

*Thank you to our staff members
not listed above for your work on
this project.*



OFFICE OF THE
Auditor General
of British Columbia