



Toolkit for Audit Committee Guide – Canadian Edition

Sample frameworks to provide practical support to audit committee members

Contents

About the KPMG in Canada Board Leadership Centre

The KPMG Board Leadership Centre in Canada champions outstanding governance to help drive corporate values. It engages with directors and business leaders to help articulate their challenges and promote continuous improvement.

Drawing on insights from KPMG professionals and governance experts, the KPMG Board Leadership Centre delivers actionable thought leadership – on risk and strategy, talent and technology, compliance, financial reporting, audit quality, and more – all through a board lens.

As a follow-up to the [Audit Committee Guide – Canadian Edition](#), this Toolkit is an expanded collection of practical and useful frameworks providing audit committee members with examples they can consult and tailor when carrying out certain tasks as part of their audit committee oversight duties.

The appendices supplied within the guide and this supplementary toolkit are intended to provide practical support and are not a prescriptive or definitive list of frameworks available to audit committee members.



Janet Rieksts Alderman
Risk Consulting Partner,
Chair Board Leadership Centre
KPMG in Canada



Jim Newton
Audit Partner,
Financial Institutions
KPMG in Canada

Contents

Appendix 1: In-camera session with the auditor4

Appendix 2: Specimen year-end timetable.....6

Appendix 3: Example questions around identifying and assessing risk.....7

Appendix 4: Internal control and risk management..... 10

Appendix 5: Sample whistleblower policy..... 18

Appendix 6: Internal audit sourcing options.....23

Appendix 7: Sample internal audit plan25

Appendix 8: Internal audit activities – key steps in the annual audit cycle31

Appendix 9: Evaluation of the internal audit functio.....33



APPENDIX 1

In-camera session with the auditor

Most audit committees want to meet the external auditor in a private session where management is not present.

Typically there should be few items to discuss. All key matters related to financial reporting should have been reviewed in a candid and robust manner with management, the audit committee and the auditor during the audit committee meeting. The audit committee can use the private session as a follow-up for answers given at the audit committee meeting or for more open ended questions such as those listed below. The in-camera session can focus on areas where the auditor can provide additional, candid, and often confidential, comments to the audit committee on other matters. The in-camera session gives the audit committee an opportunity to explore such matters in a frank and open forum. In addition, the audit committee may have more knowledge than the auditor on other matters, and this session allows the audit committee an opportunity to talk to the auditor about them.

Overall, in-camera sessions play an important role in the development of a trusting and respectful relationship between the audit committee and the auditor. Questions often focus on one or more of the following areas:

Attitudes – management’s attitude toward financial reporting, internal controls and the external auditor.

Resources – the adequacy of people and other resources in the financial management area and the internal audit function.

Relationships – the nature of the relationship between the auditor, management and the internal auditor.

Other issues – other issues of concern to the audit committee or the auditor.

The following is a list of illustrative questions. It is not an exhaustive list but is intended to stimulate thought as to the type of issues that could be raised with the auditor. Typically, each in-camera session should address a few matters which may vary from meeting to meeting, in addition to any matters of current concern.

Attitudes

- What is your assessment of the tone from the top?
- What do you believe are the reasons management did not adjust for the uncorrected audit differences?
- Does management have plans to correct these audit differences in the future?
- Was management fully supportive of the corrected audit differences?
- What is your assessment of the quality of the company’s financial reporting, narrative reporting, and press releases?
- How does this company’s approach to financial reporting compare to other companies in the industry?
- Is there excessive pressure on management or operating personnel to meet financial targets including sales or profitability incentive goals?
- Is there excessive pressure to meet unrealistic or aggressive profitability expectations by investment analysts or others?
- What is your assessment of management’s approach to disclosure controls and internal control over financial reporting?

Resources

- Do the finance and internal audit functions have the appropriate number of people?
 - Do they have a sufficiently broad range of knowledge and experience to be able to deal with the types of transactions faced by the company?
 - Has management adequately responded to any recommendations?
 - Are there other areas where internal audit should focus its activities?
 - If the company does not have an internal audit function, what is your assessment of the need to have one?
-

Relationships

- Did you receive full cooperation during the audit and did you get full, candid answers to all questions that were asked?
 - Was management forthcoming, open and candid in discussions with you?
 - How are your relationships with financial management personnel? Internal audit? CEO? CFO?
 - What was the nature of any consultations that were held with other accountants or auditors?
-

Other issues

- Did you receive everything you requested on a timely basis?
 - Did you have adequate time to carry out all your audit procedures?
 - Is the audit fee at an appropriate level?
 - On what issues was the most amount of audit time spent?
 - What is the most complex issue that was encountered during the audit that has not been discussed at the audit committee meeting?
 - What were the two or three issues that you spent the most amount of time discussing with management?
-

APPENDIX 2

Specimen year-end timetable

Year-end reporting timetables will vary for a variety of reasons. The timetable illustrated below is typical for a company with a December year-end.

Year end	31 December
Management prepares draft financial statements	By mid January
Financial statements audited by external auditor (fieldwork)	Mid January to mid February
Meeting with CFO to discuss audit findings and draft audit findings report for the Audit Committee	End of 2nd week in February
Audit committee papers circulated (including the draft financial statements and management and auditors comments thereon)	Beginning of 3rd week in February
Meeting between audit committee chair and audit partner to discuss findings in advance of the meeting	End of 3rd week in February
Audit committee meeting to: Review and recommend approval of the annual report (including the financial statements) and preliminary announcement (and analyst presentation) Review representation letters from CEO, CFO, etc.	Beginning of 4th week in February
Board meeting to approve the annual report (including the financial statements), preliminary announcement and analyst presentation	Beginning of 4th week in February



APPENDIX 3

Example questions around identifying and assessing risk

In view of the different approaches boards may take in assigning responsibilities to the audit committee in respect of risk management and the control framework, it is vital that there is an unambiguous understanding of what the board of directors, other board committees and the audit committee are responsible for in this important area of corporate governance. The audit committee's responsibilities should be reflected in its charter.

So as to meet its responsibilities under its terms of reference, the audit committee needs to assess whether it is getting appropriate risk management information regularly enough and in a format that meets the needs of members. It needs to evaluate at least annually the adequacy and timeliness of management reporting to the committee on financial, non-financial, current and emerging risk trends.

The audit committee needs also to discuss risk management with senior executives, internal and external audit. The scope of those discussions should have reference to the audit committee charter.

The following are high-level questions the audit committee may like to consider in framing discussions with management. The list is not exhaustive and will require tailoring based on the audit committee's terms of reference as well as the particular circumstances of the organization.

Risk management framework	Evaluation of risk management framework
<p>Risk strategy</p> <p>the approach for associating and managing risks based on the organization's strategies and objectives.</p>	<ul style="list-style-type: none"> – What are the risks inherent in our business strategies and objectives? – How is our risk strategy linked to our business strategy? – Is our risk management policy clearly articulated and communicated to the organization? If not, why not? If yes, how has this been achieved? – Is our risk appetite (the amount of risk the organization is willing to take) clear? how is it linked to our objectives? – How has the board's perspective on risk permeated the organization and culture?
<p>Risk structure</p> <p>the approach for supporting and embedding the risk strategy and accountability.</p>	<ul style="list-style-type: none"> – Is there a common risk management language/terminology across the organization? If not, why not? – Is accountability for risk management transparent at the management level? If not, why not? If yes, describe how this has been achieved. – Are risk management activities/responsibilities included in job descriptions? – How do our performance management and incentive systems link to our risk management practices?
<p>Measuring and monitoring</p> <p>the establishment of Key Performance Indicators (KPIs) and continuous measuring and improving of performance.</p>	<ul style="list-style-type: none"> – Are risk owners clearly identified? If not, why not. If yes, how? – Are there systems in place for measuring and monitoring risk? – How are risks, including suspected improprieties, escalated to the appropriate levels within the organization? – How is the risk management framework linked to the organization's overall assurance framework?
<p>Portfolio</p> <p>the process for identifying, assessing and categorizing risks across the organization.</p>	<p>Risk Profile</p> <ul style="list-style-type: none"> – Does a comprehensive risk profile exist for the organization? If not, why not? – Does the risk profile evidence identification and evaluation of non- traditional risk exposures? – Are the interrelationships of risks clearly identified and understood? <p>Operational Risk</p> <ul style="list-style-type: none"> – What are the risks inherent in the processes chosen to implement the strategies? – How does the organization identify, quantify and manage these risks given its appetite for risk? – How does the organization adapt its activities as strategies and processes change? <p>Reputation Risk</p> <ul style="list-style-type: none"> – What are the risks to brand and reputation inherent in the way the organization executes its strategies? – Work with members to ensure committee papers, access to management and other information flows are appropriate

Risk management framework	Evaluation of risk management framework
<p>Portfolio</p> <p>the process for identifying, assessing and categorizing risks across the organization.</p>	<p>Regulatory or Contractual Risk</p> <ul style="list-style-type: none"> – Which financial and non financial risks are related to compliance with regulations or contractual arrangements? <p>Financial Risk</p> <ul style="list-style-type: none"> – Have operating processes put financial resources at undue risk? – Has the organization incurred unreasonable liabilities to support operating processes? – Has the organization succeeded in meeting measurable business objectives? <p>Information Technology Risk</p> <ul style="list-style-type: none"> – Is our data/information/knowledge reliable, relevant and timely? – Are our information systems reliable? – Do our security systems reflect our reliance on technology? – Is there adequate cyber security for the size and complexity of our organization? <p>ESG Risks</p> <ul style="list-style-type: none"> – Are risks to achieving our ESG goals identified and monitored? – Is ESG risk management integrated throughout our business processes? – What are the responsibilities for ESG risk identification and management? <p>New Risks</p> <ul style="list-style-type: none"> – In a business environment that is constantly changing, are there processes in place to identify emerging risks? If not, why not? If yes, describe. – What risks have yet to develop? These might include risks from new competitors or emerging business models, recession risks, relationship risks, outsourcing risks, political or criminal risks, financial risk disasters such as rogue traders, and other crisis and disaster risks including climate and pandemic risk.
<p>Optimization</p> <p>balancing potential risks and opportunities based on the appetite to accept risk.</p>	<ul style="list-style-type: none"> – Does the risk approach include a regular search for new markets, partnering opportunities and other risk optimization strategies? If not, why not? If yes, how is this achieved? – Is risk a priority consideration whenever business processes are improved? If not, why not? If yes, describe how this is achieved.



APPENDIX 4

Internal control and risk management

Audit committees should critically review the design of the internal control and risk management systems related to financial reporting of the company at least annually, including the relevant documentation and disclosures. The checklist provided below aims to assist audit committees to fulfil this role.

The information below is largely extracted from the Internal Control - Integrated Framework 2013, published by the Committee of Sponsoring organizations of the Treadway Commission (CoSo). It includes the framework's principles for effective internal control and the information that is expected to be provided as part of the board of directors' description of internal control and risk management systems related to financial reporting to the extent that it is relevant to the entity. In all instances, the description provided should be adapted to the nature and complexity of the entity, its operations and its risk profile.

The COSO framework contains three categories of objectives:

- 1. Operations objectives** – related to the effectiveness and efficiency of the entity's operations, including operational and financial performance goals and safeguarding assets against loss.
- 2. Reporting objectives** – related to internal and external financial and non-financial reporting to stakeholders, which would encompass reliability, timeliness, transparency or other terms as established by regulators, standard setters or the entity's policies.
- 3. Compliance objectives** – related to adhering to laws and regulations that the entity must follow.

CONTROL ENVIRONMENT

Principles

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors and the audit committee demonstrate independence from management and exercise oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Integrity and Ethical Values

Background

Areas that relate directly to reliability of financial statement preparation include the following:

- Management's attitude toward bypassing established control procedures aimed principally at achieving financial reporting objectives.
- Management's interactions with internal and external auditors and outside counsel on financial reporting matters, such as the extent to which management provides full disclosure of information on matters that may have an adverse impact on the financial statements.
- Management's integrity in preparing financial statements (addressed further under 'Management's Philosophy and operating Style').

Information expected

- Existence and implementation of codes of conduct and other policies regarding acceptable business practice, conflicts of interest, or expected standards of ethical and moral behaviour.
- Remedial action taken in response to departures from approved policies and procedures or violations of the code of conduct. Extent to which remedial action is communicated or otherwise becomes known throughout the entity.
- Management's attitude towards intervention or overriding established controls.
- Approach to balancing performance-based compensation and short-term vs. long-term performance targets and extent to which compensation is based on achieving short term results.

Commitment to Competence

Background

Reliability of an enterprise's financial statements can be compromised if incompetent or unassertive people are involved in the financial reporting process. Directly affecting reliability of financial statements are the knowledge and skills of personnel involved in the preparation process relative to the nature and scope of operating and financial reporting issues, and whether such knowledge and skills are sufficient to properly account for any new activities, products and services, or existing ones in the face of downsizing.

Information expected

- Formal or informal job descriptions or other means of defining tasks that comprise particular jobs; announcements of job descriptions within the company.
- Process to analyze the knowledge and skills needed to perform jobs adequately.
- Hiring and performance evaluation policies and procedures.
- Process to determine segregation of responsibilities between the board and executive management.

Management's Philosophy and Operating Style

Background

The delegation of authority for financial reporting is important in achieving the entity's financial reporting objectives, in particular for making the accounting judgements and estimates that enter into financial reporting. Related issues include reasonableness of accounting policies and estimates in connection with preparation of financial statements, especially whether management's estimates and policies are conservative or aggressive (that is, on the boundary of 'reasonableness'). Management's attitude toward financial reporting also affects the entity's ability to achieve its financial reporting objectives.

Information expected

- Nature of business risks accepted, e.g. whether management often enters into particularly high-risk ventures, or is extremely conservative in accepting risks.
- Process to establish values and strategy of the organization.
- Frequency of interaction between senior management and operating management, including geographically removed locations.
- Roles and responsibilities in the selection of accounting principles including management attitude towards financial reporting e.g. selection of conservative versus liberal accounting policies.
- Establishment of a financial accounting principles and procedures manual (including e.g. time tables, execution and control of financial tasks).
- Adequate resources to implement the financial and accounting function(s) in view of adequate financial reporting process.

Organizational Structure

Background

Aspects of an entity's organizational structure that are specifically related to financial reporting objectives include factors related to accounting personnel, such as:

- Appropriateness of reporting lines;
- Adequacy of staffing and experience levels;
- Clarity of delegation of authority and duties;
- Extent to which the organizational structure allows accounting personnel to interact with other departments and activities in the organization, to have access to key data and to properly account for resulting conclusions.

Information expected

- Organizational structure, flows of information to manage activities.
- Reporting relationships.
- Process to define key managers' responsibilities, and their understanding of these responsibilities.
- Process to ensure adequacy of knowledge and experience of key managers in light of responsibilities.

Assignment of Authority and Responsibility

Background

Deficiencies in the way that authority and responsibility are assigned to employees in accounting, custodial and asset management functions may affect the entity's ability to achieve its financial reporting objectives. Matters to consider include the adequacy of the work force and whether employees are deployed to promote segregation of incompatible duties.

Information expected

- Process to assign responsibility and delegate authority to deal with organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes.
- Existence of control-related standards and procedures, including employee job descriptions.

Human Resource Policies and Practices

Background

An entity's ability to achieve its financial reporting objectives may reflect its recruiting, training, promotion, retention and compensation policies and procedures insofar as they affect performance of accounting personnel and employees outside of the accounting function who administer controls over financial reporting.

Information expected

- Appropriate number of people, particularly with respect to data processing and accounting functions, with the requisite skill levels relative to the size of the entity and nature and complexity of activities and systems.
- Extent to which people are made aware of their responsibilities and expectations of them.
- Appropriateness of remedial action taken in response to departures from approved policies and procedures.
- Extent to which personnel policies address adherence to appropriate ethical and moral standards.
- Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g. performance evaluations) and relation to the code of conduct or other behavioral guidelines

Board of Directors and Audit Committee

Background

Key aspects of the control environment are the composition and independence of the board and its audit committee and how its members fulfil responsibilities related to the financial reporting process. of particular interest for controls over financial reporting is the involvement of the board or audit committee in overseeing the financial reporting process, including assessing the reasonableness of management's accounting judgements and estimates and reviewing key filings with regulatory agencies. other committees of the board often are not a key part of controls over financial reporting.

Information expected

- Independence from management.
- Knowledge and experience of directors.
- Process to establish and publish the terms of reference of the Board and committees.
- Process to establish an audit committee and an internal function (or determine the need of).
- Frequency with which meetings are held with chief financial and/or accounting officers, internal auditors and external auditors.
- Process for informing the board of significant issues timely.
- Process to inform the board or audit committee of sensitive information, investigations and improper acts timely.
- oversight in determining the compensation of executive officers and head of internal audit, and the appointment and termination of those individuals.
- Role in establishing the appropriate 'tone at the top.'
- Actions the board or committee takes as a result of its findings, including special investigations as needed.

RISK ASSESSMENT

Principles

1. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
2. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
3. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
4. The organization identifies and assesses changes that could significantly impact the system of internal control.

Background

Are entity-wide objectives and supporting activity-level objectives established and linked? Are the internal and external risks that influence the success or failure of the achievement of the objectives identified and assessed? Are mechanisms in place to identify changes affecting the entity's ability to achieve its objectives? Are policies and procedures modified as needed?

Information expected

- Process to develop entity-wide objectives, that provide sufficient guidance on what the entity desires to achieve including the identification of objectives that are important (critical success factors) to achievement of entity-wide objectives.
- Establishment of formal risk management procedures.
- Process to communicate the entity-wide objectives and risk policy to employees and board of directors.
- Process to identify and mobilize adequate resources relative to objectives and risk management.
- Mechanisms to identify risks (e.g. strategic, reputation, compliance, financial, IT and HR risks) arising from external and internal sources.
- Establishment of a risk map or chart for all external and internal risks.
- Risk analysis process, including estimating the significance of risks, assessing the likelihood of their occurring and determining needed actions.
- Mechanisms to anticipate, identify and react to routine events or activities that affect achievement of entity or activity-level objectives and related risks.
- Mechanisms to identify and react to changes that can have a more dramatic and pervasive effect on the entity, and may demand the attention of top management
- Process to implement the same risk management language and culture through the company.
- Process to communicate risk analyses results amongst Board, audit committee and risk responsible and external parties (e.g. financial reporting compliance).
- Setting of acceptable risk appetite and tolerance level.
- Implementation of a crisis management plan.
- Process to ensure changes, if required, to the existing risk management procedures.
- Process to evaluate and continuously improve the risk management system.

CONTROL ACTIVITIES

Principles

1. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
2. The organization selects and develops general control activities over technology to support the achievement of objectives.
3. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Background

Are control activities in place to ensure adherence to established policy and the carrying out of actions to address the related risks? Are there appropriate control activities for each of the entity's activities?

Information expected

- Existence of appropriate policies and procedures necessary with respect to each of the entity's activities.
- Process in place to ensure that identified control activities in place are being applied properly.
- Existence of appropriate policies and procedures necessary with respect to the implementation and follow up of the financial manual.
- Process in place to ensure that identified key control activities are in place related to the financial and accounting process (including consolidation topics).

Information and communication

1. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
2. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
3. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Background

Are information systems in place to identify and capture pertinent information—financial and nonfinancial, relating to external and internal events – and bring it to personnel in a form that enables them to carry out their responsibilities? Does communication of relevant information take place? Is it clear with respect to expectations and responsibilities of individuals and groups, and reporting of results? And does communication occur down, across and upward in the entity, as well as between the entity and other parties?

Information expected

- Process to obtain external and internal information, and provide management with necessary reports on the entity's performance relative to established objectives.
- Process and allocation of responsibilities for the development of a strategic plan for information systems that is linked to the entity's overall strategy and responsive to achieving the entity-wide and activity-level objectives.
- Approach to ensuring completeness, sufficiency and timeliness of information to enable people to discharge their responsibilities effectively.
- Process to communicate employees' duties and control responsibilities.
- Existence of channels of communication for people to report suspected improprieties.
- Process in place for a timely and appropriate follow-up by management resulting from communications received from customers, vendors, regulators or other external parties.
- Existence of a whistle-blowing policy and procedure.
- Existence of information systems and procedures in order to meet the criteria for relevant, timely and adequate financial information and reporting.

MONITORING

Principles

1. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
2. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Background

Are appropriate procedures in place to monitor on an ongoing basis, or to periodically evaluate the functioning of the other components of internal control? Are deficiencies reported to the right people? Are policies and procedures modified as needed?

Information expected

- Existence of a mechanism by which communications from external parties is used to corroborate internally generated information, or indicate problems.
- Existence of a process to compare amounts recorded by the accounting system with physical assets.
- Scope and frequency of evaluation of the internal control system.
- Process for capturing and reporting identified internal control deficiencies and ensuring appropriate follow-up actions including reporting to the Audit Committee if significant.
- Existence of procedures with respect to periodic publication of financial information.
- Existence of a process for management and/or employees to confirm compliance with the entity's code of conduct regularly.
- Key characteristics of the internal audit department:
 - Competence and experience;
 - Position within the organization;
 - Access to the board of directors or audit committee;
 - Process to define scope, responsibilities and audit plans in function of the organization's needs.

APPENDIX 5

Sample whistleblower policy

Source: Osler, Hoskin & Harcourt LL

Provided by Osler, Hoskin & Harcourt LLP and reprinted with permission. Materials do not constitute legal or other professional advice. Specific advice should be sought for use in connection with your circumstances.

I. PURPOSE AND APPLICATION

The **[Code of Conduct and Business Ethics]** (the **"Code"**) for [Corporation] and its subsidiaries (collectively the **"Company"**) requires directors, officers, employees and independent contractors and agents that represent the Company (**"Company Personnel"**) to observe high standards of business and personal ethics in the conduct of their duties and responsibilities, and to carry them out honestly, with integrity and in accordance with all applicable laws and regulations. however, it is still possible that intentional and unintentional violations of the Code, applicable laws and applicable audit practices and accounting standards and practices may occur. when these violations do occur, the Company has a responsibility to investigate and, where appropriate, to report, these violations and the actions that the Company has taken to address them.

This policy sets out the procedures for Company Personnel to report violations, or potential or suspected violations, of the Code, applicable laws and applicable audit practices and accounting standards and practices and other matters, as outlined below.

Company Personnel are expected to talk to managers, department or business heads or other appropriate personnel about their concerns involving illegal or unethical behavior and the best course of action to take. Company Personnel can also submit confidential and/or anonymous reports or complaints of Code violations as set out below.

II. WHAT IS A REPORTABLE CONDUCT?

Company Personnel may make reports (“**Reports**”) under this Policy relating to good faith concerns about any actual, potential or suspected violation of the Code or applicable laws, including any accounting or auditing matter which is believed to be in violation of the Code or applicable law, including:

- fraud or deliberate error in the preparation, evaluation, review or audit of any financial statements of the Company;
- fraud or deliberate error in the recording or maintaining of financial records of the Company;
- deficiencies in, or non-compliance with, the Company’s system of internal controls;
- misrepresentations or false statements to or by a senior officer or accountant regarding a matter contained in the financial records, financial reports or audit reports of the Company;
- deviations from full and fair reporting of the Company’s financial condition;
- any matter that involves a significant threat to the health and safe of other Company Personnel and/or the general public;
- any other actual, potential or suspected violations of the Code or applicable laws;
- any circumstance where Company Personnel believes that he or she is being asked to commit a wrongdoing. (together, “**Reportable Matters**”).

III. HOW DO I MAKE A REPORT?

A. General

Reports made under this Policy must be made truthfully and in good faith and they should describe the Reportable Matter in as much detail as possible, including dates, individuals or witnesses involved and any supporting material or evidence that may be relevant to the Reportable Matter.

Company Personnel may make Reports to the General Counsel of **[Corporation]** (the “**Confidential Designee**”).

Reports should be addressed to the General Counsel at **[Address]** and marked “Confidential.” Reports may also be submitted by email.

Prior to making any Report, Company Personnel should, wherever possible, discuss the Reportable Matter with their manager, department or business head or other appropriate personnel who may be able to help resolve the matter. However, where the Reportable Matter continues to be unresolved following such discussion, where it is not possible for Company Personnel with their manager, department or business head or other appropriate personnel or where Company Personnel are uncomfortable doing so, or where the Reportable Matter is time sensitive, Company Personnel should submit a Report to the Confidential Designee.

B. Anonymous Reports

Reports may be made on an anonymous basis to the Confidential Designee or as described below. Although all reasonable steps will be taken by the Company to maintain anonymity of a person who makes a Report on an anonymous basis, the source or nature of the Report, or the steps required to be taken to investigate the Report, may as a practical matter make it difficult or impossible to maintain such anonymity.

This Policy also allows Company Personnel to submit anonymous Reports through **[Hotline Provider]**, a confidential third party reporting service retained by the Company, by any of the methods set forth below:

By Phone: [phone number] A qualified agent will be available 365 days-a-year, 24 hours-a-day. This person will take the information without asking for the name or personal information of the Company Personnel making the Report.

In Writing Online: [email address] which is a secure web application that asks general questions about the Reportable Matter, also without asking for the name or personal information of the Company Personnel making the Report.

In both cases, the confidential report, not including any names, will be forwarded to a designate in the Company's legal department in a secure environment for further action.

IV. RECEIPT OF REPORTS BY OTHERS

All Reports received by the Confidential Designee will be reviewed promptly and if the Report relates to a questionable accounting or audit matter or if the Confidential Designee otherwise determines that it is required by the nature of the Report, the Report will immediately be brought to the attention, and reviewed under the direction, of the Chair of the Audit Committee and, if appropriate, the Chief Executive officer and the Chief Financial officer (the **"Executive Leadership Team"**). The General Counsel will ensure that the appropriate Audit Committee members and the Executive Leadership Team are kept informed on all situations involving actual or suspected fraudulent activity unless the subject matter of the Report requires otherwise.

The General Counsel will maintain a log of all complaints or reports that are received, tracking their receipt, investigation and resolution. The General Counsel will also report complaints received and investigated under this Policy to the Audit Committee on a quarterly basis. Records pertaining to a Report about a Reportable Matter are the property of the Company and will be retained in accordance with the Company's record retention policies.

V. TREATMENT AND INVESTIGATION OF REPORTS

A. Confidentiality

All Reports will be treated as confidential, whether or not made anonymously, and Reports will only be accessible to people that the Confidential Designee, the Executive Leadership Team or the Chair of the Audit Committee determine have a "need to know": ordinarily, a need to know arises from an obligation to investigate or to take remedial or disciplinary action on the basis of the information contained in the Report. For clarity, sharing information about a Report in a manner required by this Policy will not be considered a breach of confidentiality.

The Confidential Designee may delegate the responsibilities under this Policy to another member of the legal team and for the purpose of this Policy the reference to Confidential Designee means the General Counsel or his/her delegate.

Unless the Report has been made on an anonymous basis, the Confidential Designee will advise the person who made the Report when the Report has been received by the Confidential Designee and when the investigation (if any) has been completed.

The Confidential Designee is responsible for assessing and evaluating Reports and for conducting or coordinating the conduct of investigations. In determining whether a Report should be investigated and the extent of investigation to be made in respect of a Report, the Confidential Designee, in consultation with the Executive Leadership Team and the Chair of the Audit Committee if the Confidential Designee determines it is appropriate, will consider whether the facts asserted allege a violation of the Code, applicable law or other Company policy together with the following factors, among others:

- who is the alleged wrongdoer?
- what is the nature of the alleged wrongdoing?
- how serious is the alleged wrongdoing?

Reports relating to questionable accounting or audit matters, fraud or those of a criminal nature shall be brought by the Confidential Designee to the Executive Leadership Team and the Audit Committee to determine the appropriate investigation process and participants in the investigation.

In certain cases, the Confidential Designee, in consultation with the legal group, may determine that a report should be made to the police or other law enforcement or regulatory agency where it appears that illegal activity or a regulatory breach has or may have occurred.

At any time during the investigation of a Report, the Confidential Designee in consultation with the legal group may determine that it is appropriate to notify the Company's outside auditors about the submission of the Report or about the progress of the investigation, and may provide sufficient detail to allow for appropriate consideration by such parties without compromising the confidential or anonymous nature of the Report.

During the investigation of a Report, the Company Personnel who are the subject of an investigation may be placed on an administrative leave when determined by the legal group to be appropriate and such a leave is not to be interpreted as an accusation or a conclusion of guilt or innocence of any individual, including the person on leave. Company Personnel who are informed that they are the subject of an investigation or inquiry relating to a Report will be informed of the completion of the investigation or inquiry. Any Company Personnel who are investigated will be given an opportunity to be heard prior to the taking of any disciplinary action against them.

At the conclusion of any investigation or inquiry relating to a Report, the Confidential Designee, in consultation with the legal group shall promptly inform the Chair of the Audit Committee of any proposed remedial action in a written letter. The Chair of the Audit Committee will make a recommendation to the Board of Directors if appropriate in the circumstances.

The Company Personnel who made the Report will not be advised of the results of the investigation or inquiry (if any) unless the General Counsel, the Executive Leadership Team or the Audit Committee determines otherwise.

Records pertaining to a Report about a Reportable Matter are the property of the Company and will be retained in accordance with the Company's record retention policies.

All Company Personnel have an obligation to cooperate and comply with any investigation or inquiry initiated by the Confidential Designee pursuant to this Policy as set out in the Code.

VI. PROTECTION OF WHISTLEBLOWERS

The Company will not permit any form of reprisals (including discharge, demotion, suspension, threats, harassment or any other form of discrimination) by any person or group, directly or indirectly, against any Company Personnel who, truthfully and in good faith:

- reported a Reportable Matter;
- lawfully provided information or assistance in an investigation regarding any conduct which the Company Personnel reasonably believes constitutes a violation of applicable securities laws or applicable federal laws relating to fraud against the Company's securityholders;
- filed, caused to be filed, testified, participated in or otherwise assisted in a proceeding related to a violation of applicable securities laws or applicable federal laws relating to fraud against the Company's securityholders;
- provided a law enforcement officer with truthful information regarding the commission or possible commission of an offence, unless the individual reporting is one of the violators; or
- provided assistance to the Confidential Designee, the Audit Committee, management or any other person or group in the investigation of a Report.

Any retaliation against a Company Personnel who has, truthfully and in good faith, made a Report about a Reportable Matter in accordance with this Policy or taken such an action is subject to disciplinary action, which may include dismissal.

Company Personnel should never have any fears about raising concerns truthfully and in good faith based on their reasonable beliefs, even if they are later found to be mistaken. Speaking up is a behaviour to be encouraged. However, the Company believes it is also important to make sure that representatives are protected from accusations that are frivolous or malicious, such as allegations made in bad faith or to pursue a personal grudge, and making any such accusations is a violation of the Code.

The Confidential Designee, the Audit Committee and any persons involved in or retained to assist in an investigation of a Report must take all reasonable steps to not reveal the identity of any person who reports a Reportable Matter anonymously, unless required to do so by law.

VII. QUESTIONS

Any questions concerning this Policy should be directed to the Legal & Compliance Department.

Dated this • day of •, 20 •

APPENDIX 6

Internal audit sourcing options

The relative strengths and weaknesses of different sourcing models are captured below.

Sourcing model	Pros	Cons
In-house function	✓ Continuity of staff	✗ May not be fully employed effectively and efficiently
	✓ Certain and controllable cost	✗ Difficult to acquire necessary/maintain all skills and experience to meet the risk profile of the business
	Full control of the function	need to continually invest in training and development
	✓ A resource pool for the business	✗ Recruitment hassles
	✓ Training ground for employees	✗ Ineffective/inefficient start up
	Greater cultural alignment	Retention and development strategies required
	✓ Insiders	✗ Reduces opportunity to provide fresh perspective/risk of complacency or familiarity

Sourcing model	Pros	Cons
Co-source	✓ Long term permanent onsite presence through heads of Internal Audit	✗ Time taken to recruit heads of Internal Audit (hIA)
	✓ Access to broad range of skills through the partner	✗ Possible cost impact
	✓ Draw on specialist skills as and when, and only when needed	✗ Management resource needed in recruitment and relationship development
	✓ Continuity through hIA	✗ Dependency on 3rd party
	✓ Pull in up to date skills and experience as needed	✗ Possible lack of staff continuity
	✓ Quick to implement	✗ other challenges for in house resource as above
	✓ Skills transfer to in house team	
	✓ Flexible approach, clearly defined service level and KPI measures	
	✓ Credibility to third parties	
	✓ no or reduced training cost	

Sourcing model	Pros	Cons
Full outsource	✓ Established methodologies & benefit of refreshment based on experiences across different organizations	✗ no permanent on-site resource to help other areas of the business
	✓ up to date, skilled staff	✗ Potential cost impact
	✓ Ability to draw on a wide range of skills as and when required	✗ Possible lack of staff continuity
	✓ no time taken up by managing service and resources	✗ Remote from business developments, the culture and politics
	✓ Clearly defined service level and performance measures	✗ Management time to establish and maintain relationships
	✓ Easily established and quickly effective	✗ other challenges for in house resource as above
	✓ Credibility to third parties	
	✓ Ability to manage costs by avoiding non-productive periods	

APPENDIX 7

Sample internal audit plan

Internal audit provides independent, objective assurance over an organization's risk management, internal control, governance and the processes in place for ensuring the effectiveness and efficiency of operations and compliance.

Each audit plan will be different and tailored to the organization's needs. However, there are common elements that the audit committee should expect to see when reviewing the audit plan, although in practice these elements might be presented in many different ways. These elements are discussed below.

Overview of the audit approach

The audit committee should expect the audit planning document to set out that the audit plan has been developed by:

- taking account of the risks identified by the organization in its risk register and other documents such as strategic and business plans, key projects and past years' audit plans and results;
- using the internal auditor's experience of the organization and the sector more generally to identify other areas of risk which may warrant attention; and
- discussing all identified risks and other relevant issues with the organization's management to identify the potential scope of internal audit
- discussion and input from the Audit Committee

Risk-based internal audit coverage

Where the organization's risk management program allocates each risk a likelihood and impact rating between 'high' and 'low', the audit plan might for example focus on 'high' and 'medium' priority risks over, for example, a one or two-year period and low priority risks over a longer term period. The audit committee should be fully informed of:

- which areas are being addressed;
- how many audit hours have been allocated to each area;
- when the fieldwork is being undertaken; and
- when the internal auditors will report their findings.

Exhibit 1 (below) illustrates which risks identified by the organization in the risk register are addressed by the internal audit plan. Exhibit 2 puts these risks in the context of a three-year audit plan. It is also useful to keep the audit committee apprised of the risks that are not addressed by the internal audit plan – see Exhibit 3.

Other reviews

The internal audit strategy may address some ad hoc areas that do not feature as risks. These are nevertheless areas where the organization would benefit from an internal audit review, or they are being reviewed to provide assurance to the audit committee and external auditors regarding operation of the key financial and management information systems. The audit days, fieldwork and reporting expectations for these areas should also be identified in the audit plan.

Contingencies

It is important to adopt a flexible approach in allocating internal audit resources, in order to accommodate any unforeseen audit needs or "hot spot" audits. The audit plan should give an indication as to how many hours have been allowed for contingencies.

Follow-up

For internal audit to be as effective as possible, its recommendations need to be implemented. Specific resources should be included within the plan to provide assurance to the organization and the audit committee that agreed audit recommendations have been actioned effectively and on a timely basis. A "follow up" program should be built into the annual audit plan.

Planning, reporting and liaison

The audit committee should expect the internal audit plan to identify activities relating to the following:

- quality control review by manager;
- production of reports, including the strategic plan and annual internal audit report;
- attendance at audit committee meetings;
- regular contact with the organization's management;
- liaison with external audit; and
- internal quality assurance reviews.

The internal audit team

The audit plan should identify the organizational structure of internal audit as well as total head count with a year over year comparison and identification of specialist resources. Where internal audit has outsourcing, the audit committee (and management) should expect a brief introduction to the key individuals working on the audit. This might include partners, managers and any specialist advisers.

Timing

The audit plan should set out the timing of the fieldwork and confirm the form and timeliness of reports to management and the audit committee. For example:

- a report for each area of work undertaken within x days of finishing the fieldwork;
- a progress report for each audit committee meeting; and
- an annual report on internal audit coverage to the audit committee (reporting to fit in with the committee meeting dates).

Exhibit 4 outlines how the timing might be presented for an internal audit carried out in three phases to coincide with the audit committee timetable.

Internal audit performance indicators

The internal auditor might propose a series of performance indicators against which management and the audit committee can measure the function's performance. An example of proposed indicators is included as Exhibit 5.

Exhibit 1: Internal audit plan – focus on the organization's key risks

Risk identified in the risk register	Ranking	Internal audit reviews over a three-year period
Failure of the new finance system	High	Finance system implementation
Missed ESG goals or inaccurate measures	High	ESG and related departments
Cyber security breaches not prevented	High	IT
Ineffective project assessment procedures	Medium	Contract management
Non-performance of contracts	Medium	Contract management/departmental reviews
Poor procurement of projects	Medium	Asset management
Failure to protect intellectual property	Medium	Intellectual property management
Statutory non-compliance (h&S)	Medium	health and safety
Non-prevention of foreseeable accidents	Medium	health and safety
Failure to adequately manage occupational stress	Medium	human resources
Failure to attract and retain high- quality staff	Medium	human resources
Non-financial control failure	Medium	Key financial systems/department reviews
Fraud, theft and misuse of assets	Medium	Key financial systems/department reviews
Reputation unclear or fragmented	Medium	Strategic planning
Ineffective business planning	Medium	Strategic planning/department reviews
Failure to consider future strategies	Medium	Strategic planning
Claw back of project funding	Low	Contract management/departmental reviews
Unsatisfactory procurement procedures	Low	Key financial systems – purchasing

Exhibit 2: Three-year rolling plan

Internal audit reviews	Current year	Year 2	Year 3	Total days
Risk based reviews				
Contract management	–	–	15	15
ESG	30	30	30	90
Cyber security	–	25	20	45
Asset management	–	–	15	15
Finance system implementation	50			50
Key financial systems	–	25	25	50
Health and safety	15	–	–	15
Human resources	15	–	–	15
Intellectual property management	15	–	–	15
IT systems	20	15	15	50
Strategic planning	20	–	–	20
Total risk-based days	165	95	120	380
Other reviews				
Risk management	10	8	8	26
Corporate governance	–	7	–	7
Corporate structures	–	–	22	22
Costing processes	–	15	–	15
Total other review days	10	30	30	70
Other				
Contingency/hot spot audits	8	8	8	24
Follow-up program	8	8	8	24
Planning, reporting and meeting	34	9	9	52
Total other days	50	25	25	100
Total days	225	150	175	550

Exhibit 3: Risks not subject to internal audit review

Risk	Ranking
Defamation/professional negligence	Medium
necessity for redundancies	Medium
Fire/explosion	Medium
Reputational risk	Medium
Failure to prevent a major incident	Medium
Failure to adopt equal pay provisions	Medium
Failure to prevent dismissals	Medium
Missed commercial opportunities	Low
Failure to adequately manage change	Low
Failure to prevent major health incident	Low
Statutory non-compliance – services	Low
Failure to prevent outbreak of food poisoning	Low
Building collapse	Low
Exposure to higher interest rates	Low

Exhibit 4: Annual plan

Internal audit reviews	Current year	Phase	Fieldwork	Report to audit committee
Risk-based reviews				
ESG	240	Phase 1	02.04.20xx	May meeting
Finance system implementation	400	All phases	All audit visits	Feb/May/oct meeting
Health and safety	120	Phase 2	w/c 26.02.20xx	31.05.20xx
Human resources	120	Phase 1	w/c 20.11.20xx	08.02.20xx
Intellectual property management	120	Phase 2	w/c 26.02.20xx	31.05.20xx
IT systems	160	Phase 1	w/c 20.11.20xx	08.02.20xx
Strategic planning	160	Phase 1	w/c 20.11.20xx	08.02.20xx
Total risk-based hours	1320			
Other reviews				
Risk management	80	Phase 2	w/c 26.02.20xx	31.05.20xx
Total other review days	80			
Other				
Contingency	64			
Follow-up	64	Phase 3	w/c 14.05.20xx	09.10.20xx
Planning, reporting and liaison	272			
Total other days	400			
Total Hours	2280			

Exhibit 5: Performance indicators

Key Performance indicators	Target
Percentage of audit work delivered by subject matter specialists	60%
operational plan to be submitted by September each year	September of each year
Follow-ups to be performed within 1 year of the audit taking place	within 1 year of assignments
Issue of draft reports within 30 days of work being completed	30 working days
Issue of final report within 10 working days of receipt of management responses	10 working days
Internal audit attendance at audit committee meetings	100%
Issue of internal audit annual report	September of each year



APPENDIX 8

Internal audit activities – key steps in the annual audit cycle

The key steps in an annual cycle

Produce the annual work plan

- Discuss internal audit priorities with the board to align on the organization's strategies, objectives and risks
- Create an annual internal audit plan for approval by the audit committee, typically as part of an indicative 3 or 5 year plan linked to a wider risk/audit universe
- Identify resource requirements, including relevant subject matter and industry experience to add value to the process, technological resources, and associated budgets
- Agree the timeline for performing individual assignments in the agreed plan
- Additional reviews may be required: the approach needs to be nimble to respond to the needs of the audit committee and the executive team
- Consideration should also be given at this stage to the interaction with risk management activities and the specific linkage of risk and assurance
- Discuss with the external auditor to get insights and alignment where possible

Plan individual assignments

- For each allocated audit assignment, terms of reference should be agreed in advance
- Staff requirements should be confirmed and communicated to the team reasonably far in advance of the work to help continuity
- Planning meetings with the nominated business sponsor and business process owners, information gathering and briefing of team members prior to each assignment

Perform fieldwork

- Fieldwork should commence with an opening meeting involving all relevant team members so that:
 - expectations are understood; and
 - the objectives, scope, techniques and emphasis of the review are clear
- A ‘no surprises’ approach is fundamental. The nominated business sponsor should be informed of issues as they arise
- Ways of working should be defined and consistently applied and measured (including the business responsibilities)
- Variations to timelines or budgets should be monitored and flagged as soon as they are identified to key sponsors

Exit meeting

- Prior to formal reporting, an exit meeting should be held with the relevant business sponsor and other employees as agreed
- The purpose of the meeting is to:
 - confirm that expectations have been met;
 - highlight and re-confirm the findings of the review;
 - validate the findings; and
 - where appropriate, obtain management’s acceptance and support for the recommendations made, including their commitment to actions with clear dates for implementation

Reporting

- Prepare a draft report to be issued to management within an agreed number of working days of completion of each audit and finalize the report, again within an agreed timeframe of receipt of management responses
- Report findings, specify who will address them and the planned date for them to be addressed
- Report in accordance with standard template
- Determine who should attend and present at stakeholder and audit committee meetings

Issue resolution tracking

- Following the issue of final reports, monitor agreed upon management action plans and subsequent reporting to senior management and the audit committee
- Clear protocols for follow up work as and when needed

Overall considerations

- Defined audit charter
- A defined strategy
- An ongoing awareness of key business risks and how this drives audit
- Clear role defined on related activities e.g. investigations/ad hoc assignments
- Agreed communication protocols
- Clear business case/cost analysis and monitoring
- Ways of working protocols
- KPIs to track progress and delivery
- Stakeholder satisfaction surveys



APPENDIX 9

Evaluation of the internal audit function

Periodically, the audit function should be assessed to evaluate its perception and value within the organization. This document provides an example internal evaluation approach. The Global Internal Audit Standards of The Institute of Internal Auditors provides that an internal audit activity must also obtain an external assessment at least every five years by an independent reviewer or review team. At least annually, the chief audit executive must communicate the results of the internal quality assessment to the board and senior management. The results of external quality assessments must be reported when completed.

This example assessment process focuses on your personal perception of the internal audit function as a whole – it does not seek to evaluate individuals and their personalities. The audit committee chair should determine who is asked to complete the questionnaire. It is not unusual for it to be completed by audit committee members, (prior to feedback from other areas of the organization); the heads of major business units/subsidiaries and the CFO; and the head of the internal audit function (i.e. self assessment). The external auditor may also be asked to comment.

The questionnaire takes about 10 minutes to complete and should be completed in the following manner:

- Using a scale of **1** (low) to **10** (high), complete each question by placing your score in the two boxes beside the question. **‘Actual’** is your view of the current position of the internal audit function on that issue. **‘Ideal’** is the score that you would like to see. The difference can be used to determine the relative priority of each issue.

You may wonder why there is a choice of score on the **Ideal** position as you may think it should always be a ten (the maximum). This may often be the case; however, there may be occasions where you feel an area is of less importance and therefore may merit an Ideal score lower than ten. We would stress that the main reason for asking for the two scores is to see where the biggest gaps are between **Actual** and **Ideal** as this identifies where any development priorities lie.

- There is a space for comments beside each question. You are not obliged to make comments; however, comments do improve the quality of the review and therefore are to be encouraged.
- ‘N/A’ can be used where you don’t have a view on the matter in question.
- All responses will be treated as anonymous unless the individual completing the questionnaire wishes otherwise.

Typical answers look like this:

	Actual	Ideal	N/A	Comments
1. Internal audit has a comprehensive strategic plan, developed in collaboration with the audit committee, executive management and principal stakeholders; and aligned to the organization’s own strategy and risk profile.	6	10		While the internal audit plan is comprehensive, more timely, up-front involvement could improve the process.
2. Internal audit harnesses technology throughout its audit and administrative processes to maximize efficiencies and improve audit effectiveness.	7	7		The technology used is appropriate for the current size of our organization, however more would be required as we grow in size and scale.

A. Positioning

Mandate and strategy	Actual	Ideal	N/A	Comments
1. Internal audit has a comprehensive strategic plan, developed in collaboration with the audit committee, executive management and principal stakeholders; and aligned to the organization’s own strategy and risk profile.				
2. Internal audit is recognized by business leaders as a function providing quality challenge (for example by telling them things they did not already know, identifying root causes of control breakdowns and opportunities for improving control design, and trends in risks and controls).				

Mandate and strategy	Actual	Ideal	N/A	Comments
3. Internal audit has a sound understanding of business strategy and the associated risks, and is able and willing to challenge the control environment and infrastructure supporting the strategy and is able to reach across from one part of the organization to another?				
4. Internal audit has an integral role in the governance structure (as the 'third line of defense') which is clearly aligned with its stakeholders, clearly articulated in its mandate and widely understood throughout the organization.				
Organization and structure	Actual	Ideal	N/A	Comments
5. Internal audit is independent from the business and has clear and unfettered reporting into the audit committee and direct access to the chair of the board.				
6. Internal audit is structured to enable both independence and objectivity on the one hand, and proximity to the business (so as to establish and maintain relationships with and comprehensive understanding of the business) on the other.				
7. Internal audit consults and collaborates with risk control functions to ensure an appropriate allocation of responsibility within the organization.				
8. Internal audit consults and collaborates with information technology and information security functions to ensure effective and responsible use of technological resources.				
9. Internal audit has a presence in major governance and control forums throughout the organization, for example, any other committee.				

Stakeholders	Actual	Ideal	N/A	Comments
10. Internal audit is characterized by strong relationships at the highest levels (for example, does the head of internal audit and senior colleagues have direct and strong relationships with board members, business heads and senior management)?				
11. Internal audit regularly attends executive meetings to present audit findings, trends and current views (of the control environment).				
12. Internal audit regularly attends audit committee meetings to present audit findings, trends and current views (of the control environment).				
13. Through its activities, internal audit can articulate to senior management the risks of their actions in a structured and balanced manner, and provide credible recommendations to mitigate the risks.				
14. Internal audit has strong relationships with key external stakeholders (in particular, external auditors and any relevant regulators).				
15. Internal audit proactively manages relationships with its key stakeholder population.				
Funding	Actual	Ideal	N/A	Comments
16. Internal audit has no unreasonable budgetary constraints which limit its ability to deliver on its mandate, given the risk appetite of the organization.				
17. Internal audit manages its resources effectively to maximize the value of its service to the business.				

B. People

Leadership	Actual	Ideal	N/A	Comments
1. Internal audit has the standing, credibility and impact to present its views in audit (and risk) committees and influence the organization.				
2. Internal audit includes sufficient individuals who are senior and experienced, with sufficient business understanding, to apply judgement and display professional courage to challenge the business on a broad array of topics.				
Competencies	Actual	Ideal	N/A	Comments
3. Internal audit comprises a diverse talent pool with a broad mix of skills and experience gained within internal audit and in business..				
4. Internal audit includes individuals recognized (by the business) as experts in governance, control and risk mitigation.				
5. There is an appropriate mechanism for identifying the skills and competencies required to deliver its annual plan, identifying and relieving gaps and being responsive to the changing risk profile of the organization.				
Staffing strategy	Actual	Ideal	N/A	Comments
6. Internal audit is forward thinking in its medium to longer term staffing strategy (for example, by considering growth areas in the business, new and emerging risk areas, and both internal and external factors affecting the function's ability to attract talent).				
7. Internal audit is able to attract resources by providing a value added career development opportunity to the organization's top talent.				
8. Internal audit is able to develop its personnel through comprehensive training and development.				

Culture	Actual	Ideal	N/A	Comments
9. Internal audit is characterized by a culture balancing collaboration and effective challenge.				
10. Internal audit is characterized by a culture of continuous improvement in the internal audit process.				
11. Internal audit acts as a role model and adheres to high ethical standards and values.				
Reward and appraisal	Actual	Ideal	N/A	Comments
12. Internal audit has competitive remuneration policies based on the achievement of defined performance metrics (for example, based on quality of work and impact upon the business, and not simply delivery against plan and business performance).				

C. Processes

Risk assessment and planning	Actual	Ideal	N/A	Comments
1. Internal audit has a risk based audit plan based on a risk assessment accepted and approved by the board.				
2. Internal audit is forward looking when determining the audit plan and is nimble enough to adapt its planned activities, sometimes rapidly, in the case of new and emerging risks.				
3. Internal audit submits its plan to the audit committee for approval on a timely basis (at least annually) and as appropriate when updates are required.				

Execution	Actual	Ideal	N/A	Comments
4. Internal audit reflects on and adapts its methodology to ensure that it remains fresh and relevant, through integrated (not post hoc) quality assurance and learning programs.				
5. Internal audit conducts end- to-end/ corporate wide audit activities which enable it to obtain a holistic view (for example, within and across business units, functions, processes, and jurisdictions) as to whether the primary risks facing the organization are appropriately mitigated.				
6. Internal audit harnesses technology throughout its audit and administrative processes to maximize efficiencies and improve audit effectiveness.				
7. Internal audit maintains and promotes comprehensive knowledge management systems, widely used by its staff.				
Reporting	Actual	Ideal	N/A	Comments
8. Internal audit produces evidence-based reports for individual audits with a clear rating scale which identify both root causes and consequences of issues and which are delivered on a timely basis with clarity and impact, and include credible recommendations to management.				
9. Internal audit produce evidence-based reports for the audit committee which present information in a clear, concise and impactful manner, including the identification of themes and trends, and their consequences for the organization as a whole.				
10. Internal audit has rapid and effective mechanisms in place for the escalation of issues requiring senior management attention.				
Overall	Actual	Ideal	N/A	Comments
11. Internal audit has added value to the organization. Provide examples.				

D. Comparison of XYZ’s internal audit function with other internal audit functions
you may have experience of:

Risk	Comments



kpmg.com/ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. 29766