OFFICE OF THE AUDITOR GENERAL OF CANADA

PERFORMANCE AUDIT PRACTICE GUIDE

AUDITING INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY

GUIDANCE FOR PRACTITIONERS

MAY 2014

TABLE OF CONTENTS

INTRODUCTION

This Practice Guide is one of a series of guides that provide auditors with guidance on how to examine various systems and practices during a performance audit. This guide helps define the expected knowledge about an entity’s information management and information technology systems needed to conduct OAG performance audits.

What Information Management and Information Technology (IM/IT) Is

Information management (IM) is a critical element of an entity’s business activities. It plays a central role in adequately safeguarding sensitive information, and in ensuring that information that is important to fulfilling the entity’s mandate and meeting its operational objectives is readily available. That information is typically managed through an information technology (IT) function that directs and supports effective and efficient information management, from planning and systems development to disposal or long-term preservation. The IT function ensures the confidentiality, integrity, and availability of information that is essential to government decision making and service delivery. Effective recordkeeping practices enable departments to create, acquire, capture, manage, and protect the integrity of information resources of business value in the delivery of Government of Canada programs and services.

Federal government departments and agencies use IT such as the Internet, computers, cell phones, and mobile devices every day to improve productivity, communicate and collaborate, and enhance service delivery to Canadians. In any entity, whether Crown corporation or department, the bulk of the information that is used to steer the entity is stored, generated, or managed on an IM system. IM and IT work together to gather, store, and manage the information that entities need to operate and to make business decisions.

Why Auditing IM/IT Is Important

In most cases, IM/IT systems are integral to the management of the entity, which needs good quality information to support business decisions. Delivering stakeholder value requires good governance and management of information and technology assets. Entity boards, executives, and management need to embrace IM/IT like any other significant part of the business.

Treasury Board policy requires entities to effectively manage their information, and auditing standards require performance audit teams to have a knowledge of relevant information technology. The audit team that identifies and audits an entity’s various frameworks, systems, and practices related to managing this information will add value by focusing on results rather than just the policies and processes.

In order to conduct a comprehensive and meaningful performance audit, auditors must understand the critical IM and IT risks related to the entity-specific, sectoral, and government-wide audits being conducted. Auditors should integrate related audit questions and work into the audit scope’s lines of enquiry.

How Auditing IM/IT Supports Other OAG Audit Work

OAG audits often rely heavily on entity systems and data to sample and select items for audit examination. By incorporating IM/IT examination into performance audits, OAG auditors will gain a level of comfort that entity systems and data can be relied upon for their audit work.

OBJECTIVES OF THIS GUIDE

This Practice Guide provides guidance to auditors to

- effectively integrate IM/IT into entity-specific, sectoral, and government-wide performance audit lines of enquiry; and
- find out what IM/IT knowledge they need to effectively identify potential IM and IT issues when planning the audit, preparing and updating strategic audit plans, and preparing chapter proposals.

The Guide's objectives are to

- provide an enhanced performance audit methodology that focuses on IM/IT service delivery;
- assist auditors in understanding and identifying significant IM/IT audit scoping opportunities early in or prior to the planning phase, based on the entity's corporate risk profile, integrated business plans, departmental performance reports, reports on plans and priorities, and other related documents; and
- identify where the support of the OAG Service Delivery and Information Technology Team's specialized knowledge may be required.

KNOWLEDGE OF IM/IT

IM/IT Knowledge Requirements

The Office, through its Performance Audit Manual (section 3061), follows the Chartered Professional Accountants of Canada (CPA Canada) Handbook—Assurance which relate to performance audits. These standards require auditors to have technical knowledge and expertise, including knowledge of relevant information technology.[1] In addition, the auditor should take into account the Policy on Information Management that requires entities to manage information effectively by doing the following:

1. Provide convenient access to relevant, reliable, comprehensive, and timely information for government programs and services.
2. Support the outcomes of programs and services, as well as operational needs and accountabilities.
3. Include adequate governance structures, mechanisms, and resources.

[1] CPA Canada Handbook—Assurance:

- Canadian Standards on Quality Control—CSQC 1, paragraph A31; and
- Other Canadian Standards—section 5030, paragraph 24

The Importance of Understanding IM/IT for Performance Audits

Our Office primarily conducts performance audits on the topics selected for programs and sectors as stated in the strategic audit plan (SAP). The SAP identifies the upcoming audit topics that are considered to be the highest risk.

A key component of understanding the audit topic is knowledge of business where the audit principal responsible for an entity acquires, maintains, shares, and documents up-to-date knowledge of that entity, including the risks the entity faces. This includes the key IT systems that generate information required for effective decision making by the entity's senior management.

IM/IT costs are often significant and need to be effectively managed by the entity. Failure to do so could lead to higher inherent risks (such as added complexity and overall higher costs).

The Importance of Data Integrity to Sound Information Management

Another key component to understanding information management is data integrity. Data integrity generally refers to the accuracy, validity, and completeness of data with respect to its intended purpose. For the entity, if data lacks integrity, it reduces the quality of recordkeeping, reporting, and business decisions regarding entity operations. For the auditor, the level of data integrity affects the degree to which data and information can be relied upon to plan and perform the audit, report findings, and make recommendations. Data integrity is a key component in the determination of the data's value and usefulness.

Data Integrity Standards

There are several sources of data integrity standards.

The CPA Canada Handbook—Assurance, for example, requires practitioners to consider the following to determine whether data is reliable when designing substantive analytical procedures[2]

- the source of the information available (e.g., independent sources);
- the comparability of the information with similar industries;
- the nature and relevance of the information available (e.g., whether budgets have been established as results to be expected rather than as goals to be achieved); and
- controls over the preparation of the information that are designed to ensure its completeness, accuracy, and validity.

Treasury Board's Policy Framework for Information and Technology states that entities should ensure the confidentiality, integrity, and availability of information that is essential to government decision making and the delivery of services.

[2] CPA Canada Handbook—Assurance: Canadian Auditing Standards—section 520, paragraph A12

Assessing Data Integrity

This Practice Guide does not explore in detail the many attributes of data integrity (such as validity, verifiability, neutrality, and completeness). However, audit teams should assess at the planning phase the data integrity of the performance audit information that they wish to base their findings and conclusions on. When assessing data integrity, you can examine data sources such as data files (for example, property and equipment inventory); financial transactions; Internet-based data; summarized report data; data extracts from databases or software; and program performance reports.

The following factors may support a conclusion that there is a high level of data integrity:

- The system or process was designed by people with a good understanding of data integrity.
- Data integrity is very important to users of reports.
- The information is required to report to high-level external parties.
- There is evidence that the entity would change processes or procedures if problems had been identified.
- The entity sampled data using sound principles.
- There has been a consistently good approach to data management over recent years.
- Data comes from an established vendor product (e.g., PeopleSoft) and a standard report capability within the product.
- Entity personnel are knowledgeable about and experienced with the need for data integrity and its importance in critical decision making.
- There is evidence of adequate data integrity assurance procedures and controls.
- The data and report are subject to review and approval and decision makers raise questions related to data integrity assurance.
- There are signed statements attesting to data integrity with documented challenges to data integrity originating either internally or externally.

PLANNING THE AUDIT

IM/IT Aspects of the Audit Topic to Identify

When planning a performance audit of a program or sector, audit teams should identify any IM/IT aspects that could form a line of enquiry. In the past, IM/IT performance audit lines of enquiry tended to be stand-alone and did not complement the program or sector’s overall lines of enquiry. This suggested that the program operations and IM/IT components were separate in nature and should be separately audited. With IM/IT now prevalent throughout all operations, and with information as a key resource for performance audits, auditors should look for IM/IT aspects in every audit.

When our Office conducts performance audits, we scope the lines of enquiry using a risk-based approach that follows up on the risks outlined in the strategic audit plans. This includes IM/IT aspects. Consequently, IM/IT lines of enquiry could be part of the overall lines of enquiry. Examples of lines of enquiry from recent audit chapters using this integrated approach are shown in **Appendix 1**.

Initial Planning and Scoping Questions

When planning and scoping an audit within a program or sector, the audit team should consider three critical IM/IT planning and scoping questions.

1. What data is available to support management's ability to make sound decisions?
2. Is this data reliable?
3. Is the IM/IT framework related to the program or sector consistent with the business objectives?

Examining these factors will help you determine if the entity is meeting the Treasury Board's requirements for effective information management, which are to have

- adequate governance structures, mechanisms, and resources;
- convenient access to relevant, reliable, comprehensive, and timely information for government programs and services; and
- support for the outcomes of programs and services, as well as operational needs and accountabilities.

If you judge that additional IM/IT aspects should be considered, there is a risk that the performance audit will resemble more of a technical IM/IT audit. In that case, you should consult the Service Delivery and Information Technology Team (SDIT) contact through the Internal Specialists section of our Office's INTRAnet, under Information Technology—Performance Audit.

IM/IT Risks to Identify

As indicated earlier, our performance audit topics are selected based on a risk-based assessment, which results in the strategic audit plans (SAPs). Auditors follow up at the planning phase for each audit, continually adding knowledge of business details and reviewing the SAP results. They conduct interviews and transaction walk-throughs with the entity representatives to confirm to what extent these risks are current.

For specific IM/IT risks originally identified in the SAP and related to the program or sector being audited, the audit team should consider reviewing, as a starting point, the enterprise or corporate risk plan (or equivalent document). This document would typically include the IM/IT risk categorized by severity level based on impact and the likelihood of the event happening, and could also include assigned responsibilities and a specific timeline by which the particular risk will be addressed.

Key Treasury Board guidance outlining the management of enterprise risk are the Framework for the Management of Risk and the Guide to Integrated Risk Management. Key Treasury Board polices that may affect IM/IT audit scoping are listed below. Please also refer to the associated standards and directives that are linked within these policies.

- **Policy Framework for Information and Technology**
- **Policy on Information Management**
- **Policy on Management of Information Technology**
- **Policy on Government Security**

Potential IM/IT Risk Indicators

The following are indicators of potential IM/IT risks, by management area, to look for when scoping a performance audit. The list is not inclusive but provides examples.

Keep in mind that if you discover one or several of these risks, you should not automatically include them in the scope of the audit. There may be compensating controls that render the risk severity low. Use professional judgment to assess to what extent these risks should be included in the scope of the audit.

Governance

- The Chief Information Officer (CIO) or his/her equivalent is not a member of a decision-making senior management team.
- The CIO or his/her equivalent reports to a line authority (such as the Director of Accounting) rather than to a senior manager. The line authority does not directly control a section or branch that is served by the CIO.
- There is no IT strategic and/or IT operational planning.
- The corporate strategic plan has no operational objectives involving IM/IT.
- There are no performance measurement metrics or scorecard to track progress on IT operational or tactical plans.
- There is no framework in place to assess new and emerging technology that can potentially improve and transform the entity's operations.
- There is an absence of IT risk planning (such as an IT risk management framework) or IT risk planning is inadequate.
- IM/IT risks are not included in corporate risks.
- Internal Audit has not reviewed or examined IM/IT risk areas for several years.
- Management and personnel in key areas, such as CIO and Chief Security Officer, either have a high turnover or these positions are vacant for longer periods of time.
- Management views IT as a complete service to the business side without any power to challenge business requirements.
- The number of people, particularly in IT systems and accounting, with requisite skill levels relative to the size and complexity of the operations is inadequate.
- In sectoral audits, several entities are producing common key decision-making information with different results and with little or no roles and responsibilities over data ownership.

System Acquisition, Development, and Implementation

There is no program management framework, which typically includes

- a project life cycle,
- a project control cycle, and
- tools and templates to facilitate the execution of the project.

There are no criteria for project prioritization.

There is a history of IT-enabled projects that fail to meet the initial budget and timelines, and fail to deliver the required functionalities.

Accounting systems and/or information systems, including IT systems, are not modified in response to changing conditions.

IM/IT Operations

There are inadequate or non-existent

- IT security policy
- threat and risk assessment
- offsite backup
- business continuity policy
- business impact analysis
- disaster recovery plan for critical systems and data

Critical systems continue to be impaired after a recent cyber attack.

IM/IT Service Delivery

There are inadequate or non-existent

- customer or service-level agreements
- performance metrics in customer or service-level agreements
- justification for outsourcing
- monitoring of outsourced performance metrics
- electronic record classification policy

Major business users complain about poor information for critical decision making.

There is little or no assurance that the entity is complying with all required legislation and/or its own business rules.

Questions to Consider in Scoping Data

Data is a large part of IM and the following questions help in linking IM planning and scoping. You can use these questions when scoping and forming the lines of enquiry.

- Does the data meet the following security objectives of Treasury Board's **Policy on Government Security**?

  Confidentiality: Does the data preserve authorized restrictions?

  Integrity: Does it guard against improper information modification or destruction?

  Availability: Does it ensure timely and reliable access to and use of information?

- Is the data complete and timely? That is, is there a framework that defines and maintains responsibilities for ownership of the information or data and related information systems? Are there procedures to ensure the integrity and consistency of key information stored in electronic form such as databases, data warehouses, and data archives?
- Does the data meet the requirements of the majority of business users?
- Is the data aligned to the entity's goals and objectives?

In the course of planning a performance audit, the audit team, through interviews or transaction walk-throughs, should include in the scope the IT systems and information to be examined.

From there, the audit questions and lines of enquiry are developed for the audit logic matrix, which are covered in the next section.

Developing Questions for Your Audit Logic Matrix

During the audit planning phase, IM/IT audit questions are developed that become audit sub-criteria supporting the main criteria of the audit of program or sector operations.

Appendix 2 contains examples of IM/IT audit questions to complement the program or sectoral performance audit, and relevant documents that can be reviewed, based on the three critical IM/IT questions listed **above** in the section “Initial Planning and Scoping Questions.”

Suggested Documents and Techniques for Auditing Information Management

Appendix 3 lists examples of documentation found internally and externally to the entity that are useful when auditing IM/IT.

FOR MORE INFORMATION AND GUIDANCE

This Practice Guide was prepared by the Service Delivery and Information Technology Team (SDIT). For more information, consult the SDIT contact person, found through the Internal Specialists section of our Office's INTRAnet under Information Technology—Performance Audit.

If audit teams identify IM/IT aspects while planning their performance audit, they should consult SDIT. If audit teams are considering excluding significant IM/IT risks from the scope of their performance audit, they will have to exercise professional judgment to assess the impact. At the very least, audit teams should consult SDIT early in the planning phase to determine to what extent SDIT should be involved with the audit.

No two performance audits are alike regarding the SDIT's extent of involvement. However, the SDIT team's extent of involvement with a performance audit depends mostly on the

- impact of publicly released information (e.g., news reports regarding a denial of service attack where the examined entity's critical systems are unavailable over an extended period of time);

- overall size and complexity of the audit;
- audit team’s perception of the severity of the IM/IT risks to be audited;
- initial planned IM/IT audit scope (e.g., number of IM/IT modules involved, such as business continuity planning, IT security, and IT strategic planning); and
- audit team’s previous performance audit IM/IT experience.

APPENDIX 1

SAMPLE AUDIT LINES OF ENQUIRY THAT INTEGRATE IM/IT

The following are examples of lines of enquiry (and their resulting criteria and audit objectives) in recent performance audits that integrate information management and information technology with the overall audit.

From the criteria used in the spring 2013 report, chapter 7 on federal search and rescue (SAR) activities:

> “SAR information systems adequately support operational requirements, are properly managed, and are available and usable when required.”
>
> “SAR information systems provide quality information, support strategic requirements, and facilitate decision making and reporting.”

From the criteria used in the fall 2013 report, chapter 5 on preventing illegal entry into Canada:

> “Information systems critical to preventing the illegal entry of people into Canada
>
> - provide quality information,
> - are available and usable when required,
> - are properly managed, and
> - facilitate reporting requirements and decision making.”

APPENDIX 2

SAMPLE IM/IT AUDIT QUESTIONS

The following are examples of IM/IT audit questions that teams can ask to complement the program or sectoral performance audit, and relevant documents the team can review, based on the three critical IM/IT planning and scoping questions listed in the section of this Practice Guide called "Questions to Develop for Your Audit Logic Matrix."

IM/IT Planning and Scoping Question	IM/IT Audit Questions	Examples of Relevant Documents to Review
1. What data is available?	• What is the key data for the program or sector to be audited and what are the related governance structures and mechanisms? • To what extent are business users involved in the risk assessment framework? • How does the entity ensure that its data is appropriate to make senior management decisions consistent with its mission and mandate?	• Organization charts • Working group and senior committee terms of reference and minutes • General description of the entity's risk assessment framework • Internal audit reports and third-party assessments • Related IT-enabled project descriptions and progress to date

IM/IT Planning and Scoping Question	IM/IT Audit Questions	Examples of Relevant Documents to Review
2. Is this data reliable?	• To what extent is data meeting the general security objectives of confidentiality, availability, and integrity? • How does the entity ensure that the security of its data complies with its own internal policies as well as the Policy on Government Security and other externally mandated policies? • Have meeting security objectives been previously identified as an issue and, if so, what action has been taken? • Are roles and responsibilities over data ownership and accountabilities clearly defined? • Are there service level agreements between the major business users and the IT section? If so, do these cover • availability, • reliability, • performance, • capacity for growth, • levels of support required for users, and • continuity planning and security?	• Related IT-enabled project descriptions and progress to date • Enterprise threat and risk assessments • Internal audit reports and third-party assessments • Other internal documents demonstrating compliance with specific security policies • Security policy • Data integrity policy • Terms of reference for data integrity working groups • Frameworks that relate to assurance over data being complete and timely • Examples of service level agreements and related clauses

IM/IT Planning and Scoping Question	IM/IT Audit Questions	Examples of Relevant Documents to Review
3. Is the IM/IT framework consistent with business objectives?	• What feedback mechanisms monitor if data requirements of business users are met and if they are working adequately? • Does the governance framework ensure that the requirements of business users are met? • Does the strategic planning framework ensure that the requirements of business users are met? • Do the entity's strategic documents consider data needs and data strategy?	• Results of internal surveys covering the needs of business users and related action plans where issues were noted and how these were addressed • Description of governance framework as it relates to the relevancy of data required for critical management decisions • Strategic plan • Operational (or tactical) plan • Internal audit reports and third-party assessments

APPENDIX 3

SAMPLE DOCUMENTS USEFUL WHEN AUDITING IM/IT

Documents internal to the entity

- IM/IT strategic and operational plans
- IM/IT investment plans
- IM/IT performance measurement frameworks
- Business continuity and other related plans
- Policy suites (e.g., IT security)
- Minutes of senior management committees affecting significant IM/IT decisions and related presentations and briefing notes
- Corporate risk (or equivalent) document that indicates IM/IT risks
- IM/IT risk assessments (where not included in the corporate risk document)
- Internal audits and third-party studies affecting IM/IT
- Treasury Board submissions and memoranda to Cabinet that affect significant IM/IT decisions

Documents available online

- Recent news articles, industry journals
- Parliamentary updates
- Public Accounts: detailed disclosures (e.g., aging IM/IT systems, known as “legacy” systems)
- Senate and House of Commons committee reports affecting significant IM/IT decisions

Audit techniques (common to any performance audit)

- Conducting interviews
- Analyzing documents
- Conducting walk-throughs, an audit procedure involving an interview with entity officials to assist the audit team to better understand frameworks covering
    - strategic and operational planning;
    - risk assessments, their prioritization, and mitigation;
    - investment program management (including IT-enabled projects); and
    - assurance of data integrity.
- Consulting with the Service Delivery and Information Technology Team in the early stages of planning