Municipality of Thames Centre

Audit Planning Report for the year ending December 31, 2024

KPMG LLP

Licensed Public Accountants

Prepared as of March 25, 2025 for presentation to Council on April 7, 2025

kpmg.ca/audit

KPMG contacts

Key contacts in connection with this engagement

Katie denBok
Lead Audit Engagement Partner
519-660-2115
kdenbok@kpmg.ca

Emily Pellarin
Audit Manager
519-660-2601
epellarin@kpmg.ca

Table of contents

Digital use information

This Audit Planning Report is also available as a “hyper-linked” PDF document.

If you are reading in electronic form (e.g. In “Adobe Reader” or “Board Books”), clicking on the home symbol on the top right corner will bring you back to this slide.

Click on any item in the table of contents to navigate to that section.

Audit highlights

No matters to report

Matters to report – see link for details

Scope

Our audit of the consolidated financial statements ("financial statements") of the Municipality of Thames Centre ("the Municipality") as of and for the year ending December 31, 2024, will be performed in accordance with Canadian generally accepted auditing standards (CASs).

Audit strategy

Materiality $500,000

Involvement of others

Audit strategy - Group audit

The consolidated financial statements are comprised of the unconsolidated Municipality of Thames Centre and the Dorchester Union Cemetery. For the purposes our audit, given that the processes and risks are similar, we have considered there to be one component for audit purposes. As such, our audit covers 100% of the assets and revenues of both entities.

Risk assessment

Presumed risk of management override of controls

Other significant risks

Presumed risk of fraudulent revenue recognition

Risk assessment

Other risks of material misstatement

- Cash
- Asset retirement obligations
- Tangible capital assets, including implementation of PS 3160 – Public Private Partnerships (3P)
- Revenue and accounts receivable, including implementation of PS 3400 Revenue
- Deferred revenue – general and obligatory reserve funds
- Long-term debt
- Expenses – salaries and benefits
- Accounts payable, accrued liabilities and expenses
- Contingencies

Refer to slides 8 – 17 for risk assessments.

The purpose of this report is to assist you, as a member of Council, in your review of the plan for our audit of the financial statements. This report is intended solely for the information and use of Management and Council and should not be used for any other purpose or any other party. KPMG shall have no responsibility or liability for loss or damages or claims, if any, to or by any third party as this report to Council has not been prepared for, and is not intended for, and should not be used by, any third party or for any other purpose.

Specific items

New significant risks

No new significant financial reporting risks identified

Other significant changes

Newly effective accounting standards

PS 3400, *Revenue*, becomes effective for this year end (fiscal years beginning on or after April 1, 2023).

The new standard establishes a single framework to categorize revenue to enhance the consistency of revenue recognition and its measurement.

The standard notes that in the case of revenue arising from an exchange transaction, a public sector entity must ensure the recognition of revenue aligns with the satisfaction of related performance obligations. It notes that unilateral revenue arises when no performance obligations are present, and recognition occurs when there is authority to record the revenue and an event has happened that gives the public sector entity the right to the revenue.

PS 3160, *Public private partnership*, becomes effective for this year end (fiscal years beginning on or after April 1, 2023).

The standard includes new requirements for the recognition, measurement and classification of infrastructure procured through a public private partnership.

The standard notes that recognition of infrastructure by the public sector entity would occur when it controls the purpose and use of the infrastructure, when it controls access and the price, if any, charged for use, and it controls any significant interest accumulated in the infrastructure when the public private partnership ends.

PSG 8, *Purchased intangibles*, becomes effective for this year end (fiscal years beginning on or after April 1, 2023).

The guideline allows public sector entities to recognize intangibles purchased through an exchange transaction. The definition of an asset, the general recognition criteria and GAAP hierarchy are used to account for purchased intangibles.

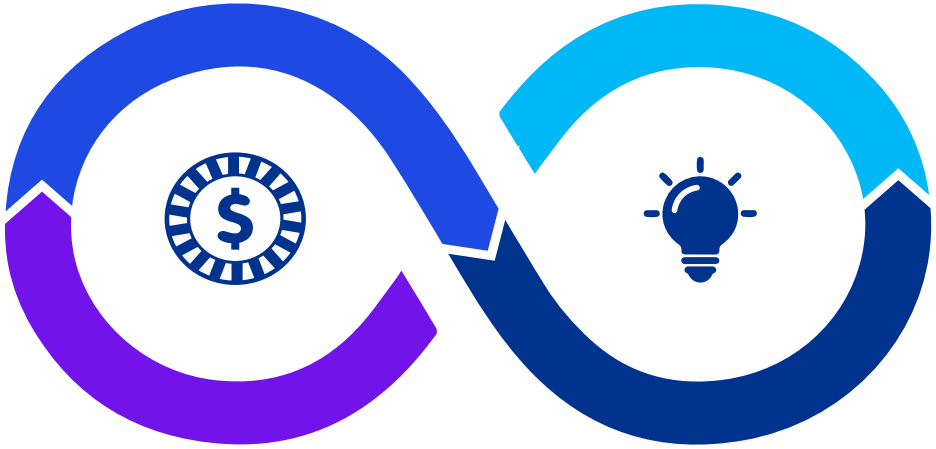
Narrow scope amendments were made to PS 1000 *Financial statement concepts* to remove the prohibition to recognize purchased intangibles and to PS 1201 *Financial statement presentation* to remove the requirement to disclose purchased intangibles not recognized.

Other accounting standards that are effective for future fiscal years have been outlined in the Appendices.

Communications with predecessor auditor

We have held communications with the predecessor auditor in relation to the fiscal 2023 audit. We discussed the work that was performed by the predecessor ,as well as any other required areas such that we were able to gain comfort around the opening balances for 2024.

Materiality



We ***initially determine materiality*** at a level at which we consider that misstatements could reasonably be expected to influence the economic decisions of users. Determining materiality is a matter of ***professional judgement***, considering both quantitative and qualitative factors, and is affected by our perception of the common financial information needs of users of the financial statements as a group. We do not consider the possible effect of misstatements on specific individual users, whose needs may vary widely.

We ***reassess materiality*** throughout the audit and revise materiality if we become aware of information that would have caused us to determine a different materiality level initially.

Plan and perform the audit

We ***initially determine materiality*** to provide a basis for:

- Determining the nature, timing and extent of risk assessment procedures;
- Identifying and assessing the risks of material misstatement; and
- Determining the nature, timing, and extent of further audit procedures.

We design our procedures to detect misstatements at a level less than materiality in individual accounts and disclosures, to reduce to an appropriately low level the probability that the aggregate of uncorrected and undetected misstatements exceeds materiality for the financial statements as a whole.

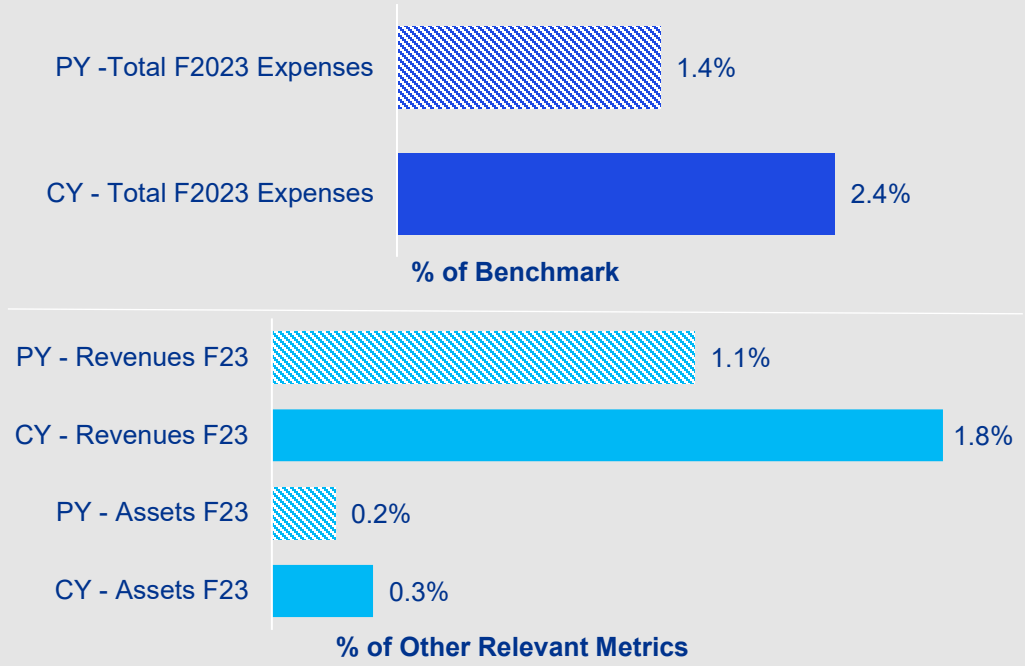
Evaluate the effect of misstatements

We also ***use materiality*** to evaluate the effect of:

- Identified misstatements on our audit; and
- Uncorrected misstatements, if any, on the financial statements and in forming our opinion.

Initial materiality

Materiality
$500,000
(2023: $315,000)



Prior Year Total Consolidated Expenses
$21,842,130
(2022: $21,398,506)

Prior Year Total Consolidated Assets
$ 186,699,339
(2022: $179,659,258)

Prior Year Total Consolidated Revenues
$27,949,169
(2022: $29,165,669)

Audit Misstatement Posting Threshold
$25,000
(2023: $15,750)

Risk assessment summary

Our planning begins with an assessment of risks of material misstatement in your financial statements.

We draw upon our understanding of the Municipality and its environment (e.g. the industry, the wider economic environment in which the business operates, etc.), our understanding of the Municipality's components of its system of internal control, including our business process understanding.

		Risk of fraud	Risk of error	CY risk rating
●	Improper revenue recognition	✓		Presumed - Rebutted
●	Management override of controls	✓		Presumed - Significant
●	Cash		✓	Base
●	Asset retirement obligations		✓	Base
●	Tangible capital assets		✓	Elevated
●	Revenue and accounts receivable (including new standard implementation of PS 3400)		✓	Base
●	Deferred revenue – general and obligatory reserve funds		✓	Base

● SIGNIFICANT RISK ● PRESUMED RISK OF MATERIAL MISSTATEMENT ● OTHER RISK OF MATERIAL MISTATEMENT

Risk assessment summary (continued)

		Risk of fraud	Risk of error	CY risk rating
●	Long-term debt		✓	Base
●	Expenses – salaries and benefits		✓	Base
●	Accounts payable, accrued liabilities and expenses		✓	Base
●	Contingencies		✓	Base

● SIGNIFICANT RISK ● PRESUMED RISK OF MATERIAL MISSTATEMENT ● OTHER RISK OF MATERIAL MISTATEMENT

Significant risks

Management Override of Controls (non-rebuttable significant risk of material misstatement)

RISK OF FRAUD

Presumption of the risk of fraud resulting from management override of controls

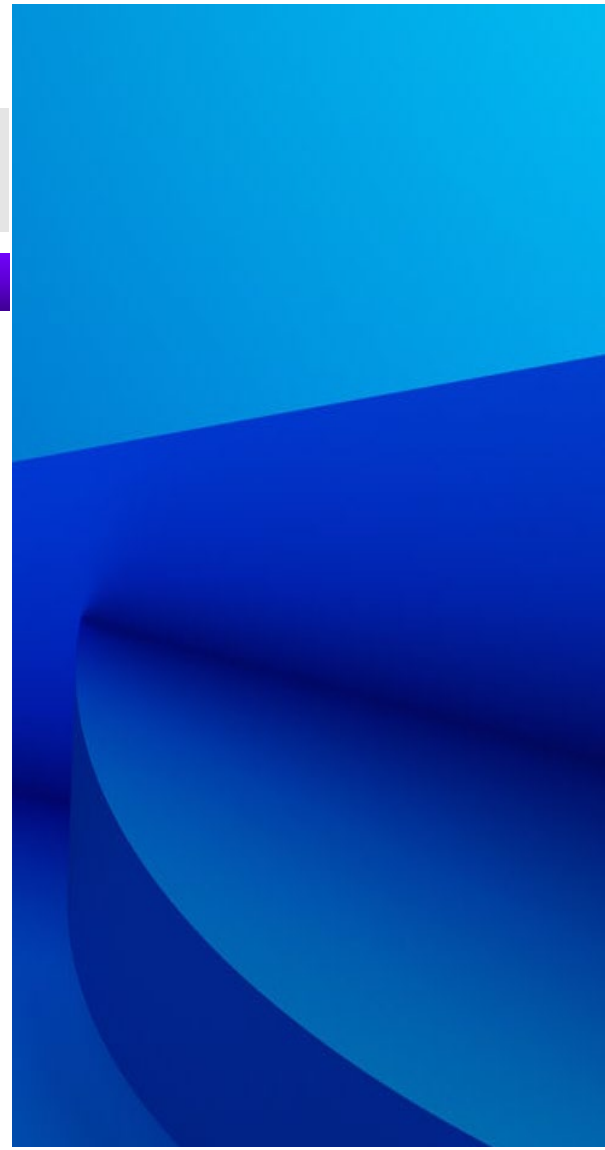
Why is it significant?

Management is in a unique position to perpetrate fraud because of its ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Although the level of risk of management override of controls will vary from entity to entity, the risk nevertheless is present in all entities.

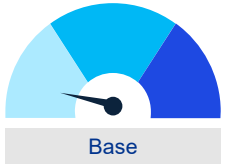
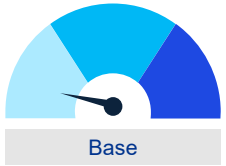
Our planned response

As this presumed risk of material misstatement due to fraud is not rebuttable, our audit methodology incorporates the required procedures in professional standards to address this risk. These procedures include:

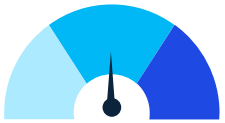
- testing of journal entries and other adjustments,
- performing a retrospective review of estimates
- evaluating the business rationale of significant unusual transactions.



Other areas of focus

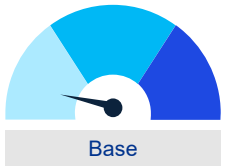
Areas	Level of risk due to error	Our planned response
Cash **Applicable Components:** The Municipality of Thames Centre	 Base	• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting. • Obtain year-end bank reconciliations and perform substantive testing over significant reconciling items. • Obtain confirmations from third party financial institutions. • Review of financial statement note disclosures in accordance with PSAS.
Asset retirement obligations **Applicable Components:** The Municipality of Thames Centre	 Base	• Update our understanding of the activities over the initiation, authorization, processing, recording and reporting. • Obtain an understanding of the approach taken by Management to identify changes to ARO, including updates to cost estimates. • Obtain management's updated assessment of ARO. If significant, select a sample of changes in the estimate and vouch to supporting documentation. • Review of financial statement note disclosures in accordance with PSAS.

Other areas of focus

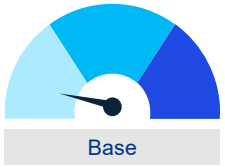
Areas	Level of risk due to error	Our planned response
Tangible capital assets **New standard implementation of PS 3160, *Public Private Partnerships (P3)*** **Applicable Components:** The Municipality of Thames Centre	 Elevated	• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting. • Perform substantive tests of details over additions (including contributed tangible capital assets) and disposals. • Obtain the amortization policy, verify the mathematical accuracy of amortization through recalculations, and assess reasonableness of the estimated useful lives. • Review construction in progress to ensure amounts are properly transferred to correct capital asset classes and amortization expense commences on a timely basis. • Perform procedures over the fair value of contributed assets, including obtaining an understanding of the process taken to determine the cost estimates. Assess the method, data and assumptions used by Management in the calculation. • Obtain an understanding of the transitional provisions applied upon initial implementation of PS 3160 and the approach taken by Management to identify the partnerships in scope of the standard. ◦ For any significant partnerships expected to be in scope of the standard, obtain the agreements and Management's analysis against the criteria set out in the standard, including the analysis as to whether an infrastructure asset should be recognized and a liability recorded, if any. • Review of financial statement note disclosures in accordance with PSAS. • Perform required procedures to assess the potential risks with respect to impairment of assets. Based on the nature of the Municipality's operations, it is not expected that this will be a significant risk during the audit.

Other areas of focus

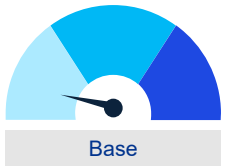
Areas	Level of risk due to error	Our planned response

Revenue and accounts receivable (including taxation revenue, user charges and other revenue sources, and government transfers)
 	
New standard implementation of PS 3400, *Revenue*
 	
Applicable Components: The Municipality of Thames Centre
		• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting.
		• Perform substantive audit procedures to recalculate taxation revenue using approved tax rates and assessment data.
		• Obtain a listing of government transfer revenue reported by the Municipality and perform tests of details using representative sampling methods. Obtain supporting documentation for the eligibility criteria for the sample selected to determine if the government transfers reported in the financial statements meet the criteria outlined in the PSAS.
		• Obtain an understanding of the approach taken by Management to identify the revenue streams which are in-scope of the PS 3400 standard.
		  ◦ Perform substantive testing to ensure the list used for the estimate is complete.
		  ◦ Obtain Management's assessment of key assumptions and assess for reasonability.
		  ◦ If adjustments are significant, select a sample and vouch to supporting documentation.
		• Obtain a listing of user charges and other revenue balances and perform tests of details using a combination of substantive analytical and sampling approaches.
		• Obtain a listing of accounts receivable balances and select significant balances to vouch to supporting documentation and assess analytical trends.
		• Review of financial statement disclosures in line with PSAS, including additional or revised disclosures required under the new standard.

Other areas of focus

Areas	Level of risk due to error	Our planned response
Deferred revenue – general and obligatory reserve funds **Applicable Components:** The Municipality of Thames Centre		• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting. • Obtain the management prepared calculation for the development charges balance and vouch receipts and expenditures on a sample basis. Verify recognition of revenue is based on project spending in accordance with the purpose of the obligatory reserve. • Perform a recalculation of interest allocated to assess reasonableness of management's calculation. • Perform substantive audit procedures over a sample of deferred capital grants, security deposits and other deferred revenue by vouching to supporting documents. • Review financial statement disclosures in line with PSAS.

Other areas of focus

Areas	Level of risk due to error	Our planned response
Long-term debt **Applicable Components:** The Municipality of Thames Centre		• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting. • Obtain and review any new or amended agreements for long-term debt issued by the Municipality, including review of by-laws issued by Council. • Confirm debt balances with third parties. Where unable to do so, select a sample of principal repayments and vouch to supporting documentation. • Review of financial statement disclosures in accordance with PSAS.
Expenses – salaries and benefits **Applicable Components:** The Municipality of Thames Centre		• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting. • Perform testing over selected controls related to the payroll process. • Select a sample of employee salary expenses and vouch to supporting documentation. • Perform substantive analytical procedures over benefits expense as a percentage of total salaries. • Perform substantive procedures over payroll-related accruals. • Obtain new or amended collective bargaining agreements. Assess if management has evaluated these agreements for implications of retroactive application. Such retroactive application can result in additional financial obligations for the Municipality that are required to be reported in the financial statements.

Other areas of focus

Areas	Level of risk due to error	Our planned response
Accounts payable, accrued liabilities and expenses **Applicable Components:** The Municipality of Thames Centre		• Obtain an understanding of the activities over the initiation, authorization, processing, recording and reporting. • Perform search for unrecorded liabilities. • Examine significant accrued liabilities and vouch to supporting documentation. • Perform substantive tests of details on selected non-payroll expenditures.
Contingencies **Applicable Components:** The Municipality of Thames Centre		• Perform a detailed review of Council meeting minutes for potential contingencies. • Directly communicate with internal legal counsel (and external as necessary) to ensure that all significant contingent liabilities are appropriately disclosed and/or recorded. • Review of significant findings with management during planning and completion stages of the audit.

Required inquiries of Council

Inquiries regarding risk assessment, including fraud risks

- What are Council's views about fraud risks, including management override of controls, in the Municipality? And have you taken any actions to respond to any identified fraud risks?
- Is Council aware of, or has Council identified, any instances of actual, suspected, or alleged fraud, including misconduct or unethical behavior related to financial reporting or misappropriation of assets?
  - If so, have the instances been appropriately addressed and how have they been addressed?
- How does Council exercise oversight of the Municipality's fraud risks and the establishment of controls to address fraud risks?

Inquiries regarding company processes

- Is Council aware of tips or complaints regarding the Municipality's financial reporting (including those received through the Council's internal whistleblower program, if such programs exist)? If so, Council's responses to such tips and complaints?

Inquires regarding related parties and significant unusual transactions

- Is Council aware of any instances where the Municipality entered into any significant unusual transactions?
- What is Council's understanding of the Municipality's relationships and transactions with related parties that are significant to the Municipality?
- Is Council concerned about those relationships or transactions with related parties? If so, the substance of those concerns?

Key milestones and deliverables

December 2024 – March 2025

Planning & Risk Assessment

- Kickoff with management
- Communicate audit plan
- Identify IT applications and environments
- Obtain and update an understanding of the Municipality and its environment
- Inquire of Council, management and others within the Municipality about risks of material misstatement
- Planning and initial risk assessment procedures, including:
  - Involvement of others
  - Identification and assessment of risks of misstatements and planned audit response for certain processes
- Perform process walkthroughs for certain business processes
- Coordinate with Internal Audit
- Evaluate the Municipality's components of internal control, other than the control activities component

April – July 2025

Risk Assessment & Final Fieldwork

- Perform process walkthroughs for remaining business processes
- Identify process risk points for certain business processes
- Complete initial risk assessment
- Evaluate the design and implementation of controls for certain business processes (control activity component)
- Perform a test of operating effectiveness of control activities
- Perform interim substantive audit procedures
- Complete year-end data extraction and processing activities
- Complete the test of operating effectiveness for remaining controls
- Perform substantive audit procedures
- Evaluate results of audit procedures, including control deficiencies and audit misstatements identified
- Review financial statement disclosures

September 2025

Reporting

- Present audit results to the Audit Committee and perform required communications
- Issue audit report on financial statements
- Closing meeting with management

Audit quality - How do we deliver audit quality?

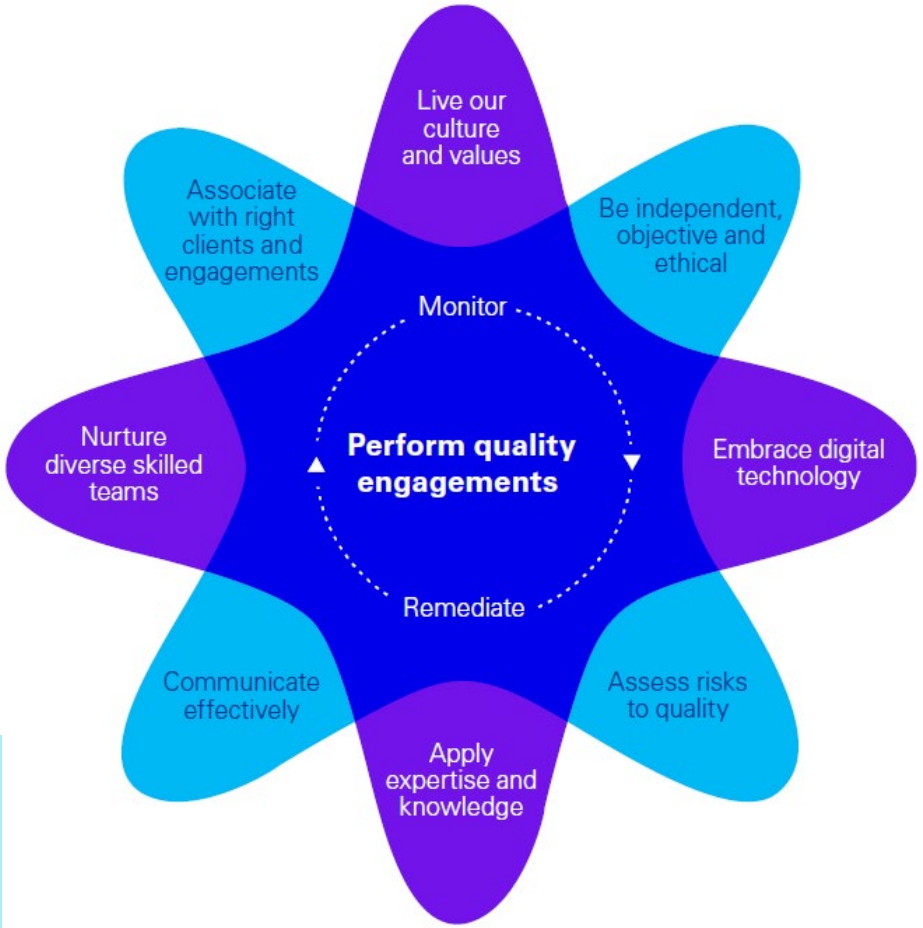
Quality essentially means doing the right thing and remains our highest priority. Our Global Quality Framework outlines how we deliver quality and how every partner and staff member contributes to its delivery.

The drivers outlined in the framework are the ten components of the KPMG System of Quality Management (SoQM). Aligned with ISQM 1/CSQM 1, our SoQM components also meet the requirements of the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA) and the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting in Canada, which apply to professional services firms that perform audits of financial statements. Learn more about our system of quality management and our firm's statement on the effectiveness of our SoQM:

KPMG Canada Transparency Report

We define 'audit quality' as being the outcome when:

- audits are **executed consistently**, in line with the requirements and intent of **applicable professional standards** within a strong **system of quality management;** and
- all of our related activities are undertaken in an environment of the utmost level of **objectivity, independence, ethics** and **integrity.**



Doing the right thing. Always.

Indicators of audit quality (AQIs)

The objective of these measures is to provide more in-depth information about factors that influence audit quality within an audit process. Below are the AQIs that we have agreed with management are relevant for the audit. We would like to obtain agreement of the Audit Committee that these are the relevant AQIs.

We will communicate the status of the below AQIs on an annual basis.

Team composition

Experience of the team

- Role – number of years experience in the industry, number of years on this engagement

Technology in the audit

Implementation of Technology in the Audit

- Increase in use of technology in the audit year over year

Engagement focus

Time as a percentage of total time spent by level and phase of the audit

- Percentage of hours incurred by Partner, Manager and audit staff

Timing of prepared by client (PBC) items

Timeliness of PBC items

- Number of timely and overdue items received by the audit team.

Quality reviews

Results of internal and external reviews

- Number and nature of findings specific to the audit engagement

Independence: Fees

In determining the fees for our services, we have considered the nature, extent and timing of our planned audit procedures as described above. Our fee analysis has been reviewed with and agreed upon by management.

Audit services	Base Fee
Municipality of Thames Centre – Audit of consolidated financial statements	$40,000
Municipality of Thames Centre Trust Funds – Audit of financial statements	$7,500
Implementation of new accounting standards (PS 3400, Revenue; PS 3160 Public Private Partnerships; PSG-8 Intangible Assets)	Fee to be determined based on total hours worked
Implementation of new auditing standards (CAS 600 Revised special considerations – Audits of group financial statements)	Fee to be determined based on total hours worked, if any
Total	$47,500 + additional one-time fees noted above, if any

Matters that could impact our fee

The proposed fees above are based on assumptions described in the engagement letter dated January 27, 2025.

The critical assumptions and factors that could cause a change in our fees include:

- Significant changes to the relevant financial reporting framework or significant new or changed accounting policies or application thereof
- Significant changes to internal control over financial reporting
- Significant audit misstatements identified
- Changes in the timing of our work
- Significant unusual and/or complex transactions
- Other significant issues (e.g. cyber security breaches)

Appendices

- **A** Regulatory communications
- **B** New accounting standards
- **C** New audit standards
- **D** Audit and assurance insights
- **E** Insights to enhance your business
- **F** Thought leadership and insights
- **G** Fraud prevention
- **H** Cyber for Municipalities

Appendix A: Regulatory communications

CPAB communication protocol

The reports available through the following links were published by the Canadian Public Accountability Board to inform Audit Committees and other stakeholders about the results of quality inspections conducted over the past year:

- CPAB Audit Quality Insights Report: 2022 Annual Inspections Results
- CPAB Audit Quality Insights Report: 2023 Interim Inspections Results
- CPAB Regulatory Oversight Report: 2023 Annual Inspections Results
- CPAB Audit Quality Insights Report: 2024 Interim Inspections Results

Appendix B: Changes in accounting standards – Future

Standard	Summary and implications
Employee Benefits	• The Public Sector Accounting Board has initiated a review of sections PS 3250 Retirement benefits and PS 3255 Post-employment benefits, compensated absences and termination benefits. It will apply to fiscal years beginning on or after April 1, 2026. Early adoption will be permitted and guidance applied retroactively. • The intention is to use principles from International Public Sector Accounting Standard 39 Employee benefits as a starting point to develop the Canadian standard. • Given the complexity of issues involved and potential implications of any changes that may arise from the review of the existing guidance, the new standards will be implemented in a multi-release strategy. The first standard will provide foundational guidance. Subsequent standards will provide additional guidance on current and emerging issues. • The proposed section PS 3251 Employee benefits will replace the current sections PS 3250 Retirement benefits and PS 3255 Post-employment benefits, compensated absences and termination benefits. • This proposed section would result in public sector entities recognizing the impact of revaluations of the net defined benefit liability (asset) immediately on the statement of financial position. Organizations would also assess the funding status of their post-employment benefit plans to determine the appropriate rate for discounting post-employment benefit obligations. • The Public Sector Accounting Board is in the process of evaluating comments received from stakeholders on the exposure draft. • Municipality year-end impacted by this change: December 31, 2027

Appendix B: Changes in accounting standards – Future

Standard	Summary and implications
Concepts Underlying Financial Performance	• The revised conceptual framework is effective for fiscal years beginning on or after April 1, 2026 with earlier adoption permitted. • The framework provides the core concepts and objectives underlying Canadian public sector accounting standards. • The ten chapter conceptual framework defines and elaborates on the characteristics of public sector entities and their financial reporting objectives. Additional information is provided about financial statement objectives, qualitative characteristics and elements. General recognition and measurement criteria, and presentation concepts are introduced. • Municipality year-end impacted by this change: December 31, 2027
Government not-for-profit strategy	• The Public Sector Accounting Board has approved its government not-for-profit ("GNFP") strategy implementation plan. All proposed changes to the PS 4200 series, PSAS, and potential customizations will be subject to due process before PSAB finalizes any changes to the PS Handbook. There is no tentative date for the change. • The approved strategy option is to incorporate the PS 4200 series of standards with potential customizations into public sector accounting standards. This means reviewing the existing PS 4200 series of standards to determine if they should be retained and added to public sector accounting standards. Incorporating the updated or amended PS 4200 series standards in public sector accounting standards would make the guidance available to any public sector entity. Accounting and/or reporting customizations may be permitted if there are substantive and distinct accountabilities that warrant modification from public sector accounting standards.

Appendix B: Changes in accounting standards – Future

Standard	Summary and implications

Financial Statement Presentation	• The proposed section PS 1202 Financial statement presentation will replace the current section PS 1201 Financial statement presentation. PS 1202 Financial statement presentation will apply to fiscal years beginning on or after April 1, 2026 to coincide with the adoption of the revised conceptual framework. Early adoption will be permitted.
	• The proposed section includes the following:
	  • Relocation of the net debt indicator to its own statement called the statement of net financial assets/liabilities, with the calculation of net debt refined to ensure its original meaning is retained.
	  • Separating liabilities into financial liabilities and non-financial liabilities.
	  • Restructuring the statement of financial position to present total assets followed by total liabilities.
	  • Changes to common terminology used in the financial statements, including re-naming accumulated surplus (deficit) to net assets (liabilities).
	  • Removal of the statement of remeasurement gains (losses) with the information instead included on a new statement called the statement of changes in net assets (liabilities). This new statement would present the changes in each component of net assets (liabilities), including a new component called “accumulated other”.
	  • A new provision whereby an entity can use an amended budget in certain circumstances.
	  • Inclusion of disclosures related to risks and uncertainties that could affect the entity’s financial position.
	• The Public Sector Accounting Board is currently deliberating on feedback received on exposure drafts related to the reporting model.
	• Municipality year-end impacted by this change: December 31, 2027

Appendix C: Newly effective and upcoming changes to auditing standards

For more information on newly effective and upcoming changes to auditing standards - see Current Developments

Effective for periods beginning on or after December 15, 2023

ISA 600/CAS 600

Revised special considerations – Audits of group financial statements

Effective for periods beginning on or after December 15, 2024

ISA 260/CAS 260

Communications with those charged with governance

ISA 700/CAS 700

Forming an opinion and reporting on the financial statements

Appendix D: Audit and assurance insights

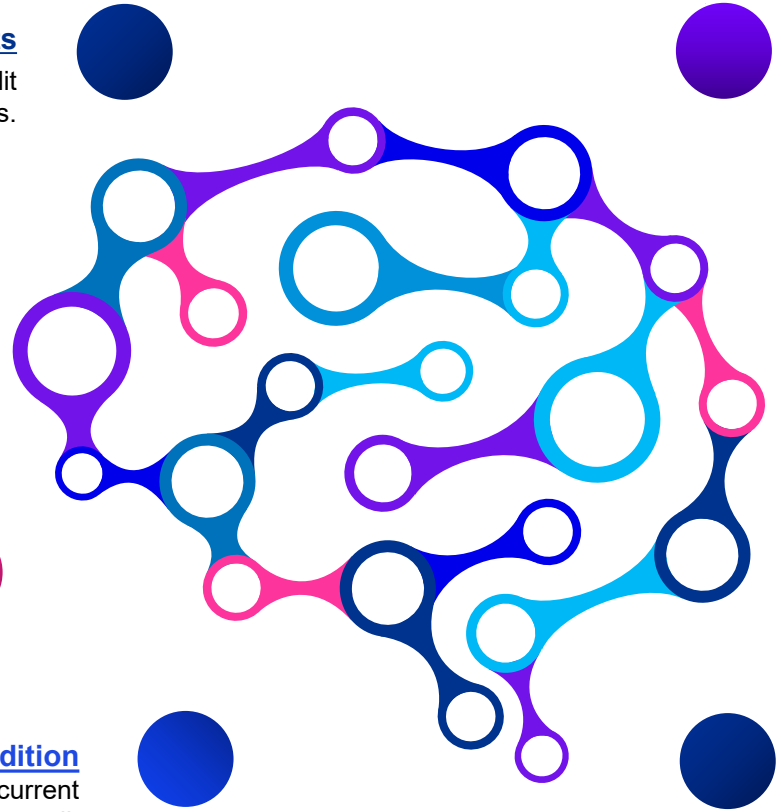
Our latest thinking on the issues that matter most to Audit Committees, board of directors and management.

KPMG Audit & Assurance Insights
Curated research and insights for audit committees and boards.

Board Leadership Centre
Leading insights to help board members maximize boardroom opportunities

Current Developments
Series of quarterly publications for Canadian businesses including Spotlight on IFRS, Canadian Securities & Auditing Matters and US Outlook reports.

Audit Committee Guide – Canadian Edition
A practical guide providing insight into current challenges and leading practices shaping audit committee effectiveness in Canada.



Government and Public Sector Insights
Navigating the contentious issues disrupting all government and public sector organizations requires the steady hand of a trusted guide.

Insights - KPMG Canada

KPMG Climate Change Financial Reporting Resource Centre
Our climate change resource center provides insights to help you identify the potential financial statement impacts to your business.

Sustainability Reporting
Resource centre on implementing the new Canadian reporting standards

Appendix E: Insights to enhance your business

Learn more

We have the unique opportunity as your auditors to perform a deeper dive to better understand your business processes that are relevant to financial reporting.

Lean in Audit

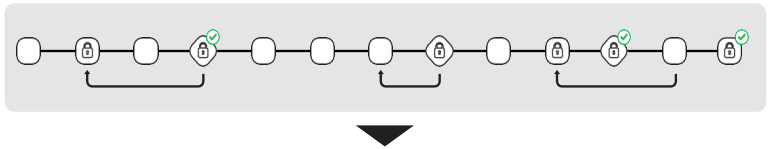
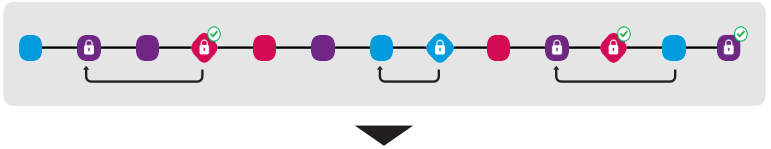
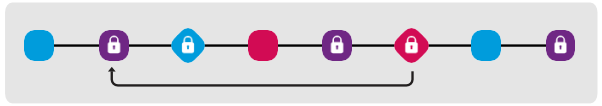
Lean in Audit™ is KPMG's award-winning methodology that offers a new way of looking at processes and engaging people within your finance function and organization through the audit.

By incorporating Lean process analysis techniques into our audit procedures, we can enhance our understanding of your business processes that are relevant to financial reporting and provide you with new and pragmatic insights to improve your processes and controls.

Clients like you have seen immediate benefits such as improved quality, reduced rework, shorter processing times and increased employee engagement.

We look forward to working with you to incorporate this approach in your audit.

How it works

Standard Audit	Typical process and how it's audited	
Lean in Audit	Applying a Lean lens to perform walkthroughs and improve Audit quality while identifying opportunities to minimize risks and redundant steps	
How Lean in Audit helps improve businesses processes	Make the process more streamlined and efficient for all	

Value: what customers want **(maximize)**

Necessary: required activities **(minimize)**

Redundant: non-essential activities **(remove)**

Process controls

Key controls tested

Appendix F: Thought leadership and insights

2024 CEO Outlook

From the race to embrace artificial intelligence (AI) to ever-mounting geopolitical concerns, the challenges faced by the CEOs of today are vast and complex. Alongside these external pressures, internal challenges such as upskilling the workforce and hybrid working are pushing CEOs to be agile and adaptable in their stakeholder management while also keeping an eye on long-term growth. The KPMG CEO Outlook surveys more than 1,300 global business leaders who share their views on geopolitics, return-to-office, ESG and generative AI.

Click here to access KPMG's portal.

Future of Risk

Enterprises are facing an array of reputational, environmental, regulatory and societal forces. To navigate this complex landscape, the C-suite should seek to embrace risk as an enabler of value and fundamentally transform their approach. KPMG's global survey of 400 executives reveals that their top priorities for the next few years are adapting to new risk types and adopting advanced analytics and AI. As organizations align risk management with strategic objectives, closer collaboration across the enterprise will be essential.

Click here to access KPMG's portal.

Resilience Amid Complexity

In today's rapidly evolving and interconnected business landscape, organizations face unprecedented challenges and an increasingly complex and volatile risk landscape that can threaten their competitiveness and future survival. We share revealing real-world examples of how companies have overcome their challenges and emerged stronger as the rapid pace of change accelerates and look at the key components of KPMG's enterprise resilience framework and how it is helping these businesses build resilience and achieve their strategic objectives in an increasingly uncertain world.

Click here to access KPMG's portal.

Future of Procurement

Procurement is at an exciting point where leaders have the opportunity to recast their functions as strategic powerhouses. In this global report we examine how these forces may affect procurement teams and discuss how procurement leaders can respond – and the capabilities they will need to thrive. Our insights are augmented by findings from the KPMG 2023 Global Procurement Survey, which captured the perspectives of 400 senior procurement professionals around the globe, representing a range of industries.

Click here to access KPMG's portal.

Appendix F: Thought leadership and insights (continued)

Artificial Intelligence in Financial Reporting and Audit

Artificial intelligence (AI) is transforming the financial reporting and auditing landscape, and is set to dramatically grow across organizations and industries. In our new report, KPMG surveyed 1,800 senior executives across 10 countries, including Canada, confirming the importance of AI in financial reporting and auditing. This report highlights how organizations expect their auditors to lead the AI transformation and drive the transformation of financial reporting. They see a key role for auditors in supporting the safe and responsible rollout of AI, including assurance and attestation over the governance and controls in place to mitigate risks.

Click here to access KPMG's portal.

Control System Cybersecurity Annual Report 2024

Based on a survey of more than 630 industry members (13% from government organizations), this report reveals that while the increase in cyberattacks is concerning, organizations have become more proactive in their cybersecurity budgets, focused on prevention, and acknowledging the threat of supply chain attacks. Furthermore, the report highlights a pressing need for skilled cybersecurity professionals in the face of escalating cyber threats. Explore the full report to help gain a clearer understanding of the growing cyber threat landscape and learn how to overcome the roadblocks to progress.

Click here to access KPMG's portal.

Cybersecurity Considerations 2024: Government and Public Sector

In every industry, cybersecurity stands as a paramount concern for leaders. Yet, for government and public sector organizations, the game of digital defense takes on a whole new level of intensity. The reason? The sheer volume and sensitivity of data they manage, which can amplify the potential fallout from any breach. These agencies are the custodians of a vast array of personal and critical data, spanning from citizen welfare to public safety and national security. This article delves into the pivotal cybersecurity considerations for the government and public sector. It offers valuable perspectives on critical focus areas and provides actionable strategies for leaders and their security teams to fortify resilience, drive innovation, and uphold trust in an ever-changing environment.

Click here to access KPMG's portal.

Appendix F: Thought leadership and insights (continued)

Why the Public Sector Must Take the Lead in Sustainability Reporting

As the world prepares for the implementation of sustainability reporting standards from the International Sustainability Board (ISSB), the need for public sector leadership is pronounced. While governments around the world have collaborated on vital policy and regulatory solutions, they have yet to provide sustainability reporting for their own government reporting entities. This presents a major obstacle to global sustainability ambitions, particularly considering the vast physical infrastructure, non-renewable resources, rare earth elements, water and natural assets controlled by governments around the world. .

Click here to access KPMG's portal.

Fighting Modern Slavery in Canadian Supply Chain

The deadline for the first year of reporting under Canada's Fighting Forced Labour and Child Labour in Supply Chains Act (the Act) was May 31, 2024. Under the Act, eligible entities are required to publicly report on steps taken to reduce the risk of forced labour and child labour in their business and supply chain. KPMG in Canada reviewed 5,794 report submissions for the act to identify key takeaways.

Click here to access KPMG's portal.

ESG for Cities Webinar Series

Cities and municipalities play a crucial role to drive climate action and resilience measures, acting as stewards for the communities they serve – including their constituents, and public, private and non-profit organizations. With the physical impacts of climate changes – including floods, wildfires and droughts – accelerating in terms of both increased frequency and severity, city and municipal leaders are increasingly considering how they can tackle the multifaced challenge of achieving net zero greenhouse gas (GHG) emissions by 2050. KPMG in Canada's Public Sector and ESG practices completed a three-part national webinar series focusing on the journey to net zero – from strategic planning and stakeholder engagement to the implementation at the asset and operational level, and subsequent reporting obligations.

Click here to access KPMG's portal.

Appendix F: Thought leadership and insights (continued)

KPMG research shows that:

Eighty-seven percent of IT decision makers believe that technologies powered by AI should be subject to regulation.

- Of that group, 32 percent believe that regulation should come from a combination of both government and industry.
- Twenty-five percent believe that regulation should be the responsibility of an independent industry consortium.

Ninety-four percent of IT decision makers feel that firms need to focus more on corporate responsibility and ethics while developing AI solutions.

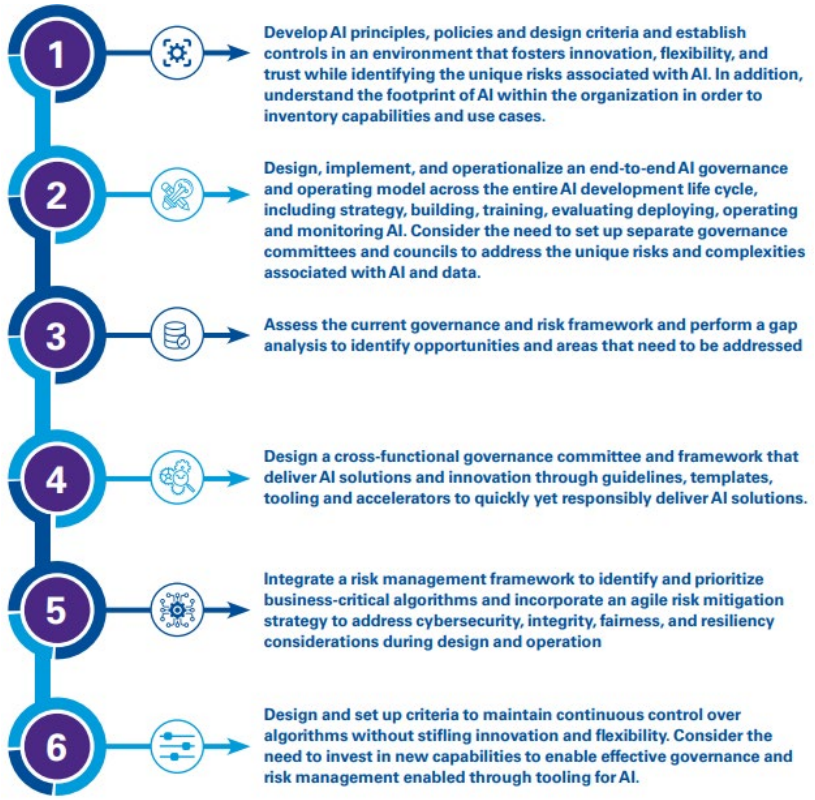
Source:

Per a study of 300 ITDMs from the UK and the US, conducted by Vanson Bourne on behalf of SnapLogic:

https://www.businesswire.com/news/home/20190326005362/en/AI-Ethics-Deficit-%E2%80%94-94-Leaders-Call

For AI solutions to be transformative, trust is imperative. This trust rests on four main anchors: integrity, explainability, fairness, and resilience. These four principles (enabled through governance) will help organizations drive greater trust, transparency, and accountability.

1. **Integrity** — algorithm integrity and data validity including lineage and appropriateness of how data is used
2. **Explainability** — transparency through understanding the algorithmic decision-making process in simple terms
3. **Fairness** — ensuring AI systems are ethical, free from bias, free from prejudice and that protected attributes are not being used
4. **Resilience** — technical robustness and compliance of your AI and its agility across platforms and resistance against bad actors



home.kpmg/ShapeofAIGovernance

Appendix F: Thought leadership and insights (continued)

Current trends in internal audit

Organizations continually face a wide spectrum of risks beyond the already complex financial and regulatory compliance risks. Many organizations are recognizing the impact and benefit of internal audit activity that is agile, properly resourced, effectively managed, and aligned with strategic priorities, which can improve risk management and control processes and drive better efficiencies.

Examples of internal audits are noted below.

Cost reduction / efficiency planning

Review the governance arrangements for the monitoring and efficiency delivery of programs / services as required. This includes considering how efficiency requirements have been apportioned and communicated to support planning.

Fraud risk management

Internal Audit assesses whether a fraud risk management framework exists and whether fraud risk assessment is performed at these levels. Internal Audit reviews the overall governance surrounding this process and review the communication and reporting protocols in place.

Staff inclusion and diversity

Assess the strategy and plan in place for inclusion and diversity amongst staff, the governance of them and the measures in place to measure achievement of the goals. Training and awareness programs are offered to staff and faculty to provide understanding of roles and responsibilities and material is updated on a regular basis.

Asset management / maintenance

Review the processes and controls in place to ensure assets are adequately managed based on an appropriate schedule.

Well being (staff)

Review processes in place to develop and promote employee wellness programs and mental health strategies for staff. Areas of focus include overall program framework, communication to faculty and staff, feedback mechanisms and management's approach to assessing the suitability of the current wellness offerings version faculty and staff needs.

Appendix G: Fraud Prevention

75%

of Canadian small and medium-sized businesses are impacted by internal or external fraud (such as credit card fraud, fraudulent cheques, false invoices, or identity fraud by hijacking bank accounts) each year.*

**based on a February 2023 KPMG in Canada survey of more than 500 small and medium-sized enterprises across Canada*

The unfortunate reality is that fraud is no longer a question of "if?" but "when?".

Organizations that effectively monitor and swiftly detect and respond to potentially damaging situations such as these are better placed to deal with them quickly and successfully, while reducing adverse financial, reputational or operational impact.

Based out of our London office, **Tyler Reavell** is a Senior Manager of KPMG in Canada's Forensic Services practice in Southwestern Ontario. With over 11 years of professional experience, Tyler assists clients in achieving and maintaining business integrity through the prevention, detection, and investigation of fraud and misconduct.

Tyler has worked with Canadian organizations of all sizes and various industry sectors. Tyler's professional experience includes fraud risk management, investigations of employee and corporate fraud for the purposes of criminal complaints, civil litigation, insurance claims and employment matters, tracing of misappropriated funds, review, design and implementation of internal controls in relation to fraud risks, business valuations for the purpose of disputes, and preparation of insurance and court-ready expert reports, for civil and criminal proceedings in Ontario.

Tyler Reavell, CPA, CA
Senior Manager, Forensic services
T: 519-660-2138
E: treavell@kpmg.ca

Tyler is the designated Forensic Risk Consulting advisor working as part of your KPMG engagement team. He will be happy to support your organization's needs for Forensic Services. You can contact Tyler directly or through your KPMG audit team.

Appendix H: Cyber for Municipalities

KPMG

Cyber for Municipalities

April 2024

Municipalities in the news

Town of Huntsville closes municipal office for 2nd day amid cybersecurity incident

Huntsville is the 2nd Ontario municipality to report hack in 3 week

Fakiha Baig · The Canadian Press · Posted: Mar 12, 2024 11:05 AM EDT

Town of Greater Napanee targeted by hackers, impact as yet unknown

By Shane Gibson • Global News

Posted January 12, 2024 6:49 pm · 1 min read

Second Ontario municipality reports cybersecurity incident within three weeks

By Fakiha Baig • The Canadian Press

Posted March 12, 2024 10:42 am · Updated March 12, 2024 11:43 am · 2 min read

Hamilton cyberattack shows municipalities need to shore up digital defences: expert

TORONTO – A recent ransomware attack that knocked out several online services in one of Ontario's largest cities has brought into sharp focus the need for municipalities to have a plan to respond to what's become an unavoidable – and increasingly sophisticated – threat, a top cybersecurity expert said.

By **Paola Loriggio** The Canadian Press

Monday, March 11, 2024 | 3 min to read

Article was updated Mar 11, 2024

NORTHERN ONTARIO | News

'It's really a coin flip': Experts weigh in on if Sudbury will recover $1.5M lost to fraud

Cyberattack cost local town $1.3M, including $290k in Bitcoin ransom

A cyberattack on the Town of St. Marys that encrypted municipal systems and stole sensitive data cost the local government roughly $1.3 million, including a $290,000 Bitcoin ransom payment made to the hackers, officials have revealed.

Galen Simmons • Stratford Beacon Herald

Published Apr 13, 2023 • Last updated Apr

Hamilton cybersecurity breach continues to paralyze city services

Public, councillors left in the dark as to nature of incident that has hampered communications, transit and payment processing

Email hack may have revealed personal information, B.C. city warns residents

WARD SOLOMON

JULY 11, 2023

Nova Scotia

Personal information 'likely stolen' in Kings County cyberattack

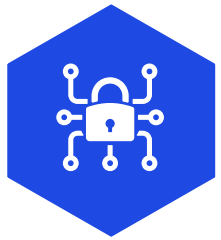
Councillors, staff and others impacted by July incident

Haley Ryan · CBC News · Posted: Aug 14, 2023 4:38 PM EDT | Last Updated: August 14, 2023

Canadian city says timeline for recovery from ransomware attack 'unknown'

The city of Hamilton, Canada, is still recovering from a ransomware attack that has affected nearly every facet of government functions.

How can a cyber attack impact you?



Organizational Disruption

Technology is a main enablement tool used in our cities, many core services rely on technology to deliver services.

When access to technology is disrupted it can have severe impacts to public services, emergency services, infrastructure and sensitive information.

Associated Costs

Cyber incidents have a variety of costs associated with recovery, which include:

- Ransom Payments
- System Restoration
- Security Upgrades
- Legal & Professional Services
- Follow-on Monitoring
- Loss of Revenue
- Financial Fraud/Theft

These costs start to balloon quickly and can have long lasting effects.

Reputational Damage & Residents Impact

A cyber incident can cause significant reputational damage to a city, leading to a loss of trust among residents and potential investors, which can indirectly impact the city's financial health. For residents, the breach of their personal information can lead to a loss of confidence in the city's ability to protect their data, potentially resulting in decreased use of city services that require personal information.

What is a cyber resilient organization?

Preparation

This involves understanding your organization's risk profile, identifying business critical assets, and developing a comprehensive cybersecurity strategy. It includes training employees on cybersecurity best practices and implementing robust security measures where possible.

Protection

This entails implementing measures to prevent cyber attacks. It includes maintaining up-to-date security software, regularly patching vulnerabilities, and controlling access to sensitive information. Protecting your organization requires cybersecurity to be a part of all business conversations.

Detection

This includes continuously monitoring systems and networks for signs of a cyber attack. It calls for the use of security tools, conducting regular security audits and making consistent updates to improve detection capabilities.

Response & Recovery

This consists of having a plan in place to respond to a cyber attack and recover from it. It is made up of incident respond planes, disaster recovery plans, and business continuity plans. These plans should be regularly tested and improved upon.

What is a cyber resilient municipality?

01

Risk Prioritization

To be a cyber resilient municipality, you must be able to prioritize your resources to address the risks that threaten you. To prioritize risks, you must understand all the risks currently facing your organization.

02

Implement the Basics

Implementing basic cyber security practices like training, maintaining security software, regularly patching and multifactor authentication can be cost effective ways to dramatically improve cybersecurity resilience.

03

Defence in Depth

This is a crucial strategy for municipalities as it reduces the risk of a single point of failure, enhances efficiency in threat detection and response, increase resilience to attacks, and provide protection against advanced cyber threats.

Steps to building cyber resilience

The following principles serve as the bedrock for establishing a continuous lifecycle that fosters cyber resilience. These principles provide a consistent framework of actions to progressively build and enhance cyber resilience.

1 – Understand Current State

To build a robust cyber resilience framework, it is imperative to start with a comprehensive understanding of your current cybersecurity status. This includes an evaluation of the protective measures already implemented, identification of critical assets, understanding the policies and procedures that regulate your operations, and an assessment of system vulnerabilities. By gaining these insights, you can make risk informed decisions that protect your organization and efficiently allocate the resources available.

4 – Increase Resilience

Increasing resilience and developing business continuity is an important part of building cyber resilience. It ensures uninterrupted business operations even in the face of cyber threats and allows organizations to quickly recover from cyber incidents, minimizing downtime and associated costs. Furthermore, a robust business continuity plan demonstrates an organization's commitment to security, which can enhance its reputation among stakeholders.

2 – Test your Technology

Testing technology is crucial for building cyber resilience as it helps identify potential vulnerabilities and weaknesses in the system that could be exploited by cyber threats. It also allows organizations to evaluate the effectiveness of their current security measures and protocols. By testing your technology, you can deepen the understanding of risks your organization faces and perform ongoing risk management. Theses tests allow for an unbiased look at your infrastructure and contribute to a proactive prevention of unauthorized users.

3 – Validate Response

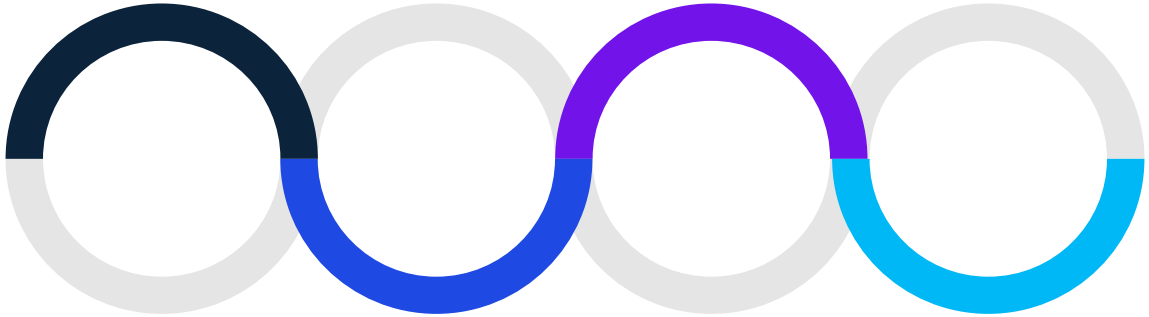
Validating response efforts is a crucial part of building cyber resilience as it ensures that the organization's incident response plan is effective and efficient. It allows for the identification of any gaps or weaknesses in the response strategy, enabling improvements to be made. Furthermore, it provides an opportunity for staff to practice and refine their skills in a controlled environment, enhancing their readiness for real cyber incidents.

Understand Current State

What should you be doing:

Identify Critical Assets

- Understanding critical systems that help the business function
- Identify the level of protection required for each asset
- Identify system interdependencies



Understand Vulnerabilities & Gaps

- Understand gaps in people, processes and technology
- Allow for proactive measures to be taken

Manage & Prioritize Efforts

- Prioritize the key gap areas, which fall outside the acceptable risk levels
- Combine efforts to tackle problems areas rather than individual problems

Obtain holistic business view

- Comprehensive perspective of all elements that present a risk
- Understand roles and responsibilities across the business for cybersecurity

How a KPMG Cyber Maturity Diagnostic (CMD) can help:

KPMG's cyber maturity diagnostic includes a critical digital asset assessment which will identify critical digital assets of the organization, which includes systems and data repositories. Additionally it will develop a high-level threat profile that focuses on threat actors, their capability, level of interest and result to the threat profile of the organization.

The CMD will leverage the framework of your choice to assess the current state of cyber security capabilities, involving a review of existing documentation and interviews with key stakeholders to identify gaps and areas for improvement.

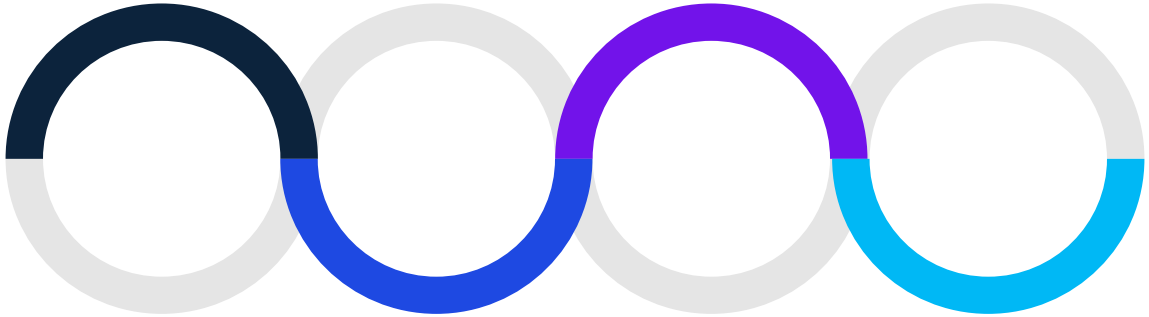
Once the assessment is complete, KPMG will produce a CMD report that includes the critical digital asset assessment and threat profile, explicit descriptions of the identified gaps and their risk level, and detailed recommendations on how to mitigate each gap. Additionally, the report will include prioritized recommendations forming a roadmap with estimated timeframes for any suggested remediation work.

Test your technology

What should you be doing:

Test your safeguards

- Test how your current technology is safeguarding your organization
- Test your monitoring and detection methods against a variety of different attack paths



Understand Vulnerabilities

- Identify weak points in your technology that could be used against you
- Use the knowledge gained to make risk informed decisions on technology

Manage & Prioritize Efforts

- Manage and prioritize efforts related to addressing critical vulnerabilities
- Allocate appropriate resources for addressing the vulnerabilities

Adjust perspective and retest

- Adjust the perspective of your testing efforts to simulate the changing threat landscape
- Retest addressed vulnerabilities to ensure that they are sufficiently mitigated

How a KPMG Penetration Testing can help:

KPMG offers a wide array of penetration testing options such as Network Penetration, Web Application, Wireless Security, Mobile Application, and Configuration Review. As organization and their technologies mature, the testing requirements tend to change and reflect the areas which require the most attention.

To build a strong foundation for understanding vulnerabilities, KPMG proposes a two phases approach to starting penetration testing which includes an external network footprint discovery exercise and a network penetration test. The network penetration test will simulated attacks both externally and internally on an organization's network infrastructure to identify vulnerabilities, assess security controls and provide recommendations for strengthen network defences.

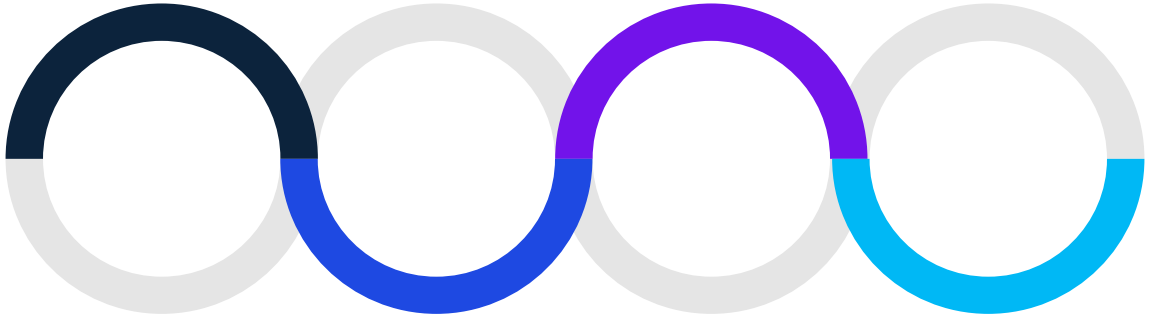
KPMG's penetration testing goes beyond traditional reporting by providing a detailed analysis of each identified vulnerability, providing the necessary evidence and proof of the vulnerability and explaining recommendations in a business context to ensure that both technical and managerial audience can understand the impact and required remediation efforts.

Validate Response

What should you be doing:

Establish Response Plan

- Establish a series of response plans that will aid the organization in responding to a variety of different threats
- Train your people on how to operate the plans and what their responsibilities are



Test & Validate Response

- Test and validate that the plan works as intended and information is accurate
- Identify gaps within your plans

Make Improvements

- Make the necessary improvements to your plan, strengthening their effectiveness
- Adapt the plans to any major changes

Adjust scenarios & retest

- Test your plans against the possible scenarios your organization may face
- Identify areas where your plans may not be able to support your team
- Test your plans again to further develop and tailor them to your organization

How a KPMG Tabletop Exercise (TTX) can help:

KPMG's tabletop exercise services take a collaborative approach to incident response testing and improvement. We will work with you to understand the specific areas your organization is looking to test and tailor an exercise to match those needs. This scenario will combine the expert knowledge of KPMG and the business expertise from your organization to create a realistic scenario.

KPMG will facilitate the exercise and gather information on how your organization responds to the cyber incident beyond just the technical aspects. KPMG will also use the exercise as an opportunity to train and educate staff on incident response processes and procedures.

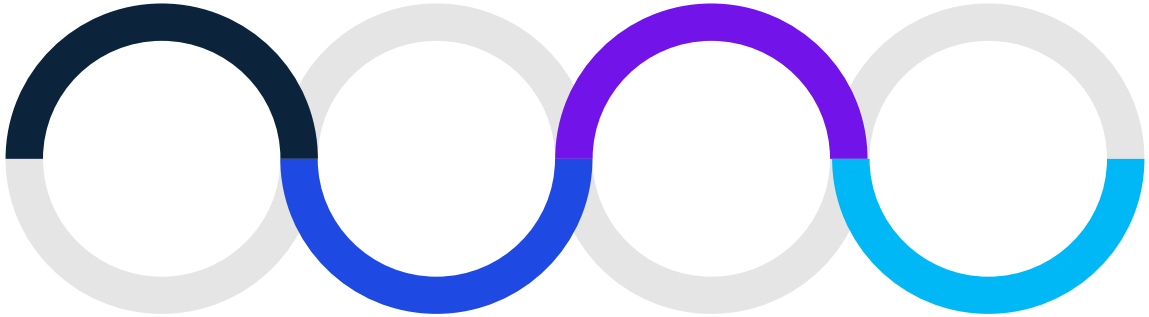
KPMG will deliver a detailed after-action report containing a summary of all findings and key recommendations, organizational strengths identified, detailed findings/gaps noted in the organizations incident response approach, detailed recommendations to address the findings/gaps, and a future tabletop exercise planning guide based on KPMG's observations to help the organization strengthen priority areas.

Increase Resilience

What should you be doing:

Business requirements and inventory

- Understand business recovery targets, resource requirements and dependencies across the organization
- Conduct business impact analysis against your critical systems



Risk assessment & remediation strategy

- Assess business continuity process risks
- Determine gaps in strategies

Plan Development

- Develop the necessary plans for the organization to operate in disruption
- Develop the necessary plans for the organization to recover from disruption

Exercising & maintaining

- Perform exercises that allow you to test the effectiveness and validity of plans
- Maintain and improve plans to mature with the growing and changing business
- Apply improvements from testing

How a KPMG Resilience Assessment can help:

KPMG's resilience assessment helps to determine what measures are currently in place at the organization and how effective they are. It will provide you with a detailed understanding of your current capabilities and what potential gaps in business information exist.

Additionally, the resilience assessment will provide the organization with a dashboard displaying the readiness of each department and how prepared they are to respond to a variety of different disruptions. The helps illustrate the types of events that departments are capable of withstand and which type of events require additional attention to achieve an acceptable level of disruption.

KPMG's resilience assessment will also produce a detailed understand and recommendations on what the businesses identified gaps are and how to remediate or mitigate them.

Pricing Options

Our goal in pricing is to provide you with the greatest possible value-for-fees. The fees below are ballpark fees and subject to change depending on scoping requires. We believe our fees are a realistic reflection of the work required, are based on the information currently available to us, and are consistent with those applied to clients of a similar size in the industry.

	Work Stream Deliverables	Total
Cyber Maturity Diagnostic	• Critical digital asset assessment and corresponding threat profile • High level cyber maturity diagnostic, containing findings, recommendations and roadmap	**$35,000**
Penetration Testing	• Detailed report with identified vulnerabilities and corresponding recommendations from the internal and external penetration tests • External attack surface discovery information	**$30,000**
Tabletop Exercise	• 3hr cyber tabletop exercise and after-action report with lessons learned, recommendations and exercise planning guide. • Value-Add session of your choice	**$30,000**
Business Resilience Assessment	• Current state assessment and department readiness dashboards • Identified gaps and recommendations report	**$25,000**
Cyber Resilience Partner Bundle ($20,000 Discount)	• Cyber maturity diagnostic, penetration test, tabletop exercise, business resilience assessment • 2 Value add sessions of your choice • Ongoing support and check-in conversations to answer any questions	**$100,000**

An experienced advisor to municipalities

KPMG in Canada and all around the world is a privileged advisor to municipal governments across our Audit, Tax and Advisory practices. We take great pride in serving the municipal sector and have highlighted here some major and relevant engagements performed for local and global Cities by our KPMG teams.

- City of Abbotsford
- City of Belleville
- City of Calgary
- City of Edmonton
- Halifax Regional Municipality
- City of Kingston
- Town of Markham
- City of Mississauga
- Regional Municipality of Peel
- City of Regina
- City of St. Albert
- City of Vaughan
- Sturgeon County
- Town of Stony Plain
- City of Brampton
- Region of York
- City of Winnipeg
- City of Hamilton
- City of Kitchener
- Ville de Montreal
- Town of Oakville
- City of Peterborough
- City of Richmond
- City of Saskatoon
- City of Toronto
- City of Spruce Grove
- Town of Banff
- Count of Wellington
- City of Lethbridge
- City of Greater Sudbury
- City of Kamloops
- Parkland County
- Town of Milton
- City of Ottawa
- City of Prince George
- City of Saint John
- City of Stratford
- Regional Municipality of Waterloo

We feel that the combination of local knowledge, our national insights on municipalities and our expert cyber knowledge make us an ideal partner for developing cyber resilience.

About KPMG cybersecurity services

Industry Leadership

"KPMG is recognized as a worldwide leader in Cybersecurity Consulting Services in the *IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment*."

Source: "IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment", January 2024, IDC #US50463423

Creating a trusted digital world together

"The breadth of offerings and deep alliance relationships, along with skilled resources and knowledge across multiple cybersecurity domains, are highly appraised by KPMG clients."

Source: "IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment", January 2024, IDC #US50463423

Vision for the future

"KPMG has a strong belief that AI will transform the way the firm delivers services to clients as well as build new products/services that is reflected in its AI innovation and investment."

Source: "IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment", January 2024, IDC #US50463423

Proven Expertise

6000+ Global Clients	9,300+ Cyber Professionals	30+ Industry Leading Alliances

Contact Us

Imraan Bashir
Partner, National Public Sector Cyber Leader
KPMG Cybersecurity

T: +1 613 212 2852
E: ibashir@kpmg.ca

LinkedIn Profile:

Luke Paron
Senior Consultant
KPMG Cybersecurity

T: +1 905 972 7468
E: lparon1@kpmg.ca

LinkedIn Profile:

kpmg.ca