Public Safety Canada | Sécurité publique Canada

Public Safety Canada
Laser Audit of IT Asset Management

March 2018

Canada

PS4-236/2018E-PDF
978-0-660-25988-8

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

Information Technology (IT) plays a vital role within the Government of Canada by supporting efficient service delivery, enabling communication among departments, citizens, and other countries, encouraging openness and transparency, and increasing the accessibility of programs and services to Canadians.

The 2006 Treasury Board (TB) *Policy on Management of Materiel* stipulates that materiel assets are to be managed by departments in a sustainable and financially responsible manner that enables cost-effective and efficient delivery of government programs. Furthermore, the 2009 TB *Policy and Directive on the Management of IT* defines IT asset management as a set of effective and efficient practices that support strategic and cost-effective decision-making and contribute to departmental requirements for program delivery. IT assets are described as intangible (i.e. software licenses) and tangible (i.e. computers) items of value that have a life span beyond one year.

The Government of Canada 2016-20 IT Strategic Plan provides guidance on IT priority setting and decision-making for departments and agencies in the development of their individual plans. It emphasizes that sound practices should focus on a strengthened governance approach, the evolution of IT management practices, processes and tools, innovation and sustainability.

IT Asset Management at Public Safety

IT is a strategic asset and key enabler of Public Safety's (PS) program mandate and goals. In the department, IT services and operations are provided by the Chief Information Officer Directorate (CIOD). They are accountable for the stewardship of all IT resources and work in conjunction with Shared Services Canada (SSC).

PS 2016-17 IT asset inventory consisted of 1245 laptops, 186 tablets, 860 computers and 2248 monitors. In the 2016 IT Asset Management Strategy, an evergreen approach was proposed to provide a single laptop device to each employee. The approach plans to increase the number of laptops to 1,600 and decrease the number of computers to a minimum of 86 that are required to support high performance computing and special uses. According to its 2014-17 Departmental IT Plan, PS estimated $11,433,000 to IT, with $2,249,000 allocated to hardware assets.

Complimentary to TB policies and directives, the 2015 PS *IT Asset Management: Policy on Personal Computers Life-Cycle Management* requires an Information Technology Asset Management (ITAM) system, which records and tracks IT hardware and outlines the process of managing assets throughout their life-cycle.

Audit Objective and Scope

The objective of this audit was to provide reasonable assurance that IT asset management controls for laptops and tablets are in place and effective[1].

The scope focused on:

- The key controls in place for laptops and tablets to be tagged, recorded and tracked; and,
- The use of asset management information for decision-making.

The audit did not assess:

- Intangible assets (e.g. software);
- The inventory managed by Shared Services Canada, (e.g. blackberry devices); and,
- Computers, monitors, immovable IT assets (e.g. printers), and peripheral IT assets (e.g. keyboards, USB keys).

Summary of Findings

- The Department has a governance structure that includes the oversight of IT management. During the scope of the audit, key IT documents, such as the Departmental IT Plan and IT Asset Management Strategy were presented to the governance committees. However, the collection of performance data and reporting requirements are insufficient to support IT asset management and decision-making.

- PS has developed internal policies and procedures in support of IT asset management that align with the TB *Policy* and *Directive on Management of IT* as well as the *Policy on Management of Materiel*. Documented processes regarding the management of IT assets were available; however, these were deemed out-of-date by the Enablement Services Team (EST). The current practices and integrated controls are dependent on PS employees and their expertise. While an IT Asset Management (ITAM) system and key controls to manage laptops and tablets are in place, opportunities exist to improve their effectiveness and efficiency to ensure the integrity of the asset inventory.

Audit Opinion

Improvements to IT asset management processes and procedures are required[2] to ensure effective and efficient safeguarding of laptops and tablets. While the Departmental key controls for IT asset management are in place and comply with TB Policies and Directive, opportunities exist to strengthen controls to increase the integrity of the IT asset inventory, monitoring and reporting.

[1] Audit criteria can be found in Annex A.
[2] Audit opinion assessment scale can be found in Annex C.

Recommendation

The Assistant Deputy Minister, Corporate Management Branch, should review processes and procedures that align with TB related policies, which includes:

a) Identifying performance measures and reporting requirements to support IT asset management and decision-making; and,
b) Implementing effective and efficient IT asset management to ensure the consistency and accuracy of the IT asset inventory.

Management Response

The key actions to be taken by management to address the findings, recommendation and the associated timelines can be found in the 'Management Response and Action Plan' section of the report.

Audit Team Members

- Daniel Giroux, Chief Audit and Evaluation Executive
- Sonja Mitrovic, A/Director, Internal Audit and Evaluation Directorate
- David Uzan, Internal Audit Project Lead
- Cathy Kwan, Internal Auditor
- Alyssa Brown, Junior Auditor

Acknowledgements

Internal Audit would like to thank all those who provided advice and assistance during the audit.

1 INTRODUCTION

1.1 Background

Information Technology (IT) plays a vital role within the Government of Canada by supporting efficient service delivery, enabling communication among departments, citizens, and other countries, encouraging openness and transparency, and increasing the accessibility of programs and services to Canadians. Informed decisions surrounding IT asset investments, costs, and risks are essential to successful government plans and priorities.

The 2006 TB *Policy on Management of Materiel* stipulates that materiel assets are to be managed by departments in a sustainable and financially responsible manner that enables cost-effective and efficient delivery of government programs. To do so, a management information system is required to hold complete and accurate asset data that accounts for the full life-cycle of all assets and supports timely management decisions.

In addition, the 2009 TB *Policy and Directive on the Management of IT* defines IT asset management as a set of effective and efficient practices that support strategic and cost-effective decision-making and contribute to departmental requirements for program delivery. IT assets are described as intangible (i.e. software licenses) and tangible (i.e. computers) items of value that have a life span beyond one year.

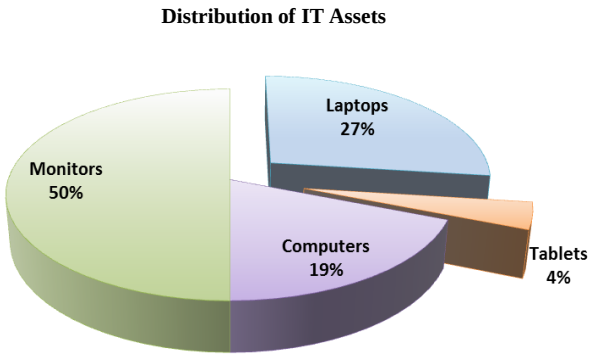
To outline key activities that ensure secure, reliable, responsive and innovative IT services, the Government of Canada published the 2016-20 IT Strategic Plan. It is intended to provide guidance on IT priority setting and decision-making for departments and agencies in the development of their individual plans. Specifically, it emphasizes that sound practices should focus on a strengthened governance approach, the evolution of IT management practices, processes and tools, innovation and sustainability.

IT Asset Management at Public Safety

IT is a strategic asset and key enabler of PS program mandate and goals. In the department, IT services and operations are provided by the Chief Information Officer Directorate (CIOD). They are accountable for the stewardship of all IT resources and work in conjunction with Shared Services Canada (SSC).

The EST in CIOD is responsible for IT service delivery by managing devices and assets, fulfilling move and repair requests, and coordinating with SSC to dispose assets.

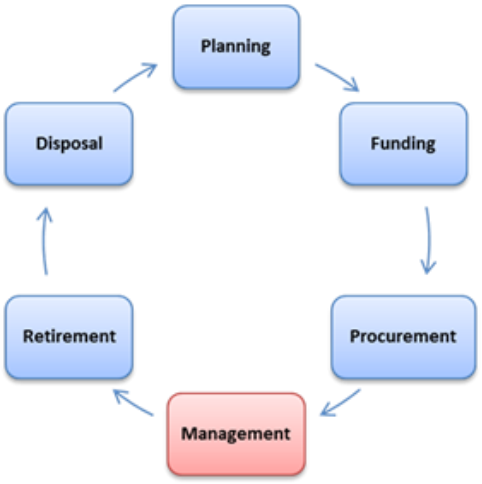
PS 2016-17 IT asset inventory consisted of 1245 laptops, 186 tablets, 860 computers and 2248 monitors.



As part of the 2016 IT Asset Management Strategy, an evergreen approach was proposed to provide a single laptop device to each employee. The approach plans to increase the number of laptops to 1,600 and lower the number of computers to a minimum of 86 that are required to support high performance computing and special uses. According to its 2014-17 Departmental IT Plan, PS estimated $11,433,000 to IT, with $2,249,000 allocated to hardware assets.

Complimentary to TB policies and directives, PS developed the *IT Asset Management: Policy on Personal Computers Life-Cycle Management* that emphasizes the importance of total cost consideration and outlines the process of managing assets throughout their life-cycle. This policy also states that assets are to be managed through the use of an Information Technology Asset Management (ITAM) system, which records and tracks IT hardware.

IT asset management is a set of practices that support strategic decision-making, and cost and risk minimization. To manage IT assets, a life-cycle containing six steps is to be followed.



1. Planning: Aligning IT needs to the identified operational requirements.

2. Funding: Identifying funds required to support departmental IT needs

3. Procurement: Selecting a cost-effective procurement method (i.e. savings through volume discounts) and purchasing assets.

4. Management: Tracking and monitoring IT assets.

5. Retirement: Identifying the outdated IT assets that cannot be redeployed.

6. Disposal: Removing and shredding the hard drives of retired assets before transferring them to Industry Canada for the Computers for Schools program.

1.2 Audit Objective

The objective of this audit was to provide reasonable assurance that IT asset management controls for laptops and tablets are in place and effective[3].

1.3 Audit Scope and Methodology

The scope included:

- The key controls in place for laptops and tablets to be tagged, recorded and tracked; and,
- The use of asset management information for decision-making.

The audit did not assess:

- Intangible assets, such as software;
- The inventory managed by Shared Services Canada, such as blackberry devices; and,

[3] Audit criteria can be found at Annex A.

- Computers, monitors, immovable IT assets (e.g. printers), and peripheral IT assets (e.g. keyboards, USB keys)

To complete the assessment, the following methods were used:

- Interviews with relevant stakeholders;
- Review of documentation produced between April 2016 to January 2018; and,
- Sample testing of key controls.

1.4 Audit Opinion

Improvements are required[4] to IT asset management processes and procedures to ensure effective and efficient safeguarding of laptops and tablets. While the Departmental key controls for IT asset management are in place and comply with TB Policies and Directive; opportunities exist to strengthen controls to increase the integrity of the IT asset inventory, monitoring and reporting.

1.5 Statement of Conformance and Assurance

Sufficient and appropriate audit procedures were conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined and within the scope described herein. The evidence was gathered in compliance with the TB *Policy* and *Directive on Internal Audit*. The audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program. The procedures used meet the professional standards of the Institute of Internal Auditors. The evidence gathered is sufficient to provide Senior Management with proof of the opinion derived from the internal audit.

2 FINDINGS, RECOMMENDATION AND MANAGEMENT RESPONSES

2.1 An IT governance structure is in place; however, performance data and reporting is insufficient to support IT asset management and decision-making.

Governance is the combination of processes and structures implemented by the Senior Management to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. The 2009 TB *Directive on Management of IT* requires the Chief Information Officer (CIO) to implement a departmental IT governance structure that:

- Supports effective IT decision making;
- Monitors and measures departmental IT management performance using both government-wide and departmental key performance indicators as appropriate; and,
- Advises the Deputy Minister, as well as the business owner and other stakeholders, of the effect of new or amended legislation and policies on departmental IT plans.

[4] Audit opinion assessment scale can be found in Annex B.

To manage its business lines, PS has implemented two governance committees: the Director General Management Committee (DGMC) and the Departmental Management Committee (DMC). According to its terms of reference, the DGMC is a governance body responsible for shaping the department's framework for decision-making and improving management excellence and best practices. This includes the responsibility for general IT management. During the scope of the audit (April 2016 to January 2018), DGMC met 33 times, seven of which included discussions regarding IT. Specifically, the committee records of decisions show that the Departmental IT Plan was presented twice; mobile device management, IT access controls, IT security working-group, and mobile device survey were each discussed once; and an IT asset management strategy was presented once in 2016-17.

The DMC, chaired by the DM and the Associate DM, is responsible for general financial and human resource (HR) management. Within the same timeframe, the DMC has met 38 times. Our review of the committee records of decisions found that six IT topics were tabled. These included presentations regarding: the Departmental IT Plan; the Dragon network; tablet and cellphone costing; IT asset management pressures and ever-greening needs; Management Accountability Framework (MAF) results; Government of Canada Electronic Document and Records Management System (GCDocs) migration; the Canadian Top Secret Network (CTSN); and, cellphone migration. While DGMC and DMC members affirmed their commitment to the one device per employee objective set by IT and recognized the need to establish an annual funding model to support effective long-term planning for IT assets, they did not make a final decision regarding the IT asset budget or next steps. Although the PS governance structure is defined, the interviewees indicated that the performance and reporting requirements related to IT management are unclear.

The TB *Directive on Management of IT* also requires the CIO to develop a departmental IT plan that covers the strategic, tactical and operational aspects of the management of IT. The Plan addresses governance, IT business, performance measures and risk management. It reflects departmental priorities and outlines planned investments, including any acquired services, for the upcoming five-year period in the following areas:

- New IT projects, systems, services or large enhancements to existing projects, systems and services;
- Planned maintenance of enhancements to existing IT systems or services; and,
- IT operations.

To keep up with the pace of technological changes, the departmental CIO is required to annually review and update the departmental IT plan. In addition to the Policy and Directive, TB has also shared a guide to support departments in the development of their departmental IT plan. While the Directive outlines the required five-year plan, the guidance recommends a three-year IT plan.

During the document review, the audit team assessed the 2014-17 and the 2017-20 Departmental IT Plans that comply with the guide's recommended length. The Plans contain departmental priorities, IM/IT priorities and risks, and planned projects with associated costs. The audit team found that both plans listed a priority that required PS to work with SSC to make use of consolidated data centres for new initiatives and plan for the consolidation of existing IT assets. In

addition, the 2017-20 Departmental IT Plan lists the life-cycle management of IT assets (IT ever-greening) activity as the 8th out of 14 priorities within this planning cycle.

While the two PS IT Plans include the majority of the required elements, the plans do not clearly outline the IT Governance in place and nor do they provide a progress update against previous commitments.

Further to the *Policy on Management of IT*, the 2006 *Policy on Management of Materiel* requires that a materiel management information system is in place which enables the collection and generation of complete and accurate data on materiel asset holdings, incorporates a risk-based stocktaking schedule, and supports timely, informed materiel management decisions. Through document review, the audit team found that service standards were established for new user requests and office moves.

Interviewees indicated that technological capability exists to collect performance data and asset information, such as diagnostics to attain records of user log-ins to confirm asset activity and primary users. Nevertheless, with only one FTE formally assigned to the asset management function, monitoring and collection of performance data is conducted on ad-hoc basis. Currently, the Management Accountability Framework Assessment is the main driver for IT reporting. The 2017-18 assessment included 34 questions that focused on practices and mechanisms in place for recordkeeping, open data, Departmental IT Plan, IT expenditures and HR capacity, sustainability of mission critical applications, inventory of all supported applications and their life-cycle, service-level-agreements and workplace technology device related incidents tracking and response.

In December 2016, a multi-year ever-greening approach was presented at the DMC as part of the IT Asset Management Strategy. The analysis conducted for the development of the ever-greening approach considered IT asset stock and the average acquisition costs. While reliant on SSC for the purchase of new laptops, PS has opted to select the most convenient choice to ensure efficiency and cost savings.

Although PS has an established governance structure for IT management and complies with TB policy instruments, the audit found that the performance data and reporting is insufficient to support IT asset management and decision-making.

2.2 The key controls to manage laptops and tablets are in place; however, there are opportunities to improve their effectiveness and efficiency.

According to the 2009 TB *Policy on Management of IT*, the Departmental CIO is responsible to develop and maintain efficient and effective departmental IT management practices and processes, with priority placed on IT asset management, IT service catalogue and IT service costing and pricing. As previously mentioned, the 2006 *Policy on Management of Materiel* requires that a materiel management information system is in place that enables the collection and generation of complete and accurate data on materiel asset holdings (capital assets, inventories, and materiel in use), incorporates a risk-based stocktaking schedule, and supports timely, informed materiel management decisions.

In addition to the TB policies and directives, PS has also implemented the *IT Asset Management: Policy on Personal Computers Life-Cycle Management* in 2015 and the *PS Workplace Technology Devices Asset Management Life-Cycle* in 2016. These internal documents define and describe the process of managing assets throughout their life-cycle while emphasizing the importance of total cost consideration. The internal policy also requires the use of the Information Technology Asset Management (ITAM) system to record and track IT assets.

The EST within the CIOD provided the audit team with PS IT asset management workflows for the deployment, receipt and management of assets. However, during the walkthrough, the audit team was informed that all the workflows are out-of-date and need to be revised. According to the asset inventory contained in ITAM, the department manages a number of tablets such as iPads, Playbooks and SurfacePro. Although, we were informed that tablets are being phased out due to their expired warranty, we were not provided any policy, procedure or process in place for management of current or future tablets.

The processes and procedures are clear to the EST; however, the effectiveness of IT asset management controls is dependent on the current employees and their expertise. In addition to the lack of documented and up-to-date processes and procedures, there is no formal training offered for new employees. Interviewees indicated that new hires and students are trained on the job.

Currently there is one full time equivalent (FTE) who is supported by students and is responsible to collect, tag, record and track the PS IT asset inventory. The EST practices timely management of IT assets by assigning assets, such as laptop and tablets, to a specific office number before new employees begin work. Since employee information is not available in ITAM until their official start date and IT account is set up, employee names are assigned to assets at a later time.

While IT asset management is centralized within PS national headquarters, in Ottawa, an employee within CIOD is required to visit the regional offices to update the IT asset inventory in ITAM each year. To minimize the risk of loss of IT assets, the *PS Workplace Technology Devices Asset Management Life-Cycle* procedure requires that an annual confirmation of IT asset holdings is conducted. According to the interviewees, a physical inventory was completed in 2015-16 and one was being conducted during the course of the audit. The physical inventory requires a visit to all PS offices to locate the IT asset, scan and confirm the asset tag, and update the information contained in the inventory.

The information contained in ITAM includes asset tag number, model, serial number, type, life-cycle status, location and the name of the employee it is assigned to. To differentiate various PS office locations, the EST developed naming conventions for each building. The evidence showed a lack of integrity of IT asset inventory due to missing and inconsistent information. Specifically, the audit team found an inconsistent application of location naming conventions and that several employee names associated to the listed assets were missing.

The integrity of the IT asset inventory was assessed through a sample of 188 laptops and 32 tablets located in Ottawa. The sample included assets located on the five office floors that were not yet updated through the program's physical inventory, which was being performed during the conduct of the audit.

The audit team performed two tests:

1. **ITAM Information to Assets**: Selection of 94 laptops and 32 tablets from ITAM and compared to the assets in the identified offices; and,
2. **Assets to ITAM Information**: Selection of 94 laptops found in offices were identified and compared with the information in ITAM.

The tests looked into verifying the accuracy of ITAM information, specifically:

- asset tag number;
- location;
- asset model;
- serial number; and,
- assigned employee name.

Three laptops and three tablets sampled from ITAM were identified as located in SIGNIT (Signals Intelligence) Secure Areas (SSA). These areas do not permit any wireless devices. During the office walkthroughs, the audit team did not find any laptops or tablets within the SSAs.

Laptops:

The audit team assessed 171 out of the 188 sampled laptops. Due to limitations such as empty offices, telework arrangements, and employee extended leave, the audit team was unable to fully complete the assessment of the remaining 17 laptops. For those assessed, the results demonstrated that across all PS buildings in Ottawa, the main inconsistencies found in the asset inventory were the location of assets (64 out of 171 laptops) and the assigned employee name (44 out of 171 laptops).

Tablets:

While the audit team sampled 32 tablets, the full testing was performed on 25. For 7 out of the sampled 32 tablets, the audit team could not complete the assigned testing due to empty offices and employee extended leave. The results of the assessed tablets demonstrated that the information contained in the inventory was inaccurate, with incorrect location being the most prevalent representing 23 out of 25 tablets. Furthermore, 23 out of 25 tablets were found to have asset tags that did not match the inventory.

Storage:

The IT assets can be stored in various locations within the department. To test the accuracy of the stored inventory, the audit assessed a sample of 16 laptops that were located in the basement storage room. The results showed that the asset tag, model and serial number information contained in ITAM were accurate. However, 6 out of 16 laptops inventory locations were incorrect.

Throughout the testing procedures, the audit team observed that within ITAM, there is an inconsistent use of naming conventions. Specifically, to trace an asset, further queries in ITAM are required to determine its exact location. While a materiel management system is in place to enable

the collection of data on materiel asset holdings, improvements are required to ensure its integrity through timely updates.

Recommendation:

The Assistant Deputy Minister, Corporate Management Branch, should review processes and procedures that align with TB related policies, which include:

a) Identifying performance measures and reporting requirements to support IT asset management and decision-making; and,
b) Implementing effective and efficient IT asset management to ensure the consistency and accuracy of the IT asset inventory.

2.3 Overall Conclusion

PS has a defined governance structure and internal policies and practices that comply with the TB *Policy on Management of IT* and *Policy on Management of Materiel*. However, improvements are required to ensure effectiveness and efficiency of IT asset management controls and processes, and address weaknesses in monitoring, and gathering of performance information for decision-making.

2.4 Management Response and Action Plan

Recommendation	Actions Planned	Target Completion Date
The Assistant Deputy Minister, Corporate Management Branch, should review processes and procedures that align with TB related policies; which includes:		
a) Identifying performance measures and reporting requirements to support IT asset management and decision-making; and	1) Identify and confirm performance measures with executive management.	June 30, 2018
	2) Quarterly reports on performance measures and status to executive management.	September 30, 2018
b) Implementing effective and efficient IT asset management to ensure the consistency and accuracy of the IT asset inventory.	1) Complete physical inventory and IT Asset Management system (ITAM) reconciliation to ensure that the current physical and virtual inventories coincide.	September 30, 2018
	2) Develop a continuous monitoring approach that reflects adequate sampling of IT assets.	September 30, 2018
	3) Review internal processes and procedures in line with TB-related policies.	June 30, 2018
	4) Produce communications tools to ensure staff follow asset management processes.	September 30, 2018

ANNEX A: AUDIT CRITERIA

The following are the audit criteria used to assess the effectiveness of IT asset management controls for laptops and tablets that are in place.

Audit Criteria		
Criterion 1:	An appropriate governance structure is in place for IT asset management and is operating efficiently and effectively.	• PS has an established governance structure that includes responsibilities over general IT management. • The governance committees have approved terms of reference and documented records of decisions that include discussion related to IT asset management, such as IT asset management pressures and ever-greening needs. • The Departmental IT Plan and the MAF results report were the only regular reports provided to the committees.
Criterion 2:	PS IT Asset Management internal policies, practices, and processes comply with relevant TB policies and standards.	• PS policies, practices, and processes generally complied with relevant TB policies. However, improvements can be made regarding reporting and performance measurement. • Internal processes, practices, and procedures were not up-to-date and communicated with employees to ensure consistency.

Criterion 3:	PS processes and controls to manage IT assets are appropriately designed and operating efficiently and effectively.	• While the sampled assets were tagged and tracked, the IT asset inventory was not complete and accurate.
		• The tests included verification of five information fields (location, asset tag, asset model, serial number and assigned employee name)
		  ○ The main inaccuracies were found in location (64 out 171 laptops) and assigned employee name (44 out of 171 laptops).
		  ○ The main inaccuracies for tablets were location (23 out of 25 tablets) and asset tag (23 out of 25).

Criterion 4:	Performance information for IT asset management is appropriately collected, tracked, and used to inform decision-making.	• Other than the physical inventory that was conducted during the audit, there was no evidence to support on-going monitoring of IT asset management. • Beyond the information found in the MAF results report, performance information was not tracked to inform decision-making. • While the EST is able to collect information to inform decision-making, interviews demonstrated that reporting is completed on an ad-hoc basis.

ANNEX B: INTERNAL AUDIT AND EVALUATION DIRECTORATE OPINION SCALE

The following is the Internal Audit and Evaluation Directorate audit opinion scale by which the significance of the audit collective findings and conclusions are assessed.

Audit Opinion Ranking	Definition
Well Controlled	• Well managed, no material weaknesses noted; and • Effective
Minor Improvement	• Well managed, but minor improvements are needed; and • Effective
Improvements Required	Improvements are required (at least one of the following two criteria are met): • Control weaknesses, but exposure is limited because likelihood of the risk occurring is not high; • Control weaknesses, but exposure is limited because impact of the risk is not high;
Significant Improvements Required	Significant improvements are required (at least one of the following two criteria are met): • Financial adjustments material to line item or area or to the department; • Control deficiencies represent serious exposure; • Major deficiencies in overall control structure;