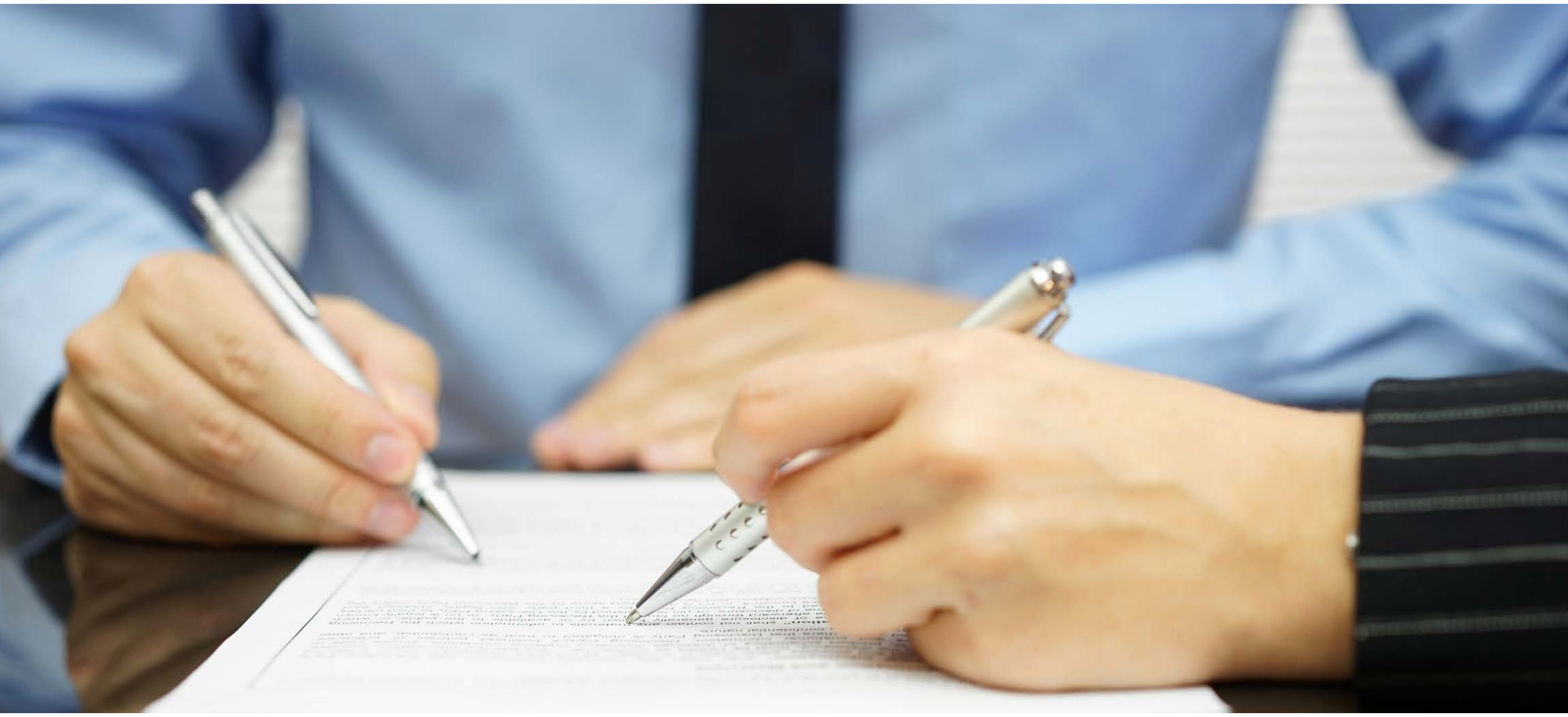
20 Questions Directors Should Ask about **Internal Audit**

REVISED 2015

Bruce Webster



CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

20 Questions Directors Should Ask about **Internal Audit**

REVISED 2015

Bruce Webster

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

DISCLAIMER

This publication was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

Library and Archives Canada Cataloguing in Publication

Webster, Bruce J. (Bruce James), author
20 questions directors should ask about internal audit / Bruce James Webster. -- 3rd edition.

Includes bibliographical references.
ISBN 978-1-55385-977-2 (paperback)

1. Auditing, Internal. 2. Auditing, Internal--Miscellanea. I. Canadian Institute of Chartered Accountants, issuing body II. Title. III. Title: Twenty questions directors should ask about internal audit.

HF5668.25 W42 2016 657'.458 C2015-907878-4

Preface

The Risk Oversight and Governance Board (ROGB) of the Chartered Professional Accountants of Canada (CPA Canada) has commissioned this publication *20 Questions Directors Should Ask about Internal Audit* to help directors overseeing the internal audit function understand the rapidly changing environment in which their organizations are operating. The publication can also be used by management and members of the internal audit community to guide their discussions and prepare for interaction with their boards.

This *20 Questions* addresses the increasing number and complexity of risks facing organizations, and focuses on how internal audit must adapt its role in order to “build value” while helping to mitigate these risks.

The publication identifies the most important questions a board should consider in order to effectively oversee internal audit. The questions and responses reflect leading industry practices, as well as The Institute of Internal Auditors’ (IIA’s) Standards for the Professional Practice of Internal Auditing.

The author has approached the questions and responses using various concepts of “value” as a central framework throughout the *20 Questions*. The fundamental question of whether a particular organization should have an internal audit function is explored up front. This then sets the stage for an in-depth examination of several key areas that impact the internal audit function:

- Mandate
- Relationships
- Organizational design and resources
- Reporting and communication
- Evaluation of the internal audit function

In summary, this publication provides an overview of the responsibilities of directors in overseeing the internal audit function in an environment of increased expectations of the internal auditor.

The ROGB acknowledges and thanks the members of CPA Canada's Directors Advisory Group for their invaluable advice, the author, Bruce Webster, and contributors from IIA Canada.

Bryan Held, FCPA, FCA, ICD.D
Risk Oversight and Governance Board

Author

Bruce Webster, CPA, CA.IFA, CFE, CFF
PwC LLP

The author would like to thank and acknowledge Mark Burnes and Richard Wilson of PwC for their support throughout this project and valuable contribution to the publication.

Risk Oversight and Governance Board	Directors Advisory Group
Bryan Held, FCPA, FCA, ICD.D, *Interim Chair*	Giles Meikle, FCPA, FCA, *Chair*
Andrew Foley, J.D.	Hugh Bolton, FCPA, FCA
Alex Guertin, MBA, CPA, CA	John E. Caldwell, CPA, CA
Douglas Hayhurst, FCPA, FCA, ICD.D	William Dimma, F.ICD, ICD.D
Giles Meikle, FCPA, FCA	Carol Hansell, LL.B. F.ICD
Sue Payne, FCPA, FCA, C.Dir	Thomas C. Peddie, FCPA, FCA
Vincent Tophoff, RA	Guylaine Saucier, CM, FCPA, FCA, F.ICD
John E. Walker, CPA, CA, LL.B.	Hap Stephen, CPA, CA
Richard Wilson, HBA	Peter Stephenson, PhD, ICD.D
	Janet Woodruff, FCPA, FCA, ICD.D

Project Direction, CPA Canada

Gigi Dawe, LL.M.
Principal, Research, Guidance & Support
Leader, Corporate Oversight & Governance

Gordon Beal, CPA, CA, M.Ed.
Vice-President, Research, Guidance & Support

Contributors from IIA Canada

Carmen E. Abela, MPA, CIA, CCSA, C. Dir.

Richard G. Arthurs, MBA, CPA, CMA, CIA, QIAL

Brian G. Brown, CIA, CPA, CMA, C.Dir.

Judith K. Burke, MBA, CCSA

Jeff Erdman, CPA, CA, CIA, CRMA, CISA, CISSP

John Fraser, FCPA, FCA, CIA, CRMA

Hal Garyn, CIA, CRMA, CISA

Carman Lapointe, CIA, CCSA

Jodie Lobana, MA, CPA, CA, CIA, CISA, PMP, IFRS

Amipal Manchanda, CPA, CA, CMA

Archie Thomas, CIA, FCPA, FCMA, C.Dir., CFE

Table of Contents

Preface iii

Introduction 3

Mandate 5

1. Should our organization have an internal audit function? 5
2. What is the Board's role and responsibility with Internal Audit? 6
3. What strategy and culture should Chief Audit Executives create for their departments? 7
4. How does Internal Audit maintain its independence and objectivity? 8

Relationships 11

5. What type of relationships should Internal Audit develop with its stakeholders? 11
6. To whom should Internal Audit report? 12
7. How can the Board optimize its relationship with the Chief Audit Executive? 13

Organizational Design and Resources 15

8. Is your IA function agile and prepared to continuously improve as needed? 15

9. What qualities should a Chief Audit Executive possess? 16

10. What new capabilities are leading internal audit functions developing today? 17

11. What are the top priorities in the Internal Audit plan? 18

12. Should Internal Audit place reliance on other assurance functions? 19

13. How does Internal Audit anticipate and adapt to emerging or changing risks? 21

14. How should management be held accountable to address/resolve audit findings? 22

15. How should Internal Audit deal with concerns of management (and even Board) misconduct? 22

Reporting/Communication 25

16. What content should Internal Audit communicate in quarterly reports to the Board? 25

17. How does Internal Audit determine what risk and control issues should be reported to the Board? 27

18. Effectively utilizing the in-camera session. "Are there any other matters that you wish to bring to the Board's attention?" 28

Evaluation of the IA Function 29

19. How should the Board evaluate the Internal Audit function? 29

20. Is Internal Audit continually following industry leading practices? 30

Conclusion 33

Where to Find More Information 35

About the Author 37

Introduction

Since the original *20 Questions Directors Should Ask about Internal Audit* document was published the complexity of the risk universe facing organizations has changed substantially. Reasons for this include, but are not limited to, growing cyber based issues (e.g. security, mobile technology, social media, emergence of big data), increasing regulation, uncertain economic and political situations, focus on sustainable development and the environment, and frequent natural disasters. This has resulted in higher expectations of the internal audit function.

Boards and management teams should expect their Internal Audit departments to adapt to this new environment. The revised *20 Questions Directors Should Ask about Internal Audit* acknowledges this changing landscape, addressing fundamental questions about the function's evolving role in governance, risk, and compliance, presenting challenging questions about the future value that Internal Audit can provide. The questions and responses are designed to comply with IIA's Standards for the Professional Practice of Internal Auditing (IIA's Standards), as well as leading internal audit practices. They are meant to be the basis for an informed discussion amongst Board members, management, and the internal audit function itself about the aspirational concepts underlying how internal audit can adapt to the new expectations that are being created for the profession.

A key theme throughout this revised edition involves the concept of "building value." There is an "ask" of many Internal Audit departments to evolve, create, and preserve sustainable value for their stakeholders. The term "value" has many competing definitions. Does it involve helping the organization to more efficiently and effectively pursue its strategic priorities? Is it focused on supporting the organization on key initiatives such as new products, mergers and acquisitions, and business transformation initiatives? Or does it equate to providing assurance over compliance with external regulations and internal policies and procedures? The answer to these questions will depend on the nature and complexity of the risks that an organization faces and the level of involvement that it feels the internal audit function should have in helping management address them and Boards gain assurance about them.

NOTE: This document is written for the governing body, or committee, that is responsible for internal audit. Although this is typically the Audit Committee, in small or privately held companies it could be the full Board. In this document, we refer to either interchangeably as the “Board”.

Mandate

1. Should our organization have an internal audit function?

Boards are recognizing the complexity that increasing governance expectations, emerging risk, and new regulation can add to their accountability. Independent assurance and advisory services can play a critical role in helping them discharge their governance responsibilities.

If you are a Board member for a publicly traded entity, this is almost certainly a moot question. Should your organization be without an internal audit function, the decision to introduce this capability is an important consideration for you from a governance and operational perspective. Internal Audit can assist you in discharging your roles and responsibilities by providing you with a level of independent objective assurance regarding the quality of controls over the risks to the organization. An internal audit function can help your organization manage its risks, processes, and controls impacting key strategic goals and objectives, mitigating scrutiny by regulators, and if desired, assist management in providing its assurance over fraud and financial reporting controls.

The size and maturity of your organization are important factors to consider, as internal audit is not a requirement for all organizations. Boards of smaller organizations may believe that sufficient comfort is already being obtained through the oversight currently present at the organization. For example, self-monitoring, direct supervision by the owner/management, information system security, and health and safety checks are all forms of potential oversight. Therefore, smaller organizations may already have an acceptable level of assurance inherent in their existing risk management arrangement without requiring a designated internal audit function. Nevertheless, Boards should seriously consider the value that independent assurance and advisory services provides in helping them discharge their governance responsibilities.

Boards of smaller growing organizations should consider the added risks that encompass expansion and whether they can benefit from the independent assurance and advisory support that can be provided by an internal audit function. For instance, organizations entering into new markets of developing new lines of business/products, an internal audit function can help prepare for the increased risk landscape, and provide management their insights as the associated processes and controls are developed.

Complex businesses may face risks which require a heightened level of oversight, monitoring, and expertise. They typically have a complex risk management arrangement that necessitates the need for having an independent internal audit function that tests the design, efficiency and effectiveness of its control environment.

2. What is the Board's role and responsibility with Internal Audit?

The Board should have an understanding of what they expect from internal audit, to be in a position to maximize the relationship with the function.

The following sets out typical responsibilities of the Board with respect to internal audit:

- Approve the internal audit function's charter — and review periodically to ensure it provides the appropriate independence and mandate;
- Participate in the appointment, evaluation, replacement, and compensation of the Chief Audit Executive (CAE);
- Ensure there is an open direct relationship and ongoing communication with the CAE;
- Approve a risk-based internal audit plan, review the process used to develop the plan, and gain an understanding of why other potential audits were excluded from the plan;
- Ensure internal audit has sufficient resources and budget to execute the audit plan;
- Require the CAE to regularly report on the status of the audit plan and results of internal audit activities; and
- Invite the CAE to attend regular Audit Committee meetings, including in-camera sessions.

In addition, although it is acknowledged and agreed that management and the Directors are responsible for determining the appropriate strategy for the organization, Boards must consider whether they want internal audit to have a "seat at the table" during such discussions. Leading internal audit functions can provide their Boards comfort that the right risks are being considered and discussed relating to the proposed strategy and any outcomes of its success. However, Boards need to ensure that internal audit's "seat at the table" is limited to an advisory role and not as a direct participant to ensure internal audit is not in a decision making capacity or performing a management function, which could impact its independence and objectivity.

3. What strategy and culture should Chief Audit Executives create for their departments?

Boards should consult with the CAE to agree upon the type of strategy and culture that is most appropriate and valuable for the organization.

As the leaders, CAEs are responsible for shaping the strategy and culture of their internal audit functions. Strategy, in this context, refers to the value proposition that the internal audit function creates in relation to the strategy and objectives of the organization, and how this will be continuously sustained and improved over time. This strategy should include:

Foresight	Looking towards the future to determine what are the most relevant and probable risks facing the organization that may interfere with the organizations strategy and objectives.
Insight	Proactively seeking out best practice for continuous improvement of risk management, controls, and the capabilities of the internal audit function.
Hindsight	Providing independent assurance over how effective and efficient the risk management program and controls have been to date.

Culture, in this context, refers to the common ideals, philosophy and behavior of the internal audit department. Effective, crucial cultural elements that Boards should look for in an internal audit function include:

Integrity and ethics	Planning, executing, and reporting audits in an unbiased and balanced manner, escalating ethics issues to the appropriate level of management and the board when required, and generating findings and recommendations that are supported by evidence
Risk focus	Alignment of audit plan to strategic plans and their corresponding risks, and a dynamic approach to scoping and conducting audits that addresses business level risk arrangements
Cost effectiveness	Maximizing impact with a fixed budget through prioritization, an effective resourcing model, efficient audit processes, and standardizing processes where possible
Quality and innovation	Bringing to bear the appropriate skills to conduct value added audits, a robust quality assessment process, and conducting audits using the most relevant technologies and practices available
Service culture	Working with its clients (the business/process owner) to develop practical, actionable solutions

4. How does Internal Audit maintain its independence and objectivity?

Independence and objectivity is required for the board, audit committee and external parties to place reliance on the work completed by internal audit.

In order for the IA function to execute their role in an effective and efficient manner, the Board and management must be confident that there is a pervasive and sustainable level of independence and objectivity within the team itself, with co-sourced audit resources, and across all IA activities.

Of the CAE and IA team: The Board will expect and look for evidence that the CAE has recruited and lead a team that performs its duties with objectivity, independence, strong moral character, candor, and fairness with all work completed. The Board should regularly remind IA that it is their "eyes and ears" into the organization and as such independence is critical.

Attribute standard 1100 of the IIA's Standards defines independence as "…freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner", and objectivity as "…an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made." Does IA have a motive to be influenced by management in reporting their findings? Can management exert inappropriate expectations? Establishing a formal, functional reporting relationship from IA to the Board, and demonstrating ongoing support and guidance to IA significantly reduces this risk.

Of any IA co-sourced resources: The Board should expect and look for evidence of service providers that avoid conflict of interest between their clients' interests and their own, in addition to the traits listed above for the IA team and process. Is the service provider shaping its findings in order to gain follow-on remediation revenues? The more independent IA is in choosing its service providers, and the closer they are managed, the less incentive and opportunity there is for the service provider to put its interests before the organization's.

The IA activities: The Board should expect and look for evidence that IA processes are designed to identify, validate and report significant unmitigated risks to senior management and the Board.

Internal audit should establish policies that promote these behaviors, and conduct ongoing monitoring and training. Boards can gauge internal audit's integrity, objectives and performance through discussions with the CAE, as well as through examining the results of external quality assessments.

Relationships

5. What type of relationships should Internal Audit develop with its stakeholders?

The Board should be satisfied that internal audit has an effective working relationship with management, the external auditor, and third parties required to meet the audit plan.

Internal audit is required to balance the needs and expectations of a number of stakeholders. A list of key stakeholders is described in the following table:

Stakeholder	Nature of relationship with Internal Audit
Board/Audit Committee	The Audit Committee of the Board, if present, is most commonly responsible for overseeing IA, and providing guidance and direction. Its responsibilities typically include reviewing and approving the internal audit mandate and audit plan; ensuring that the internal audit function is sufficiently resourced to carry out its responsibilities and maintains the right culture; supporting internal audit in fraud related matters; and maintaining a direct and open line of communication with the CAE. It is important for Audit Committees to meet with internal auditors *in camera* at least a few times each year, since this reinforces internal audit's independence from management as well as gives them an opportunity to discuss sensitive issues and topics without management present. It is equally important that the CAE and Audit Committee Chair to consider getting together informally in order to strengthen their relationship. Leading internal audit functions also have relationships with other relevant committees of the Board beyond the Audit Committee (i.e., risk, finance, governance, etc.) where appropriate.

Stakeholder	Nature of relationship with Internal Audit
Line/senior Management (CEO, CFO & Other ELT members)	Internal audit requires cooperation and collaboration with senior management in order to carry out its plan. The board should be satisfied that there is an effective working relationship between management and internal audit. This will increase the likelihood that internal audit work will result in observations and recommendations that are valued by the business, and contribute to a culture of continuous improvement of the organization's strategic and operational processes, including the man management of risk.
Enterprise Risk Management (ERM)	The ERM function supports management in identifying and managing risk. The board should ensure that internal audit is incorporating the appropriate ERM outputs into the development of its audit plan. IA should develop a strong relationship with the ERM team. As part of its oversight responsibilities, however, internal audit must also provide assurance to the board and senior management that ERM activities are effective.
Other assurance functions	Internal audit should leverage the work of other assurance functions (e.g. compliance, health and safety), and determine the level of reliance that can be placed on them when establishing internal audit coverage required in these areas.
External Auditor	External auditors consider IA's effectiveness as part of their assessment of the control environment. They may also rely on the work of IA to test certain internal controls.

Internal audit is required to manage a number of stakeholder relationships, often with competing needs. The CAE should appropriately balance these needs and expectations, and periodically assess internal audit's performance relative to them.

6. To whom should Internal Audit report?

Internal audit's independence, both real and perceived, is optimized when it reports functionally to the board, or to the audit committee of the Board.

Internal audit's independence from management is important to fulfilling its mandate to provide objective assurance over the organization's governance, risk, and control activities. The IIA provides guidance on maintaining independence, stating that it is considered to be good practice when the CAE reports functionally to the Board and administratively to management. The functional reporting relationship to the Board allows for Board involvement in key decisions such as approving the internal audit plan and budget as well as approving the compensation and appointment or removal of the CAE. Internal audit is responsible for engaging the Board on key decisions involving the people, processes, technology, and structure of the function, as well as interpreting significant audit findings. Other Board committees may have an interest in hearing from internal audit periodically as well. This could include the Risk Committee regarding coverage of applicable operational risks.

IIA guidance indicates the “higher the better” when it comes to determining IA’s administrative reporting relationship. The most common administrative reporting relationship of the CAE is (in order of recommended practice), to the CEO, Senior Legal Officer, and then CFO. The individual to whom the CAE reports administratively can have a significant impact on the function’s profile and influence within the organization. A reporting relationship to the CEO can benefit the function in advising and working with operational departments that align closely with the organization’s core strategic objectives. Good governance advocates that care should be taken to ensure IA’s independence and objectivity can be maintained notwithstanding its administrative reporting relationship.

The administrative reporting relationship to management is important as it enables internal audit to operate on a day to day basis without direct board involvement, and provides the basis for internal audit’s role as an independent, collaborative, trusted business advisor to management.

7. How can the Board optimize its relationship with the Chief Audit Executive?

The relationship between the Chair of the Audit Committee and the CAE is critical for Internal Audit to maximize its value to the Board.

A strong relationship between the two individuals will enable healthy and honest discussions.

A 2013 paper published by the IIA’s Research Foundation titled “The Audit Committee and the CAE, Sustaining a Strategic Partnership” discussed the importance of a CAE and their audit committee chair to have an open, trusting relationships and suggested four opportunities for these positive interactions to be developed:

- Attending training programs together.
- Sitting in on webcasts targeted at both CAEs and audit committee chairs.

- Getting together for open-ended discussions on an ongoing basis, perhaps even during the evening or on a weekend.
- Jointly visiting business sites to foster mutual understanding of operations and business issues.

Organizational Design and Resources

8. Is your IA function agile and prepared to continuously improve as needed?

Forward looking internal audit functions are continuously asking what capabilities are going to be needed to meet future expectations.

Boards should not only gain comfort over the IA function's strategy, but should also determine whether the IA function is agile enough to deliver this mandate.

Boards should look for the following characteristics in an internal audit function:

- **Agility:** As an organization changes, so should internal audit. The design of the function should be responsive to new risks that an organization faces as it evolves and grows. IA's staffing must match its Audit Plan, as well as the organization's risk profile, in terms of skills and experience. This starts with recruiting the right people and can then be enhanced through training and education programs for the core internal audit team, as well as the ability to leverage internal/external subject matter expertise when required. It is also critical that permanent IA staff at all levels be involved in a diverse range of assignments to help them gain a broad perspective on the organization.
- **Staff development and subject matter expertise:** High performing internal audit functions have had great success with job rotations and utilizing guest auditors. Job rotation assignment, outside of internal

audit, allows internal auditors to broaden their perspectives and become more well-rounded professionals. Job rotations also solidify a collaborative working relationship between IA and the business areas they are responsible for auditing. For non-internal auditors (seconded from other departments), rotations into internal audit provide opportunities to broaden their experience and knowledge, and to appreciate the contribution and valuable work of internal audit. Guest auditors are often used to utilize subject matter experts, although it is critical to find individuals who are independent from the area being reviewed.

- **Continuous improvement:** Does internal audit challenge itself to improve the relevance, effectiveness, and efficiency of its work, including how it interacts with and supports the various stakeholders? Also, when internal audit conducts and reports to the board regarding internal and external assessments, this is a good sign that they are constantly striving for improvement. Benchmarking within your industry or with other internal audit groups can be a great source for best practices and opportunities to share with leadership and the audit committee.

Organizations may also consider using part-time staff, contractors and outsourcing arrangements rather than hiring a full-time team in order to recognize the need to scale the functions to the size of the organization.

9. What qualities should a Chief Audit Executive possess?

A CAE must be a leader with high integrity, courage, executive presence, a strong understanding of the business, a desire to learn, the ability to manage expectations and influence, and be an effective communicator.

The traditional qualities of the CAE are typically focused on strong leadership, interpersonal, organizational, and analytical skills. CAEs are role models for their IA teams, and set the tone in terms of how their departments operate and interact with their Boards and the rest of their organizations. They know that the strength and effectiveness of their teams are critical to their department's success, so they build the right team and have sufficient interpersonal skills to motivate and empower the individuals to succeed in achieving IA's objectives.

In addition to the qualities listed above, modern CAEs have developed an ability to manage two roles — the more traditional assurance role as well as an advisory role. Managing both roles requires salesmanship, diplomacy, humility, assertiveness, and an ability to earn the trust and respect of the stakeholders they are working with. They are also flexible and responsive, and recognize that the IA function must continually review and assess whether it is aligned with new risks and organizational changes.

Boards should look for someone who can be viewed as a leader not just within their department, but across the organization as a whole. In these cases, Boards should insist that management include the CAE in any leadership/planning/strategic type meetings or discussions to allow IA to be mindful of current and emerging issues and priorities affecting the organization. (Ask yourself: Does my CAE have executive c-suite presence?)

10. What new capabilities are leading internal audit functions developing today?

Emerging risk and best practice internal control trends should dictate what new capabilities your internal audit group should invest in, such as data analytic expertise and cyber security knowledge.

It is critical that IA functions develop and continually update their skillset to keep pace with the challenges facing their organizations (being industry trends, new product/service offerings, new business partnerships, etc.). Assembling the right skills is dependent upon the risk profile of your organization and the audit strategy/plan developed to provide the Board assurance over the controls in place to mitigate risks to an acceptable level. It is critical that the skills assembled must be aligned with that needed to successfully execute the audit plan. Leading internal audit functions recruit staff with a variety of backgrounds and professional experience to match the operations and risk areas of its company (for example, engineers, actuaries, information technology, healthcare). Before approving the audit plan, Boards should ask whether the skill set assembled in the IA function is sufficient to successfully execute the audit plan.

New capability such as data analytics is becoming very popular with internal audit functions for specific audit testing, continuous monitoring and auditing, and it is also being used for predictive analysis. As technology and software becomes more sophisticated and user friendly, the use of data analytics will continue to grow. Internal audit functions either have an in-house data analytics expert or outsource this capability to a third party.

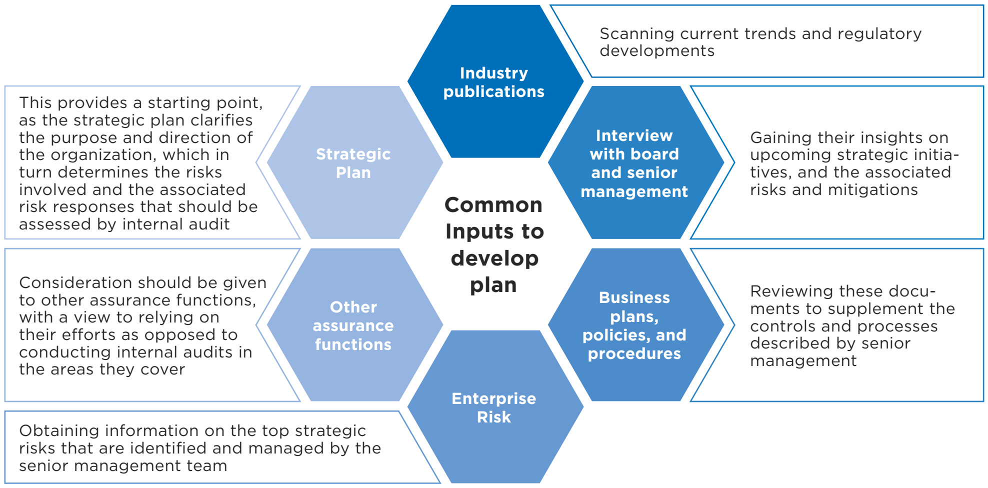
Organizations are also seeking greater capability within internal audit to support IT governance and cyber security. Some of the key risks related to this are cyber attacks that disrupt business operations or result in |a breach of privacy or confidential data.

Every internal audit organization should continually ask what capabilities will be required to address emerging risks.

11. What are the top priorities in the Internal Audit plan?

IIA Standards require that the audit plan must be risk based and as such the internal audit risk assessment is the foundation to any audit plan.

The audit plan must be aligned with your organization's strategic objectives to make sure the right audits are performed with the right scope. This alignment will help Internal Audit provide assurance to its Board that the risks that could impact the success of these objectives are being adequately mitigated. IIA Standards require that the audit plan must be risk based and as such the internal audit risk assessment is the foundation to any audit plan. At a minimum, Internal Audit must gain an understanding of the organization's key risk areas (both current and emerging) that are specific to an organization as well as those that are inherent to the relevant industry. The board should ensure that internal audit is incorporating the appropriate ERM outputs into the development of its audit plan. Inputs that Internal Audit should consider in developing an internal audit plan to provide coverage over these key risk areas, over a reasonable period of time, are set out in the table below:



The leading practice is to have a multi-year strategy (maximum 3-years) that includes a detailed rolling 12 to 18 month audit plan. Both the strategy and plan are continuously updated through an ongoing risk assessment process, in order for internal audit to respond to emerging risks or issues. As it is common for Internal Audit to have a budget, decisions must be made as to which risks/areas are to be audited. For this reason, the plan should not only set out the audits in scope but also advise the Board which audits were considered then excluded from the plan, as well as an explanation as to why any key risk areas/priorities/issues are not in scope.

The Board must approve the audit plan and any changes made to the plan.

12. Should Internal Audit place reliance on other assurance functions?

Coordinating with and relying on internal assurance functions reduces duplication of efforts, minimizes audit fatigue, and provides a forum for sharing risk assessment insight and best practices.

Organizations typically have a number of different assurance functions in addition to internal audit. These include compliance groups, quality management functions, internal control teams that assess controls (e.g. financial reporting), and IT governance groups. Also these assurance groups are a great source of insight on risk assessment and for continuously finding out more cost effective ways of providing assurance and advisory services.

Examples of assurance groups which internal audit could work together with include, but is not limited to: Enterprise Risk Management; IT governance (including cyber security); Environment, Health, and Safety; Security; Insurance; Legal and Ethics; and Project Risk Management.

Elements that should be considered as part of the reliance process include (IIA Practice Guide—Reliance by Internal Audit on Other Assurance Providers, December 2011):

1. **Purpose**
   The assurance provider is clear in purpose, and is committed to providing assurance on a specified risk area so that their work is relevant to internal audit's objectives and scope.
2. **Independence and Objectivity**
   The professional judgment of the assurance provider is impartial, without inappropriate interference from others.
3. **Competence**
   The assurance provider has appropriate organizational process expertise, education level, professional experience, relevant professional certifications, continuing education, and reputation for sound judgment.
4. **Elements of Practice**
   The assurance provider establishes and follows appropriate policies, programs, and procedures. In execution, assurance work is appropriately planned, supervised, documented, and reviewed. Finally, results are based on persuasive evidence sufficient to support the level of assurance.
5. **Communication of Results and Remediation**
   The assurance provider communicates results and looks to management to take action in a timely manner. Weaknesses and deficiencies are reported to the person directly responsible for taking corrective actions and to the members of management that have oversight responsibilities.

Once a listing of reliable assurance providers has been developed, the scope of each provider should be mapped to the internal audit plan. This should be presented to the board each year at the same time as the audit plan so that the board can determine how the various audit and compliance functions have been integrated into the company's overall governance, risk and assurance framework.

13. How does Internal Audit anticipate and adapt to emerging or changing risks?

Internal audit should be engaging senior management and other internal and external stakeholders about the latest initiatives, projects, external trends, and best practices on a continuous basis.

Organizations navigate a wide range of external and internal drivers of risk. These can include:

- Business disruption or data loss caused by a cyber attack;
- Material financial misstatement caused by changes in leadership;
- Incurring penalties and reputation risk in relation to new regulatory requirements;
- Revenue loss due to competitive entities, products, and services;
- Credit rating decline driven by economic conditions;
- Legal and regulatory issues caused by hostile mergers and acquisitions;
- Cost overruns caused by change such as implementing a new ERP system;
- Financial loss related to major capital projects;
- Extraordinary expenses linked to changing climates and environmental events;
- Demand loss due to shifting social and cultural attitudes;
- Market share erosion due to technological changes and competitive innovations;
- Incremental expense related to changes in government leadership or policies; and
- Margin erosion tied to shifts in the price of commodities, oil & gas, and other inputs.

The Board should be satisfied that internal audit is anticipating, and has considered the impact of, these risks on its objectives, strategy, audit plan, structure, and resources. Internal audit should be engaging senior management and other internal and external stakeholders about the latest initiatives, projects, and external developments on a continuous basis. Boards can also play a role in informing internal audit of any anticipated significant changes on the planning horizon. Once known, the Board may want to engage with the CAE to discuss potential changes to the audit plan.

14. How should management be held accountable to address/resolve audit findings?

Management will always be the first line of defense to prevent, detect, or react to risk, and therefore they should also be expected to expedite control improvements recommended by internal audit.

Internal audit is responsible for developing a program to monitor and report on the status of management action plans resulting from audit findings. This can be done through periodic checkpoints and by conducting follow-up audits. The result is that internal audit has an opportunity to examine remedial actions in detail, and gather evidence to support management's conclusion that action plans have been carried out and completed sufficiently. The results of these follow-up actions should be reported to the Board.

Boards should determine whether management is engaged in developing and completing action plans to mitigate the risks associated with internal audit findings. The status of open action plans should be reported. As well, significant past due action plans, with corresponding executive sponsors, deadlines, and reasons for the delay should be reported to the board at each meeting. When response timelines are not adhered to by management, boards may choose to invite the executive sponsor to provide an update and revised plan. Taking an active role to hold management accountable will reinforce the board's commitment to corrective action, and send a message to senior management that resolving audit findings is important.

There are certain instances where management may decide not to take any corrective actions associated with an audit finding. If this is the case, internal audit should document that senior management understands and accepts the risk, and then highlight this to the board.

15. How should Internal Audit deal with concerns of management (and even Board) misconduct?

The CAE is often relied upon as an independent leader, who reports functionally to the board, to help lead or support fraud investigations; this includes concerns involving management and the Board.

Boards should be reminded that although internal audit is responsible for considering fraud when conducting audit work in areas susceptible to fraud and testing the relevant controls, management is actually responsible for preventing or detecting fraud. But what if management itself is involved?

Boards should reiterate the importance of being notified of any activities that indicate management misconduct. This communication is easier when there is open candid relationship between the CAE and Board, fostered by ongoing formal and informal interactions, including in-camera meetings. Furthermore, it is imperative that the Board establish a protocol that protects the CAE and internal audit when sensitive issues or findings are brought to their attention.

When notification is received, the CAE should be asked about the following background details to determine the next steps required:

1. How reliable is the source? Did internal audit observe or detect the misconduct directly?
2. What additional validation (if any), or audit procedures, should be conducted by internal audit?
3. Should internal audit recommend that an investigation be required?
4. Does the behaviour contravene the organization's Code of Conduct?
5. What is the potential nature and depth of the misconduct?
6. What is the role of senior management (or even the board) in the activity (which determines whether IA should bypass management and communicate directly to board or external authorities)?

Once a determination on next steps has been made, internal audit can be leveraged to coordinate investigative activities, contain the flow of information, and maintain privilege, depending on who from senior management is involved in the suspected activity.

Reporting/Communication

16. What content should Internal Audit communicate in quarterly reports to the Board?

Leading internal audit functions present materials and information in a succinct, clear, prioritized manner.

Content should be presented in an executive summary format with themes and trends tied to the organization's key strategies and risk areas. Internal audit functions typically report to the Board on at least a quarterly basis. Items reported can include:

- **Observations and findings:** Significant observations and findings (along with corresponding management action plans to remediate the findings) from completed internal audits should be prioritized and reported at the Board level. This should extend beyond exceptions, as the Board should be asking for assurance that key activities are operating as intended, controls are designed well and risks are reasonably managed. The progress of management action plans associated with prior high risk observations and findings should also be reported when they become past due.

- **Performance metrics/balanced scorecard:** It is important to understand internal audit's mandate and objectives, and how they are performing relative to them. Internal audit should report on metrics that are aligned to their mandate at each board meeting. Leading internal audit functions take a balanced scorecard approach, reporting on performance against the audit plan, internal audit practice management, people development, and stakeholder expectations.

- **Risk assessment, internal audit plan, and resource requirements:** Internal audit is responsible for presenting a risk-based internal audit plan to the board that sets out the function's priorities and assurance coverage across the organization, as well as the resources required to complete the plan. The audit plan should also include any anticipated advisory or consulting engagements. The Board is required to approve the plan and the associated resources. Internal audit often provides insights into other assurance and risk management activities across the organization to provide a broader perspective on assurance over key risks across the organization.

- **Practice management initiatives:** Practice management refers to all activities that internal audit undertakes to execute its mandate and continuously improve as a leading assurance function. This includes scheduling and planning, implementing audit software and technologies, training and development, and hiring/resourcing.

- **Management requests:** Internal audit is frequently asked to support management, either in an advisory capacity or by providing assurance in a traditional internal audit model, to help respond to frauds, quality failures, health and safety incidents, mergers and acquisitions, divestitures, and other situations that arise throughout the year that put a strain on management's resources. Before undertaking any action on such management requests, internal audit should consider the relative risk of the issue and the impact on its audit plan to undertake the request. It is helpful for the Board to be aware of these activities.

- **Whistleblower activity and potential management misconduct:** Internal audit is often responsible for administering certain whistleblower activities, including receiving and escalating complaints to the appropriate authority, which includes the Board for more serious accusations.

- **Quality Assurance:** IIA Standards require external assessments of the IA function to be conducted at least every five years, and internal reviews to be conducted at least annually. They also require the CAE to report on the results of quality assurance activities associated with IA function to the Board.

Independence is a consideration in ensuring that the required information gets reported to the board. It is important to talk about independence with the CAE, letting her or him know that the Board should be informed if they are ever placed in a position where senior management is attempting to inappropriately influence what is being reported.

17. How does Internal Audit determine what risk and control issues should be reported to the Board?

Judgment is required in order to determine whether a risk exposure or control issue is significant enough to warrant highlighting at the Board level and this is why the establishment of criteria is critical.

The Board should work with the CAE to establish criteria to provide guidance on what the IA function should report to the Board. As a starting point, the criteria should comply with IIA Standards, which state that significant audit findings, such as risk exposures and control issues, including fraud risks, should be reported. Judgment, however, is required in order to determine whether a risk exposure or control issue is significant enough to warrant highlighting at the board level and this is why the establishment of criteria is critical. The following are three categories of findings/developments that are typically reported to the Board:

1. Issues that result in residual risks that exceed the organization's stated limits for risk taking
2. Issues that relate to management failing to report on an inability to achieve organizational performance goals
3. Matters of organizational integrity (fraud, ethical behaviour, social responsibility and social license to operate, etc.)

Criteria for escalating audit issues should reflect the board's priorities and preferences. The board should be satisfied that internal audit applies the framework consistently, free from any influence or pressure from management or external third parties.

18. Effectively utilizing the in-camera session. "Are there any other matters that you wish to bring to the Board's attention?"

The CAE must use professional judgment to determine both "what" and "how" to succinctly communicate sensitive information in the in-camera session. This can also be a great opportunity to make sure the Board has clearly understood matters of high importance.

It is important to leave time in each Board meeting to give the CAE, and the internal audit team, a forum (i.e. an in-camera session) to discuss any items that may not have been presented in the pre-read materials or in the meeting itself. Sometimes issues arise within days of Board meetings that warrant discussion in meetings. There may also be certain items that the CAE does not feel comfortable including in the formal meeting materials. If the agendas of the meetings get sidetracked, delayed, or compressed, this question serves as a nice reminder to address anything that may have been skipped over. This single question is a simple, powerful way for Board members to uncover learnings that may be "between the lines" of an internal audit report.

Evaluation of the IA Function

19. How should the Board evaluate the Internal Audit function?

IIA Standards require that Internal Audit departments undergo an external quality assessment every five years.

Boards should continually evaluate their internal audit functions in order to enhance the department and to improve on its future performance (and this role should be included in the Audit Committee Charter). In addition to considering their own views, the Board's assessment of internal audit should take into account the perspectives of management, the business units that have been audited and also the CAE. Recommended practices to evaluate internal audit include:

- **Board level metrics**—develop quantitative key performance metrics (for example, audits per year, annual audits per headcount, % time spent on an audit versus budget, etc.) to measure the IA functions performance.
- **Management evaluation**—obtain managements views on IA's performance (for example, does IA understand the business? does IA have the necessary skills and experience to provide value added advice to the business? were audit results appropriately communicated to management? were audit recommendations practical?).

- **Internal Audit self-assessment**—ensure that your CAE is monitoring quality within the department (for example, are audit working papers reviewed? are internal quality reviews of audit engagements performed? are client satisfaction surveys obtained?).

- **Results from external quality assessments**—IIA Standards require that Internal Audit departments undergo an external quality assessment every five years. Boards can gain valuable insights from these reviews about the performance of their IA departments (including, an independent assessment that their IA function is complying with globally recognized standards, comparison of performance to that of peer organizations, assessment of reporting structure/people/skills, review whether IA's processes and practices are aligned with what the Board expects).

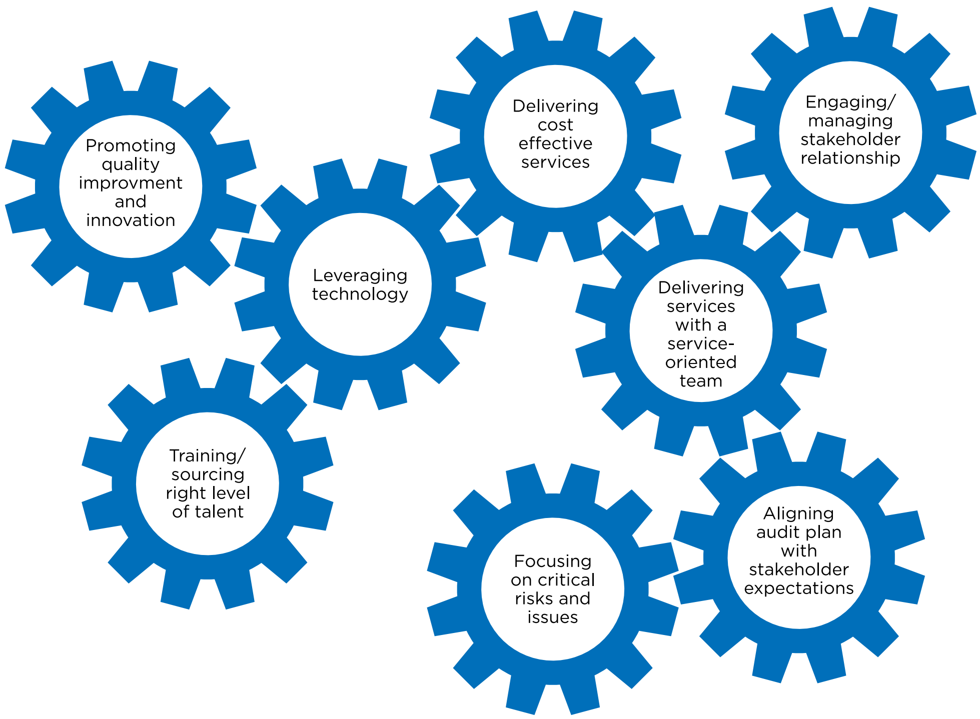
- **Results from client surveys**—Internal Audit functions should conduct surveys of the business units that are audited after every engagement. Results from these surveys can not only assist the Board in assessing internal audits performance but can also serve as the basis for improving the future effectiveness of the department (for example, were findings and recommendations appropriate and/or value-add, were reports well written/organized and easy to understand, was communication coordinated).

20. Is Internal Audit continually following industry leading practices?

Your Internal Audit department should be as dynamic and nimble as your organization, and should always be looking for high value continuous improvement opportunity.

If your board is providing governance and oversight for significant external and/or internal change, then the Internal Audit activities must be equally agile. Boards should be satisfied that internal auditors are receiving timely and relevant training and education that will equip them to provide their services in accordance with the applicable requirements. CAEs should be able to demonstrate to the Board that their team's skills map to their mandate.

Further to maintaining or obtaining adequate skills, board members should ensure that Internal Audit understands and is integrating evolving audit practices into its department. Performance areas that boards should examine within Internal Audit include:*



*** Source:** *PwC State of the Internal Audit Profession*

Boards should inquire about how Internal Audit is instilling a forward-looking, strategic plan to evolve the practices they follow.

Conclusion

Many internal audit functions have increased their profile within their organization by evolving their capabilities to deliver greater strategic value (with the definition of value being defined by key stakeholders, including the board, audit committee, executive line management, and other risk focused functions within the organization). This evolution required an approach whereby the scope of its assurance coverage is strongly aligned to the strategic objectives and considers the key risks that could inhibit their organization's success. The continuing ability to engage stakeholders to create a productive dialogue, produce intelligent findings, and issue reports that are appropriate to their intended audience is essential to the future success of any Internal Audit team.

In conclusion, Boards should encourage:

- Your CAE to design and manage its Internal Audit department to deliver objective assurance, as well as provide valuable recommendations that help their organization to achieve strategic objectives while effectively and efficiently addressing relevant risks.
- Your Internal Audit departments to be designed to be strategic, agile, informed, collaborative, and capable. Relationship management and communication skills should carry equal weight to technical auditing capabilities.

Where to Find More Information

CPA Canada Publications on Governance
(available at **www.cpacanada.ca/governance**)

The Director Series

The 20 Questions Series

- 20 Questions Directors Should Ask about Building and Sustaining an Effective Board
- 20 Questions Directors Should Ask about CEO Succession
- 20 Questions Directors Should Ask about Codes of Conduct (2nd ed)
- 20 Questions Directors Should Ask about Crisis Management
- 20 Questions Directors Should Ask about Crown Corporation Governance
- 20 Questions Directors Should Ask about Director Compensation
- 20 Questions Directors Should Ask about Directors' and Officers' Liability Indemnification and Insurance (2nd ed)
- 20 Questions Directors Should Ask about Executive Compensation (2nd ed)
- 20 Questions Directors Should Ask about Governance Assessments
- 20 Questions Directors Should Ask about Governance Committees
- 20 Questions Directors Should Ask about Insolvency
- 20 Questions Directors Should Ask about Internal Audit (2nd ed)
- 20 Questions Directors Should Ask about IT (2nd ed)
- 20 Questions Directors Should Ask about Responding to Allegations of Corporate Wrongdoing
- 20 Questions Directors Should Ask about the Role of the Human Resources and Compensation Committee

- 20 Questions Directors Should Ask about Special Committees (2nd ed)
- 20 Questions Directors Should Ask about Strategy (3rd ed)

Director Briefings

- Board Oversight of Tax Risk — Questions for Directors to Ask
- Controlled Companies Briefing — Questions for Directors to Ask
- Diversity Briefing — Questions for Directors to Ask
- Guidance for Directors: Disclosure and Certification — What's at Stake
- Guidance for Managers: Disclosure and Certification — What's at Stake
- Shareholder Engagement — Questions for Directors to Ask
- Sustainability: Environmental and Social Issues Briefing — Questions for Directors to Ask

Frameworks

- A Framework for Board Oversight of Enterprise Risk
- Overseeing mergers and acquisitions — a framework for boards of directors

CFOs

- Deciding to Go Public: What CFOs Need to Know

About the Author

Bruce Webster

Partner, Internal Audit Services
PwC LLP

Bruce leads PwC Canada's National Internal Audit Practice. He provides advice and assistance to public sector entities as well as public and private companies dealing with internal audit, risk management, governance and compliance issues.

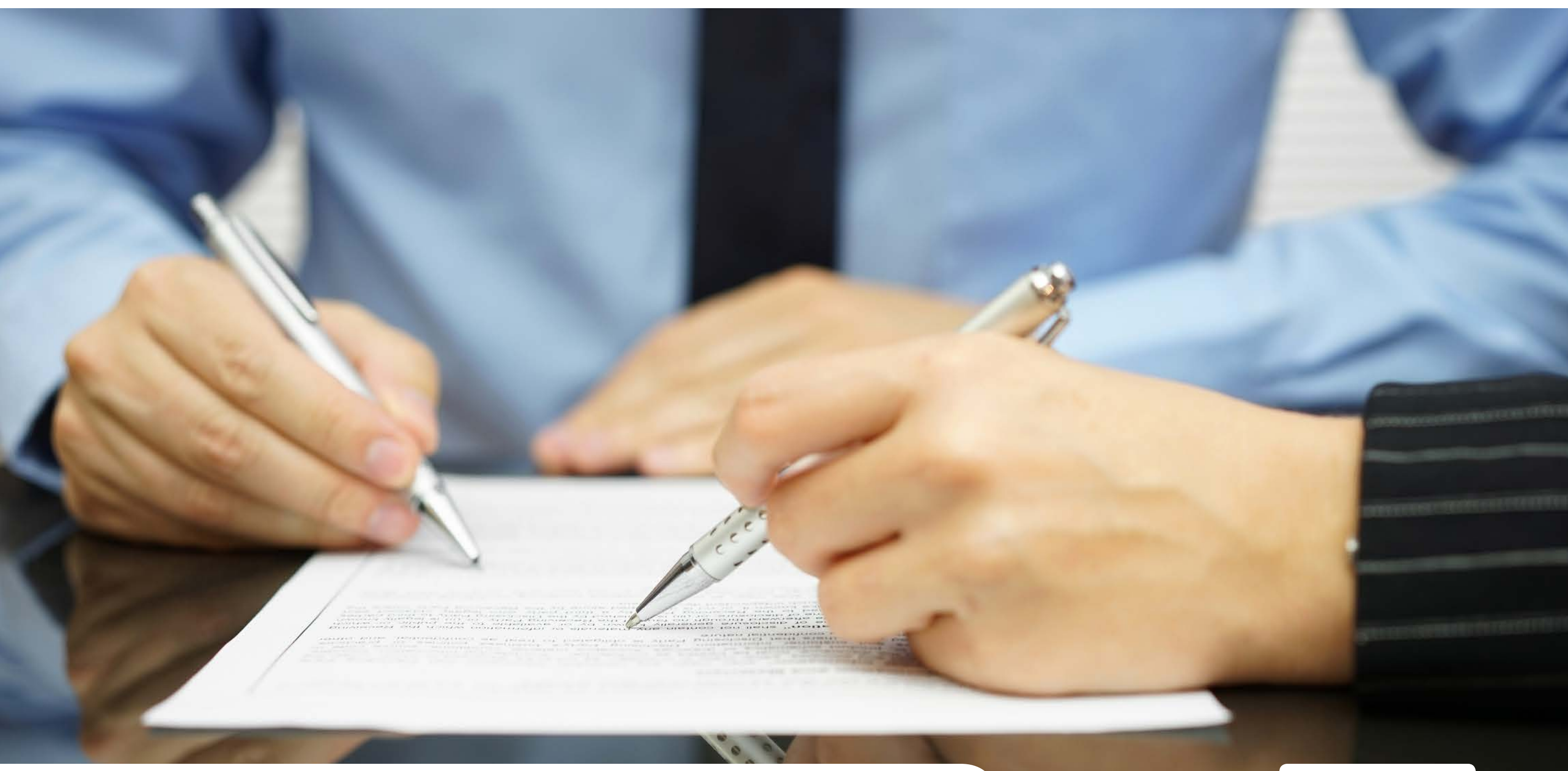
Bruce's internal audit responsibilities involve directing and managing a range of assignments including: acting Chief Audit Executive, internal audit full outsource and co-sourcing mandates, project based internal audits; enterprise wide risk assessments and transforming the results into risk-based strategic internal audit plans; performing external compliance reviews of the internal audit function; performing testing for internal controls certification; and reviewing internal control systems following a control breakdown to assess the manner in which controls were circumvented.

Bruce has been involved in the preparation and presentation of numerous professional development seminars to clients, associations, and in-house.

Bruce's education and memberships include:

- Bachelor of Commerce, McMaster University, 1986
- Chartered Accountant, 1989, Member of The Canadian Institute of Chartered Accountants (CICA) and Member of The Institute of Chartered Accountants of Ontario
- Certified Fraud Examiner, 1993, Member of the Association of Certified Fraud Examiners

- CAIFA, 2000, Qualified as one of the inaugural CICA CA-designated specialists in investigative and forensic accounting
- Certified in Financial Forensics, 2014, AICPA
- Board member of the CICA Alliance for Excellence in Investigative and Forensic Accounting (2000–2007)
- Member of the CICA Certification Committee for the Alliance for Excellence in Investigative and Forensic Accounting (2007–2014)
- Member of the Institute of Internal Auditors (IIA)
- Governor for the Toronto Chapter of the IIA



CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA

ISBN-13: 978-1-55385-977-2
9 781553 859772
04000086