Capital Regional Hospital District

Audit Planning Report

For the year ended December 31, 2017

KPMG LLP

For meeting on February 28, 2018

kpmg.ca/audit

The contacts at KPMG in connection with this report are:

Lenora Lee
Audit Engagement Partner
Tel: 250-480-3588
lenoramlee@kpmg.ca

Heather Crow
Audit Senior Manager
Tel: 250-480-3504
hcrow@kpmg.ca

Table of contents

At KPMG, we are **passionate** about earning your **trust**. We take deep **personal accountability**, individually and as a team, to deliver **exceptional service and value** in all our dealings with you.

At the end of the day, we measure our success from the **only perspective that matters – yours**.

Executive summary

Audit approach

Our audit is risk-focused. In planning our audit we have taken into account key areas of focus for financial reporting.

See pages 5 and 6

KPMG team

The KPMG team will be led by Lenora Lee, Partner. She will be supported by Heather Crow, Senior Manager. Subject matter experts will be involved to ensure our approach is appropriate and robust.

Effective communication

We are committed to transparent and thorough reporting of issues to management and the Board of Directors.

Audit Materiality

Materiality has been determined based on an estimate of total revenue. We have determined materiality to be $650,000 for the year ending December 31, 2017 (2016 - $600,000).

See page 4

Independence

We are independent and have extensive quality control and conflict checking processes in place. We provide complete transparency on all services and follow Board of Directors approved protocols.

Current developments

Please refer to Appendix 5 for relevant accounting changes relevant to the Hospital District.

Annual inquiries of the Board of Directors

Professional standards require that during the planning of our audit we obtain your views on the risk of fraud.

- Are you aware of, or have you identified any instances of, actual, suspected, possible, or alleged non-compliance of laws and regulations or fraud, including misconduct or unethical behaviour related to financial reporting or misappropriation of assets? If so, have the instances been appropriately addressed and how have they been addressed?
- What are your views about fraud risks in the entity?
- How do you provide effective oversight of programs and controls to prevent, detect and deter fraud, including oversight over internal controls management has established to mitigate fraud risks?
- Is the Board aware of tips or complaints regarding the entity's financial reporting and, if so, what are the responses to such tips and complaints?

Materiality

The determination of materiality requires professional judgment and is based on a combination of quantitative and qualitative assessments including the nature of account balances and financial statement disclosures.

The first step is the determination of the amounts used for planning purposes as follows:

Materiality determination	Comments	Amount
Metrics	Relevant metrics include revenue and expenses.	
Benchmark	Based on an estimate of revenues for the year. This benchmark is consistent with the prior year (2016 - $33.7 million).	$34.3 million
Materiality	Determined to plan and perform the audit and to evaluate the effects of identified misstatements on the audit and of any uncorrected misstatements on the financial statements. The corresponding amount for the prior year's audit was $600,000.	$650,000
% of Benchmark	The corresponding percentage for the prior year's audit was 1.7%	1.8%
Performance materiality	Used 75% of materiality, and used primarily to determine the nature, timing and extent of audit procedures. The corresponding amount for the prior year's audit was $450,000.	$487,500
Audit Misstatement Posting Threshold (AMPT)	Threshold used to accumulate misstatements identified during the audit. The corresponding amount for the previous year's audit was $30,000. Different threshold used to accumulated reclassification misstatements.	$32,500 $65,000

Professional standards require us to re-assess materiality at the completion of our audit based on period-end results or new information in order to confirm whether the amount determined for planning purposes remains appropriate. Our assessment of misstatements, if any, in amounts or disclosures at the completion of our audit will include the consideration of both quantitative and qualitative factors.

Audit approach

Inherent risk is the susceptibility of an assertion related to a significant account or disclosure to a misstatement which could be material, individually or when aggregated with other misstatements, assuming that there are no related controls.

Our assessment of inherent risk is based on various factors, including the size of the balance, its inherent complexity, the level of uncertainty in measurements, as well as significant external market factors or those particular to the internal environment of the entity.

We did not identify any areas with significant financial reporting risks. Areas of audit focus include those set out in the accompanying table. The Summit at Quadra Village Project will be an area of focus given the significance and the changing shift in operations that it represents.

Financial Statement Caption	Our audit approach
Cash and Investments	• Confirm year end balances with financial institutions • Inspect year end bank reconciliations and cut-off
Tangible Capital Assets	• Review and verify mathematical accuracy of the capital asset continuity schedule • Inspect a sample of capital asset additions including the underlying source documentation • Assess accounting treatment and policy of capital expenditures and expenditures related to Summit at Quadra Village Project • Review contracts related to Summit at Quadra Village Project • Review a sample of capital asset additions including the underlying source documentation related to Summit at Quadra Village Project
Accounts Payable	• Perform cut-off testing to determine if all expenses relating to fiscal 2017 have been recorded • Review and verify mathematical accuracy of significant accruals at year end
Long-term debt and Interest on long-term debt	• Confirm year end balances, interest paid and accrued with financial institutions • Inspect associated bylaws
Revenue	• Inspect Board approved budget for requisitions value and compare to revenue • Inspect associated bylaws • Perform substantive analytical procedures of actual to budget
Expenses	• Select a sample of expenditures, compare sample to source documentation, payment and authorization • Perform substantive analytical procedures of actual to budget

Audit approach

Professional standards presume the risk of fraudulent revenue recognition and the risk of management override of controls exist in all companies.

The risk of fraudulent revenue recognition can be rebutted, but the risk of management override of control cannot, since management is typically 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.

Professional requirements	Why	Our audit approach
Fraud risk from revenue recognition	This is a presumed fraud risk. There are generally pressures or incentives on management to commit fraudulent financial reporting through inappropriate revenue recognition when there is an expectation to maintain a balanced budget from year to year.	— Evaluation and testing controls related to recording of journal entries — Detailed review of Board approved requisitions — Detailed cut-off testing of revenues with large or unusual reconciling items — Detailed testing of journal entries at period end and subsequent to year end
Fraud risk from management override of controls	This is a presumed fraud risk. We have not identified any specific additional risks of management override relating to this audit.	As the risk 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 and evaluating the business rationale of significant unusual transactions.

Value for 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.

Our fees are estimated as follows:

	Current period - 2017 (budget)	Prior period - 2016 (actual)
Audit of the annual financial statements, base fee	$ 13,000	$ 15,200

Matters that could impact our fee

The proposed fees outlined above are based on the assumptions described in the engagement letter.
The critical assumptions, and factors that cause a change in our fees, include:

- Significant changes in the nature or size of the operations of the Hospital District beyond those contemplated in our planning processes;
- Changes in professional standards or requirements arising as a result of changes in professional standards or the interpretation thereof;
- Changes in the time of our work;
- Capital activity and related audit procedures associated with the construction of Summit at Quadra Village Project will be billed separately ($4,500 in fiscal 2016).

Audit cycle and timetable

Our key activities during the year are designed to achieve our one principal objective:

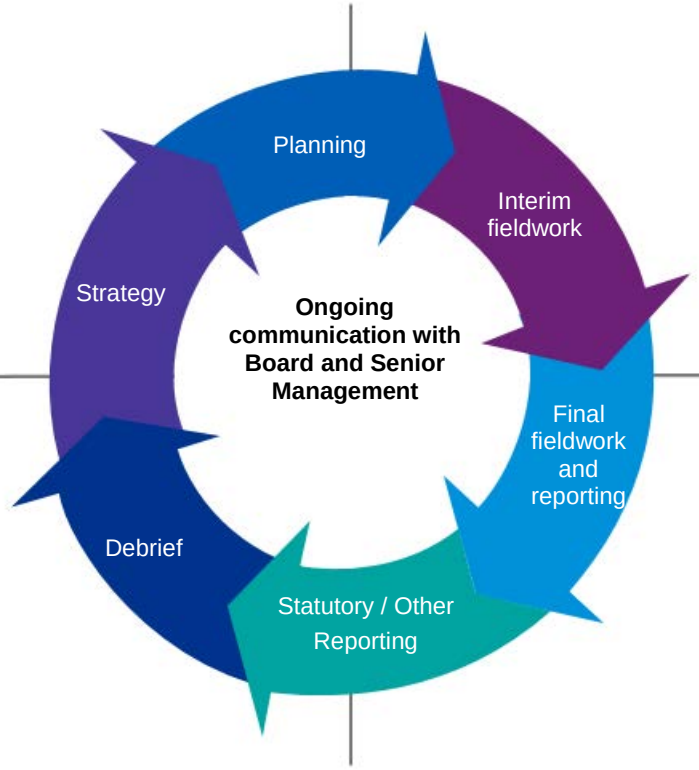
- To provide a robust audit, efficiently delivered by a high quality team focused on key issues.
- Our timeline is in line with the prior year.

Commence year end planning
November 2017

November 2017

Interim fieldwork and meet with management to debrief planning issues: November 2017

Audit plan discussion with Board of Directors February 28, 2018



November 2018

Audit strategy discussions based on debrief of audit June 2018

February 2018

Final fieldwork: starting April 2, 2018

Closing meetings: May 2018

Audit findings discussion with the Board of Directors: June 2018

Issuance of audit report on financial statements June 2018

June 2018

Appendices

Appendix 1: Audit quality and risk management

KPMG maintains a system of quality control designed to reflect our drive and determination to deliver independent, unbiased advice and opinions, and also meet the requirements of Canadian professional standards.

Quality control is fundamental to our business and is the responsibility of every partner and employee. The following diagram summarises the six key elements of our quality control systems.

Visit our Audit Quality Resources page for more information including access to our audit quality report, Audit quality: Our hands-on process.

- Other controls include:
  - Before the firm issues its audit report, Engagement Quality Control Reviewer reviews the appropriateness of key elements of publicly listed client audits.
  - Technical department and specialist resources provide real-time support to audit teams in the field.
- We conduct regular reviews of engagements and partners. Review teams are independent and the work of every audit partner is reviewed at least once every three years.
- We have policies and guidance to ensure that work performed by engagement personnel meets applicable professional standards, regulatory requirements and the firm's standards of quality.

- All KPMG partners and staff are required to act with integrity and objectivity and comply with applicable laws, regulations and professional standards at all times.
- We do not offer services that would impair our independence.
- The processes we employ to help retain and develop people include:
  - Assignment based on skills and experience;
  - Rotation of partners;
  - Performance evaluation;
  - Development and training; and
  - Appropriate supervision and coaching.
- We have policies and procedures for deciding whether to accept or continue a client relationship or to perform a specific engagement for that client.
- Existing audit relationships are reviewed annually and evaluated to identify instances where we should discontinue our professional association with the client.

Appendix 2: KPMG's audit approach and methodology

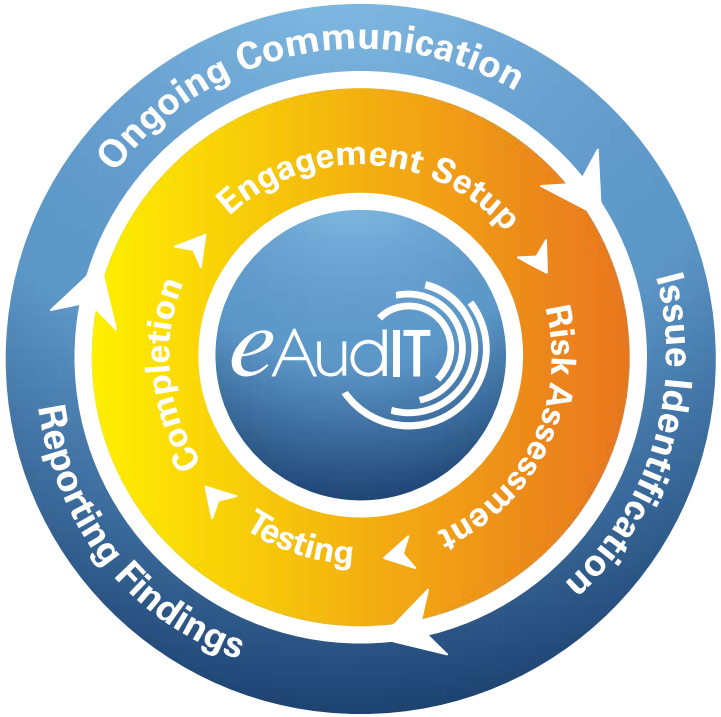
Technology-enabled audit workflow (eAudIT)

Engagement Setup

- Tailor the eAudIT workflow to your circumstances
- Access global knowledge specific to your industry
- Team selection and timetable

Completion

- Tailor the eAudIT workflow to your circumstances
- Update risk assessment
- Perform completion procedures and overall evaluation of results and financial statements
- Form and issue audit opinion on financial statements
- Obtain written representation from management
- Required Board of Director communications
- Debrief audit process



Risk Assessment

- Tailor the eAudIT workflow to your circumstances
- Understand your business and financial processes
- Identify significant risks
- Plan the use of KPMG specialists and others including auditor's external experts, management experts, internal auditors, service organizations auditors and component auditors
- Determine audit approach
- Evaluate design and implementation of internal controls (as required or considered necessary)

Testing

- Tailor the eAudIT workflow to your circumstances
- Perform tests of operating effectiveness of internal controls (as required or considered necessary)
- Perform substantive tests

Appendix 3: Required communications

In accordance with professional standards, there are a number of communications that are required during the course of and upon completion of our audit. These include:

- **Engagement letter** – the objectives of the audit, our responsibilities in carrying out our audit, as well as management's responsibilities, are set out in the engagement letter and any subsequent amendment letters as previously provided. The terms of the engagement have not changed.
- A**udit planning report** – as attached
- **Required inquiries** – professional standards require that during the planning of our audit we obtain your views on risk of fraud and other matters. We make similar inquiries to management as part of our planning process; responses to these will assist us in planning our overall audit strategy and audit approach accordingly
- **Management representation letter** – we will obtain from management certain representations at the completion of the annual audit. In accordance with professional standards, copies of the representation letter will be provided to the Board of Directors
- **Audit findings report** – at the completion of our audit, we will provide a report to the Board of Directors

Appendix 4: KPMG's Cyber Security Protocol

This summary is intended to provide management and Board of Directors members with some insight into KPMG's strategies and procedures regarding our cyber defence.

KPMG Global

KPMG Global provides managed security services for member firms which includes 24x7 monitoring and alerting services to identify potential attacks on our environment. We use a series of centrally managed firewalls among our network of member firms to identify and address potential attacks to member firms and to prevent attacks from spreading between member firms. This approach was in place during the Wanna Cry outbreak and was a critical element in our successful defence against that incident.

KPMG Global has also implemented enhanced email protection to address malware and attacks through email and we have implemented automated vulnerability detection services. This service scans equipment that is exposed to the Internet and identifies known vulnerabilities on a real-time basis. "Good housekeeping" is a central tenet of our approach and we continue to focus on known vulnerabilities and patching.

KPMG Global believes the cloud represents a secure environment when appropriately configured and monitored as a platform to deliver services. Our approach to secure the cloud includes deploying full-time, dedicated security and privacy resources, integrating the cloud platform into our managed security services to promote "good housekeeping," and deploying a continuous monitoring plan for each of the cloud platforms that we deploy to member firms and to our clients.

KPMG Global has invested heavily in enhancing the security of our environment, evidenced by the introduction of our Global Security Operations Centre, managed services and other enhancements to our cyber defence.

KPMG Canada Approach

- KPMG Canada does not currently use Office 365 or Cloud based email.
- Cloud environments provide robust security when properly configured, with proper password management.
- The Canadian firm's email servers are hosted in Canada and controlled and managed by KPMG Canada.
- In compliance with our global security controls, we enforce strong passwords that need to be renewed at regular intervals.
- We also maintain a specific IT security platform for the maintenance and management of privileged accounts.
- KPMG's Information Security Program is built on a comprehensive framework of policies, standards, and processes based on ISO 27001:2013.
- KPMG's security requirements are set out in Global Information Security Policies and Standards (GISP).
- The Canadian firm undergoes an internal audit every year to ensure compliance to key security controls in the GISP.
- Every three years, the Canadian firm goes through a Compliance Review conducted by a team from non-Canadian member firms.

Cyber Security, Is your organization at risk?

Cyber-attacks are an inevitable part of life today, and the financial and reputational costs of not being prepared against such attacks are significant. Cyber-attacks are being launched against all forms of valuable information including both financial and non-financial data sources. Estimates suggest the global financial impact of cybercrime is US$114 billion; companies are thought to bear almost 80% of those costs. The nature of these attacks and the perpetrators behind them are always changing. Hacktivists, organized criminals, competitors, and even rogue governments are mounting attacks with a high level of sophistication and persistence. These perpetrators have different motives, however are common in that they are looking to either disrupt or better themselves by stealing another entities data.

Patching servers and installing intrusion detection systems is no longer enough to protect your critical assets and business processes. Cyber Security has never been solely about IT; it has always been a business issue first. To survive and prosper requires a business-wide understanding of the threats, safeguards, and responses involved. Key elements to consider include:

- Preparing your people, processes, infrastructure and technology to resist an attack
- Detecting the attack and initiating your response
- Containing and investigating the attack
- Recovering from an attack and resuming business operations
- Reporting on and improving security

Organizations should be reviewing their organization and considering Cyber Risks. Key data that may be identified includes student, banking, payroll data etc.

Appendix 5: Current developments

Public Sector Accounting Standards

Standard	Summary and implications
Related Party Transactions and Inter-entity Transactions	— Two new Handbook sections are effective for fiscal years beginning on or after April 1, 2017. — Related parties include entities that control or are controlled by a reporting entity, entities that are under common control and entities that have shared control over or that are subject to shared control of a reporting entity. — Individuals that are members of key management personnel and close members of their family are related parties. Disclosure of key management personnel compensation arrangements, expense allowances and other similar payments routinely paid in exchange for services rendered is not required. — Determining which related party transactions to disclose is a matter of judgment based on assessment of: • the terms and conditions underlying the transactions; • the financial significance of the transactions; • the relevance of the information; and • the need for the information to enable users' understanding of the financial statements and for making comparisons. — A related party transaction, with the exception of contributed goods and services, should normally be recognized by both a provider organization and a recipient organization on a gross basis. — Related party transactions, if recognized, should be recorded at the exchange amount. A public sector entity's policy, budget practices or accountability structures may dictate that the exchange amount is the carrying amount, consideration paid or received or fair value.
Assets, Contingent Assets and Contractual Rights	— Three new Handbook sections are effective for fiscal years beginning on or after April 1, 2017. — The intended outcome of the three new Handbook Sections is improved consistency and comparability. — The standard includes enhanced guidance on the definition of assets and disclosure of assets to provide users with better information about the types of resources available to the public sector entity. — Disclosure of contingent assets and contractual rights is required to provide users with information about the nature, extent and timing of future assets and potential assets and revenues available to the public sector entity when the terms of those contracts are met.

Employee Future Benefit Obligations	— PSAB has initiated a review of sections PS3250 Retirement Benefits and PS3255 Post-Employment Benefits Given the complexity of issues involved and potential implications of any changes that may arise from this review, the project will be undertaken in phases. Phase I will address specific issues related to measurement of employment benefits. Phase II will address accounting for plans with risk sharing features, multi-employer defined benefit plans and sick leave benefits. — An Invitation to Comment was issued in November 2016 and closed March 2017, seeking guidance on whether the deferral provisions in existing public sector standards remain appropriate and justified and the appropriateness of accounting for various components of changes in the value of the accrued benefit obligation and plan assets. Responses are currently under deliberation. — An Invitation to Comment is expected to be issued in November 2017 seeking guidance on the present value measurement of accrued benefit obligations. Webinars with an overview of the Invitation to Comment are scheduled for January 2018. — The ultimate objective of this project is to issue a new employment benefits section to replace existing guidance.
Asset Retirement Obligations	— A new standard is under development addressing the recognition, measurement, presentation and disclosure of legal obligations associated with retirement of tangible capital assets in productive use. Retirement costs would be recognized as an integral cost of owning and operating tangible capital assets. PSAB currently contains no specific guidance in this area. — PSAB recently released an Exposure Draft following the consideration of comments received in response to the previously released Statement of Principles. Responses are currently under deliberation. — The proposed ARO standard would require the public sector entity to record a liability related to future costs of any legal obligations to be incurred upon retirement of any controlled tangible capital assets (“TCA”). The amount of the initial liability would be added to the historical cost of the asset and amortized over its useful life. — As a result of the proposed standard, the public sector entity would have to: • consider how the additional liability will impact net debt, as a new liability will be recognized with no corresponding increase in a financial asset; • carefully review legal agreements, senior government directives and legislation in relation to all controlled TCA to determine if any legal obligations exist with respect to asset retirements; • begin considering the potential effects on the organization as soon as possible to coordinate with resources outside the finance department to identify AROs and obtain information to estimate the value of potential AROs to avoid unexpected issues. — The Exposure Draft has a proposed effective date of April 1, 2021 for the standard.

Public Private Partnerships	— A taskforce was established in 2016 as a result of increasing use of public private partnerships for the delivery of services and provision of assets. — A Statement of Principles (SOP) was issued in August 2017 which proposes new requirements for recognizing, measuring and classifying infrastructure procured through a public private partnership. Responses are currently under deliberation. — The SOP proposes 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 P3 ends. — The SOP proposes the public sector entity recognize a liability when it needs to pay cash or non-cash consideration to the private sector partner for the infrastructure. — The infrastructure would be valued at cost, with a liability of the same amount if one exists. Cost would be measured by discounting the expected cash flows by a discount rate that reflects the time value of money and risks specific to the project.
Revenue	— PSAB is proposing a single framework to categorize revenues to enhance the consistency of revenue recognition and its measurement. — An Exposure Draft (ED) was issued in May 2017 seeking feedback from stakeholders. Responses are currently under deliberation. — The ED proposes that in the case of revenues arising from an exchange, a public sector entity must ensure the recognition of revenue aligns with the satisfaction of related performance obligations. — The ED proposes that unilateral revenues arise 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. — The new section would be applied retroactively with restatement for fiscal years beginning on or after April 1, 2021.

kpmg.ca/audit