Internal Audit Hot Topics

The Internal Audit & Risk Agenda 2024

IDEAS | PEOPLE | TRUST

Contents

01

The internal audit and risk agenda: Welcome

The internal audit & risk agenda

Welcome

2024 looks to be another year of permacrisis with significant geopolitical disruption continuing. Most of the world's major economies are undergoing elections in the coming year and the conflicts in Ukraine and the Middle East continue to impact the global economy. Organizations that are only just beginning to recover from the disruption of three years of pandemic face further uncertainty in respect of inflation, interest rates, energy supply costs, and talent shortages.

Dependency on technology has increased even though cyber threats are higher than ever. Despite this, digitalization is driving business transformation and recent developments in artificial intelligence (AI) and blockchain present new opportunities for innovation but these carry a heightened level of risk. Cyber, privacy, and digital transformation risks are understandably high on the audit committee agenda.

Non-financial data is taking on a much higher profile with reporting obligations and stakeholder requirements being extended to compel disclosure of ESG performance and responses to climate change risks. Additionally, The Securities and Exchange Commission introduced rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.

This has required organizations to introduce new systems and controls to ensure that this data will stand up to stakeholder scrutiny. Regulators have sought to keep pace with these changes - introducing new legislation and disclosure requirements that need to be complied with.

Expectations of internal audit remain high with demand for assurance expanding to cover a wider range of areas than ever before. Alongside the traditional controls knowledge and softer skills essential to the role, internal auditors now need to enhance their understanding of governance and regulatory requirements and to develop their technical knowledge of information technology, data analytics, program and project management, business resilience, and ESG.

The new global internal audit standards reflect this and look to raise the bar by making actions that were previously good practice into mandatory requirements for high-performing internal audit functions. In addition to this, the new standards now include the audit committee's responsibilities for the first time. Heads of internal audit need to work with their committee chairs to make sure these are understood and addressed.

Internal audit, therefore, has a key role to play in supporting organizations to navigate a path through this uncertain and changing risk landscape. This document sets out some of the key challenges on the horizon that heads of internal audit should be considering when thinking about the wider risks relevant to their organizations, and the technical skills required to deliver meaningful assurance.

As we enter into another challenging year, the internal audit profession can continue to show its value by demonstrating its depth of understanding and breadth of business knowledge by getting to grips with the many new and challenging areas for assurance.

Gavin Hayes | Head of Policy and Public Affairs | Chartered Institute of Internal Auditors

02

Hot topics

Artificial intelligence

Providing assurance over AI

Using the term artificial intelligence to describe certain types of automation has become increasingly popular. However, when an organization is genuinely using AI, how do we, as internal auditors, properly assess the risk and deliver a valuable internal audit report?

Organizations that are leveraging AI are looking to govern it as comprehensively and responsibly as possible, and where practicable, in line with their jurisdiction's AI governance framework. For example, in April 2024, the EU AI Office and the U.S. AI Safety Institute have made a commitment to work together on tools to evaluate artificial intelligence models. The United States and the European Union are taking a risk-based approach to manage emerging technology risks, while advancing safe, secure, and trustworthy AI technologies. Canada is also working on an AI and Data Act, which is overseen by the Ministry of Innovation, Science and Economic Development, and the Office of the Privacy Commissioner of Canada.

When a framework for the use of AI is created at an organization, it should define the policies, processes, and controls necessary for responsible AI deployment, whilst being future-proofed to take into account future regulatory movements as well as the ethical use of AI.

A potential risk in the usage of AI is the lack of clarity and transparency within AI models that facilitate their decision-making processes. A focus on the risks associated with these topics, and the ongoing monitoring/tweaking of the AI model could feature in most audits of an organization's AI technology.

A related risk will be legal compliance and copyright infringement risks, based on what inputs are used within AI models.

Linking to another one of our hot topics in internal audit in 2024 is the concept of cybersecurity controls associated with AI technology. Consideration should be given as to the nature of sensitive data being inputted into AI tools (e.g. sensitive personal data, or confidential corporate data/earnings, etc.; and where the data goes after it is submitted to an AI tool), as well as how well protected the AI environments are from external cyber threats, and ongoing patching and vulnerability management.

Internal audits over AI, as well as technology concepts within the wider realm of AI (e.g., machine learning), will vary from organization to organization, as the levels of maturity are certain to vary greatly based on industry, country, and the technology being used. Internal audits need to be tailored given the number of variables at play to avoid a mismatch in applicable AI risks and coverage by the internal audit plan.

Despite this, as a starting point, the recently released ISO/IEC 42001:2023(E) provides a base level of expected controls and risks to be managed when using AI.

Additionally, the E.U. AI Act provides an official framework for the use of AI. The organizations within the Act's scope will be providers, importers, and distributors of AI systems or general-purpose AI models that are placed on the E.U. market, put into service, or used in the E.U.

Artificial intelligence cont.

Using AI to provide assurance

Internal Audit functions themselves are similarly identifying methods to leverage AI in a beneficial way – in some cases increasing efficiencies and being able to arrive at insightful recommendations and insights that would not have otherwise been feasible with a standard/manual approach.

One such method is in the way of predictive analytics and machine learning. By partnering with other lines of defence, internal audit can identify methods to implement real-time predictive analytics to identify – for example – software changes that are more likely to introduce a problem or incident in the live environment. This identification can be based on a range of factors such as the size of the change, the time of day it is deployed, the software package, the IT or end users involved, and a history of previously deployed changes, to name a few.

Just as transparency is a key concept to be cognisant of in leveraging and interpreting information that is subject to an internal audit, it is equally important to perform checks to confirm the validity of data generated by an AI tool being used to partner with the auditors to complete an engagement.

Continuous monitoring and machine learning can be useful audit tools to analyze historical data, which may lead to the ability to detect trends that human analysis might overlook.

AI can be a hugely beneficial tool to work alongside human internal auditors, provided the appropriate guardrails and other ethical considerations are taken into account. The integration of AI tools within an internal audit department can provide more in-depth insights to stakeholders as well as improve the efficiency and accuracy of audit procedures. By embracing AI, internal audit can align with the dynamic requirements of modern business.

Corporate governance in Canada

Canada's evolving disclosure landscape

The disclosure landscape for Canadian public companies is undergoing an expanded focus on diversity and environmental, social, and governance (ESG) reporting. While the substance of Canadian Securities Regulators' continuous disclosure requirements remains consistent with past years, Canadian regulators have signalled that additional reporting is near. Public companies will soon need to augment their reporting with information on their nominating processes as they relate to board renewal and improving board diversity.

In addition, public companies will likely soon have to report climate disclosures. Canadian regulators have previously put forward draft guidance under draft instrument 51-107. However, this has been eclipsed by the Taskforce on Climate-related Financial Disclosures (TCFD) recommendations. Canadian and U.S. public company reporting requirements generally converge, and thus, it is anticipated that the TCFD recommendations will become the de facto Canadian standards.

Finally, the Corporate Governance Guidelines of the Toronto Stock Exchange (TSX) delineate the criteria for listed companies regarding board composition, independence, disclosure, and shareholder rights. These standards and guidelines serve to enhance transparency, accountability, and overall governance effectiveness in Canadian corporations.

Approaches to internal controls continue to be influenced by the U.S.

Canadian equity markets include a large number of dual-listed companies. As a result, many of the standards of practice applied in Canada reflect those used in the U.S. While Canadian National Instrument 52-109 is different than the requirements of the Sarbanes-Oxley Act, the approaches to internal controls tend to mirror each other.

While entity-level controls, disclosure controls, process controls, and IT controls continue as perennial elements of all internal control considerations, certain areas are recently attracting more attention. IT controls continue to grow in importance as advances in digitization accelerate. Technology is not only becoming more integrated and complex, but it is moving at a pace that's faster than has been previously experienced, and controls (and our evaluation of controls) is stretched as a result.

In addition, there is increasing attention being paid to the level of precision and detail being incorporated into the evaluation of control systems. Whereas small inconsistencies across issuers and industries may have previously passed muster, regulators and professional service firms alike have raised expectations with respect to the integrity and consistency in the internal control evaluation process.

How internal audit can support

Regardless of the specific measures coming into or out of force, corporate governance and the associated regulatory compliance requirements are fundamentally a question of ensuring robust risk management processes. Internal audit understands this and brings the requisite suite of skills and experience to help clients understand and respond effectively to their regulatory landscape, now and into the future.

Corporate governance cont.

How internal audit can support

Regardless of the specific measures coming into or out of force, corporate governance and the associated regulatory compliance requirements are fundamentally a question of ensuring robust risk management processes. Internal Audit understands this and brings the requisite suite of skills and experience to help clients understand and respond effectively to their regulatory landscape, now and into the future.

Economic crime, whistleblower and anti-bribery and corruption

Companies should have in place a focused fraud risk assessment and have designed and implemented procedures to prevent and detect fraud. This should include a Whistleblower program and policies for fraud and suspected fraud to be reported through to the audit committee. A review of existing arrangements against the Foreign Corrupt Practices Act (FCPA) requirements should be a priority for 2024.

Board performance

Even the best-performing boards should reflect on their own processes, behaviours, and relationships and learn from the failings of others. Regular self-assessment, including board members' appraisal, should be encouraged in between independent reviews.

Data privacy

All organizations process personal data as part of routine operations, while for some it may form part of their core business activities. Canada has revamped its privacy laws further to strengthen privacy protections at the provincial and federal levels. The focus is on bringing Canada’s privacy and data protection laws in line with international data privacy laws, enhancing individuals' rights and protections, and implementing fines and penalties.

Personal data is considered to now be a valuable asset and in the last five years, an increasing number of jurisdictions across the globe have enacted legislation resembling aspects of the E.U. General Data Protection Regulation (GDPR), which have quickly become the expected global standard. As individuals are increasingly aware of their rights in relation to their personal data, this can influence the companies they engage with.

From a risk perspective, the financial penalties for organizations in the event of non-compliance with data protection legislation can be significant. organizations should also be aware of the associated reputational damage arising from non-compliance and the associated negative public perception.

In June 2022, the Canadian federal government introduced Bill C-27, the Digital Charter Implementation Act, which contains newly proposed legislation relating to consumer privacy, data protection, and the first comprehensive laws governing AI systems in Canada. The bill is before the Standing Committee on Industry and Technology and could be passed in 2024, replacing the existing Personal Information Protection and Electronic Documents Act (PIPEDA).

Quebec’s recent legislation, Law 25 (previously known as Bill 64, An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information), brings substantial modifications to the privacy laws governing both the private and public sectors in the province. It is imperative for every organization processing personal information in Quebec to understand the novel requirements and establish suitable processes for compliance.

Finally, the European Commission concluded that Canada (along with 10 other countries) continues to provide an adequate level of protection for personal data transferred from the European Union (E.U.) to recipients in Canada that are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). This is an important decision, as it allows commercial organizations to continue transferring personal information from the E.U. to Canada without additional, burdensome transfer mechanisms such as standard contractual clauses or binding corporate rules.

Data privacy cont.

How internal audit can support

- Internal audit is an invaluable tool to provide audit and risk committees with current levels of compliance while outlining recommendations to support the organization in remedying any gaps in their data protection framework. It is an opportunity to benefit from the knowledge and experience of specialist data protection subject matter experts.
- Data protection audits look at whether an organization has the necessary controls in place to ensure data protection compliance and, if so, whether they operate effectively. This may include, amongst others, checking whether the organization has mapped their personal data flows as well as whether the relevant policies and procedures have been developed and are fit for purpose.
- Internal audit is also a useful tool to determine whether resourcing arrangements are appropriate, to meet ongoing compliance requirements.

Digital transformation

Digital transformation goes beyond simple digitisation and represents a fundamental change to the 'how' an organization's functions through IT-enabled means. Changes of this nature typically present a significant financial investment along with a multitude of business risks, therefore, appropriate for inclusion within an internal audit plan.

Within digital transformations, technology is the enabler for new ways of working that can open up new markets, enable the deployment of new products more quickly/efficiently, improve back-office efficiency, and create data-driven organizations, to mention a few. Internal audit plays a critical role in these transformations by providing assurance at a point in time or throughout the lifecycle of such projects to help identify/mitigate potential risks/failures of the transformation.

Examples of key focus areas that are relevant to most digital transformations include the following:

- Alignment of new technology with operating model changes and strategic objectives
- Program governance, delivery frameworks, and planning
- Requirements and scope definition
- Change management and communication
- Data strategy, migration, and re-platforming
- Testing and validation
- Benefits definition, tracking, and realisation
- Deployment and service transition

A spotlight on the software development lifecycle (SDLC)

SDLC plays a significant role in ensuring effectiveness, efficiency, and reliability of a business's software development processes and is a key area of risk to consider for many digital transformations, as well.

The way in which organizations execute SDLC to deliver value has been a rapidly evolving landscape that has had numerous changes over the last few years. Initially, organizations transitioned from the traditional waterfall approach (performing software development in a manner whereby each stage is dependent upon finalised deliverables from the previous stage) to a more agile software development approach (development of software using cross-functional teams to perform smaller sprints of activity in order to analyze prototypes of code more rapidly and subsequently learn and adapt.) This happened at a similar timeframe to when organizations also tended to remove legacy siloed approaches and instead began to combine software development and operations into DevOps and DevSecOps. organizations have migrated their ERPs and related systems to the cloud, which has accelerated the adoption of an agile and/or DevOps software development approach.

There has also been a shift towards automation through the principle of continuous integration - using pipelines and automated testing to streamline the delivery of updated platforms. This has changed the frequency of delivering software changes in many organizations from the traditional expectation of a few major releases each year to instead entail consistent and frequent smaller releases being migrated to the live environment, on a daily or weekly basis.

Digital transformation cont.

How internal audit can support

Internal audit can be a critical friend throughout the digital transformation's lifecycle, or pinpoint risks and perform audits over these areas when and where necessary. Each transformation will present a different array of risks that will need to be analyzed to determine the most appropriate means of providing assurance to the audit committee. Some examples of internal audits that can be especially relevant for digital transformations and/or a review of SDLC to include the following:

- Digital/IT/data strategy
- IT operating model
- Cloud infrastructure readiness
- Research and development tax credits review
- Transformation readiness
- Cloud migration and data readiness
- Project or program assurance (periodic or continuous)
- Compliance with organizational SDLC policies/standards

Supply chain and commercial risk

Managing your third-party risk and driving better outcomes from supplier contracts across the lifecycle.

With ever more reliance on third parties to deliver business-critical outcomes, alongside the macro-economic, geopolitical, and environmental landscape, businesses are having to navigate an increasingly complex world when it comes to managing risk and driving better outcomes from their third-party relationships across the contracting lifecycle.

The last four years have seen a seemingly relentless set of challenges which have fundamentally shaken global supply chains. Major disruptions including the global pandemic, the war in Ukraine, inflation, and more recently, the instability in the Red Sea, have all highlighted fragilities across global supply chains and driven businesses to re-evaluate strategic supply chain models and governance to build greater resilience across the value chain.

Gaining greater transparency and building resilience and better performance across supply chains are therefore integral to helping organizations succeed. Prevalent supply chain and commercial risk themes include:

Supply chain resilience

Resilient supply chains are able to absorb shocks and quickly respond to new situations whilst simultaneously delivering against operational objectives. Creating robust strategic supply chain plans alongside a robust, ongoing risk management environment including key supplier monitoring/due diligence and sourcing contingency plans will significantly reduce the impact of disruptions and help sustain business operations in the face of global change.

Building an understanding of how financially resilient and stable key suppliers are is a core pillar of providing greater visibility of risks across the supply chain. In addition, understanding the supplier’s own risk exposures (geographical, sector, ownership) puts supply chain management teams at an advantage by enabling greater foresight and proactive issue management.

Contract compliance and performance

Most organizations struggle to realize the value and performance expected from their third-party relationships. As such, value leakage and non-compliance are commonplace. World Commerce & Contracting research has identified that contract non-compliance and wider value leakage cost companies the equivalent of 8.6% of annual revenue.

Reliance on suppliers to manage your reputation and delivery commitments places high importance on ensuring effective and value-focused third-party management. In the current macroeconomic environment, businesses which excel in this area will generate a tangible competitive advantage.

Supply chain and commercial risk cont.

Managing your third-party risk and driving better outcomes from supplier contracts across the lifecycle.

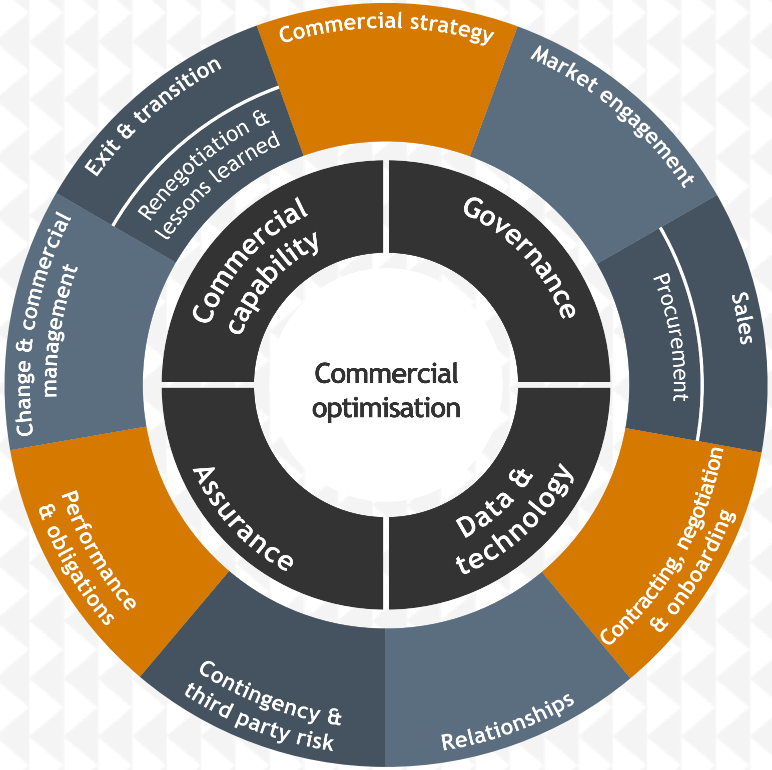
ESG across the supply chain

Managing an organization's ESG impact extends well beyond its own operations. Reliance on third parties also brings supply chain ESG performance into focus, meaning that in order to fully monitor and manage ESG risks, businesses need to incorporate ESG criteria into procurement and sourcing decisions and ongoing supplier monitoring.

Increasing pressure and regulation from governments is on the way. In Canada, the Canadian Parliament passed Bill S-211, An Act to enact the Fighting Against Forced Labour and Child Labour in Supply Chains Act and to amend the Customs Tariff (Act). Businesses that meet certain thresholds will be required to file detailed public reports on measures they have taken to identify, address, and prevent forced labour, prison labour, and child labour in their supply chains. The first report was required to be filed on or before May 31, 2024

This, in addition to broader societal shifts and consumer expectations means that by embedding ESG principles across the supply chain, businesses are not only better able to deliver on sustainability goals, but also enhance their own reputation, viability, and resilience.

Internal audit plays a key role in enabling organizations to enhance and optimize overall supply chain and commercial management outcomes. Overleaf we highlight where IA is well-placed to support the business by identifying and delivering tangible value back into the organization.



How internal audit can support

Internal audit plays a crucial role in supporting the wider business in its supply chain and commercial management functions. Ensuring a robust and effectively operating supply chain and commercial framework has a fundamental impact on the business' performance. IA is well-placed to drive value across the lifecycle including:

- Procurement function maturity assessments
- Strategic sourcing and responsible procurement (ESG)
- Contract and third-party management effectiveness reviews
- Supplier resilience programs
- Contract compliance and cost recovery audits
- Contract exit/transition plan assurance
- Final account settlement support
- Supply chain mapping and risk analysis
- Inventory management assessment and stock counts
- Supply Chain due diligence programs
- Strategic third-party spend reviews

Economic crime

Bribery and corruption remain one of the most common economic crime schemes in North America, resulting in increased losses since the breakout of the COVID-19 pandemic. The pandemic has resulted in changes to businesses from multiple strategic, operational, and financial aspects. These changes present significant risks to existing control frameworks to prevent and detect economic crime schemes. Even though Canadian laws do not criminalize failure to prevent bribery and corruption, the application of the Remediation Agreement has emphasized the importance of an effective control framework.

In Canada, failure to prevent bribery is not an offence under the Corruption of Foreign Public Officials Act (CFPOA) and the Criminal Code. However, in 2022 and 2023, the Canadian courts approved Remediation Agreements (RA) in two cases in response to economic crimes such as fraud and bribery. The application of RA emphasizes the importance of control frameworks. Under the RA, organizations are required to agree with certain internal control obligations and to implement reasonable measures to remediate the control frameworks under a monitoring program.

Despite a general lack of guidance provided by law enforcement in Canada, regulators in the U.S. and the U.K. have published detailed guidance, bearing substantial similarity, on building an effective control framework to prevent bribery and corruption throughout the years. The guidance published by the U.K. Ministry of Justice with respect to the Bribery Act 2010 sets out the six principles for these frameworks. Developing and embedding these frameworks as leading practices provide organizations with the comfort that bribery taken place within any part of their businesses will be identified effectively on a timely basis.

The U.S. Department of Justice (DOJ) Criminal Division also provides guidance in the Evaluation of Corporate Compliance Programs (ECCP), which describes the factors the DOJ considers when evaluating the effectiveness of a company's compliance program. Specifically, in its revision in 2020, the DOJ signals an increasing importance of data analytics. Following this guidance, it is anticipated that organizations need to use compliance analytics as evidence of effectiveness in preventing and detecting noncompliance for their organizations' prioritized risks, including:

i. Use data and technology available to other departments (e.g., sales, HR, marketing, etc.)

ii. Combine compliance data and operational data to consider multidimensional risk analysis

iii. Analyze trends, patterns, and relationships in the data to identify anomalies

iv. Use data as part of ongoing compliance process

v. Allocate resources based on insights created by compliance analytics

Bribery Act 2010 - U.K. Ministry of Justice Guidance
Failure to prevent bribery

Adequate procedures

- Principle 1 – Proportionate Procedures
- Principle 2 – Top-level Commitment
- Principle 3 – Risk Assessment
- Principle 4 – Due Diligence
- Principle 5 – Communication (including Training)
- Principle 6 – Monitoring and Review

Evaluation of Corporate Compliance Programs 2023 - US DOJ Guidance
Factors to be considered for evaluation of a compliance program

Reasonable elements

- Risk-based approach to identify risks and allocate resources
- Training and communications (including commitment by top management)
- Proportionate policies and procedures
- Due diligence on third party relationships
- Confidential reporting and investigation
- Consequent management procedures for non-compliance
- Continuous review of compliance framework

Economic crime cont.

How internal audit can support

- Heads of internal audit will already be familiar with the two earlier failures to prevent offences under both the Bribery Act and Criminal Finances Act and audits in relation to the design and effective implementation of adequate procedures and reasonable procedures and defences should have been taking place for some time.
- With the new failure to prevent fraud offences, heads of internal audit for large organizations within the scope of the act should be ensuring this is high on the agenda of the audit committee and management.
- Fraud is not a new risk consideration for heads of internal audit. IIA Standard 2120 requires that “internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.” They should already have a clear view of their organization’s exposure to fraud and how this is being managed. Previously, organizations’ focus on fraud has been to ensure that they are not victims of fraud, which means financial controls are imperative, however, the new offence relates to the organization benefiting from fraud and will therefore be more aligned with building framework and compliance controls.
- With their experience of helping the organization establish procedures to address legislation such as the Bribery Act in the past – internal audit teams are well placed to support management in establishing the policy, procedures, fraud risk assessment, and monitoring arrangements necessary to meet the requirements of the new Act.

Data visualization

In today’s rapidly evolving technological and data-driven landscape, internal audits are no longer confined to historical number-crunching exercises. In 2023, we saw some significant advancements in how more sophisticated and interactive visualizations are being used to present data, moving from simple charts and graphs. As we navigate through 2024, the symbiotic relationship between internal audit and data visualization becomes increasingly important.

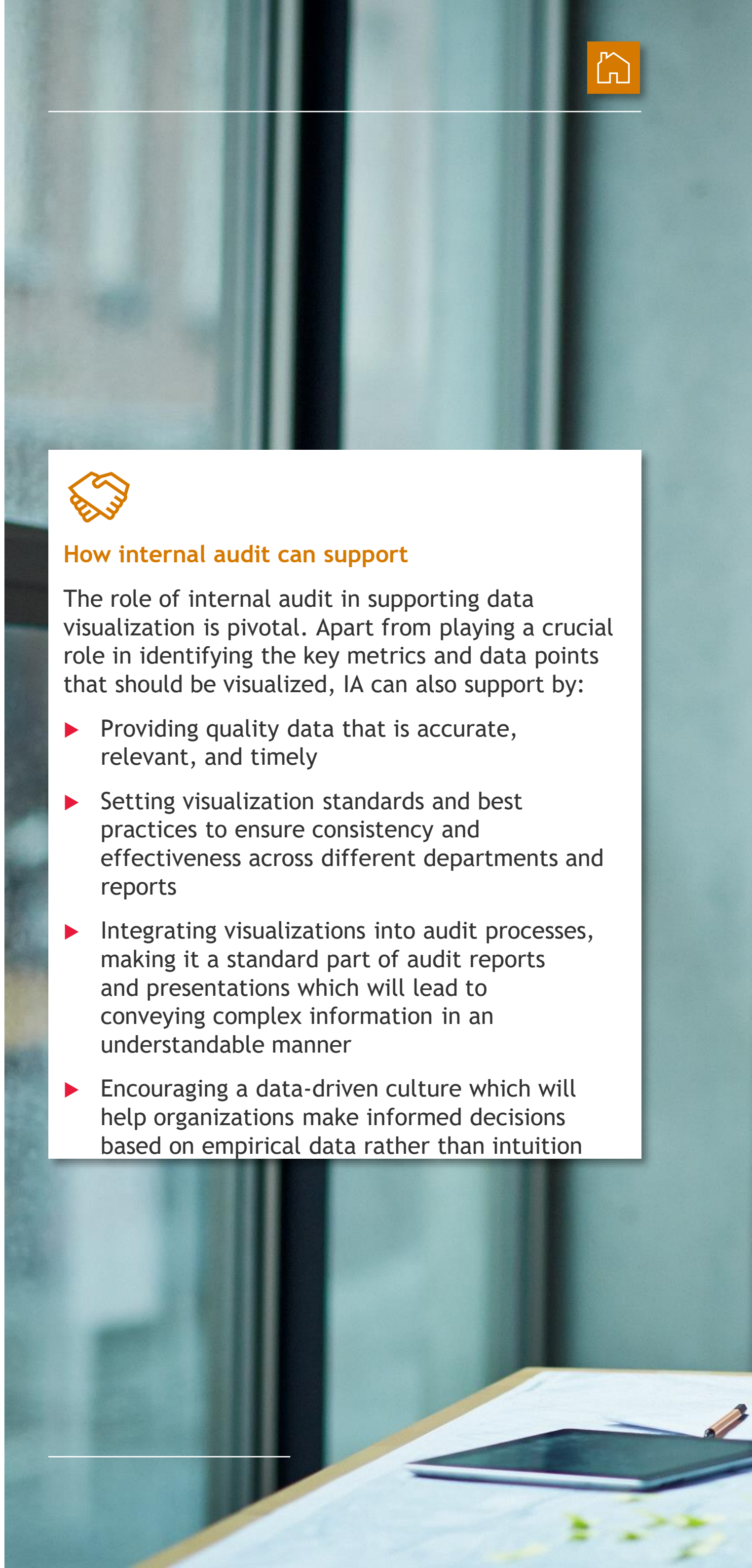
We have seen a substantial leap in how visualization tools now incorporate advanced analytics, AI, machine learning algorithms, and real-time data processing which can be leveraged to allow for a more dynamic, insightful, and user-friendly visual representation of the internal audit reports and presentations.

As we move forward, we must see data visualization beyond mere aesthetics. A powerful dashboard, backed by robust data, not only provides insights on static data but also enables continuous monitoring/real-time analysis of key risks and controls which from an internal audit perspective allows us to proactively identify potential problems before they escalate. This ongoing oversight significantly enhances the audit function.

Moreover, the ongoing oversight that data visualization has to offer is also being seen as a tool to aid communication with non-auditors. Findings and insights gained from internal audits can be presented more effectively through visual means, making them more comprehensible to a wider group of stakeholders. This is particularly vital in translating complex findings to executive management or the board.

An increased use of data analytics and visualizations is also significantly reducing, and in some cases, eliminating the traditional reliance on sample sizes. This paradigm is being re-shaped in several ways since with the advancements of data analytics/visualization tools and techniques, entire datasets can be analyzed quickly and efficiently, removing the inherent risk of sampling errors.

The advancements in the field of data visualization as well as AI have also opened new horizons for internal audit in terms of accuracy, efficiency, and impact. As these trends continue to evolve, they will undoubtedly shape the future landscape of internal auditing.



How internal audit can support

The role of internal audit in supporting data visualization is pivotal. Apart from playing a crucial role in identifying the key metrics and data points that should be visualized, IA can also support by:

- Providing quality data that is accurate, relevant, and timely
- Setting visualization standards and best practices to ensure consistency and effectiveness across different departments and reports
- Integrating visualizations into audit processes, making it a standard part of audit reports and presentations which will lead to conveying complex information in an understandable manner
- Encouraging a data-driven culture which will help organizations make informed decisions based on empirical data rather than intuition

Modern slavery

Modern Slavery has been on the internal audit's agenda since the introduction of the Modern Slavery Act (MSA) in 2015. However, the global occurrence of modern slavery is increasing and remains one of the most serious crimes that have devastating effects on communities and destroy people's lives.

In the last couple of years, geopolitical issues such as the invasion of Ukraine, the conflict in Gaza, and other regional conflicts have all led to devastating effects on humanity and the global economy and have changed lives across the world. The cost-of-living crisis, reduced accessibility to competitive mortgages and increased rents, as well as new challenges post-COVID all have a disproportionate effect on those most vulnerable in our society and as a result, the statistics on modern slavery are on the rise.

Statistics on modern slavery

Unseen, a U.K. charity that provide support for the survivors of trafficking and modern slavery and run the U.K. Modern Slavery & Exploitation Helpline estimates that:

- 50 million people worldwide are in modern slavery
- 28 million are in forced labour
- 22 million people are in forced marriages
- Around 10,000 people in the U.K. are in modern slavery, according to the U.K. Government
- More than 100,000 people in the U.K. are in modern slavery, according to slavery experts (i.e. much more than official figures)

However, the role of business has not changed, and it is fundamental that organizations, whether within the scope of the MSA or not, do all they can to prevent and mitigate all aspects of modern slavery including slavery, servitude, forced or compulsory labour, and human trafficking both within their own organization and their supply chains. There is a clear expectation set out in the U.K. Government's statutory guidance that businesses will aim to improve year on year and that this is reflected within their published modern slavery statements.

How internal audit can support

Internal audit can provide assurance for organizations and their boards that the processes and controls are in place to prevent and detect modern slavery within the organization and its supply chains.

In addition, internal audit can assess that those controls are adequately designed and implemented to meet the expectations of both the Modern Slavery Act itself as well as the good practice set out in the home office statutory guidance – transparency in supply chains and that they are operating effectively.

Change of IIA standards

The greatly anticipated new Global IIA Standards have been released, alongside a report outlining the process followed for developing them, consulting, and responding to the consultation comments.

The release of the new Standards is the biggest change for the profession in over 20 years and over 1,612 consultation surveys were submitted. This number seems relatively low given global membership of over 235,000, although we understand that over a quarter (418) of the surveys were submitted on behalf of organizations and the IIA estimates this represents over 110,00 individuals.

So how does the final version differ from the draft Standards offered for consultation? Firstly, we should reflect there is no substantially new content added to the Standards. The Standards have not become more restrictive, and the changes made are based on the feedback and comments collected as part of the consultation process.

In response to feedback that the new Standards were overly prescriptive, the IIA has reviewed the requirements sections and moved some of the detailed descriptions of how to implement the requirements to the considerations for implementation which provides guidance on common methods, but which is not mandatory to adopt. We also note that the use of ‘must’ has been toned down throughout the final version.

In relation to the performance of external quality assessments, we are pleased to see some of the requirements for external assessors, such as requiring them to obtain the IIA assessor qualification, have moved to the considerations for implementation. We note the requirement that at least one person (on the assessment team) holds an active Certified Internal Auditor designation, which is welcomed.

The IIA has recognized the challenges faced by smaller internal audit functions and those operating in the Public Sector and reflected on these in the newly titled ‘Fundamentals of the Global Internal Audit Standards’ section, alongside incorporating a new section ‘Applying the Global Internal Audit Standards in the Public Sector’.

The IIA responded to multiple concerns raised over the Standards’ requirement for non-certified internal auditors to obtain at least 20 hours of CPE annually, and this has been removed, now reflecting that “practicing internal auditors who have attained professional internal audit certifications must follow the continuing professional education policies and fulfil the requirements applicable to their certifications.”

The key changes introduced by the new Standards are not new concepts for high-performing internal audit functions and include:

- The introduction of the purpose statement for internal audit to assist auditors and stakeholders to understand and articulate the value of internal audit.
- Development of an internal audit strategy (including a vision) that supports the strategic objectives and success of the organization.
- Formal internal audit performance objectives and measures to evaluate functional performance, which needs to be approved and monitored by the board.
- Internal audit methodology requirements related to identifying root causes, prioritizing findings, developing engagement conclusions, and communicating themes.

Probably the largest change between the consultation draft and the new Global Standards is to Domain III: Governing the Internal Audit Function, where a new section has been added requiring the chief audit executive to meet with senior management and the board to discuss the Standards and clarify roles. The requirements for the board have also been changed to ‘Essential conditions’ with supporting information on how to address disagreements and non-conformance.

Change of IIA standards cont.

What does this mean for internal audit and what should you do?

- Plan your response. The Standards become effective on 9 January 2025, so use this time to plan how you are going to comply accordingly.
- Utilise the free resources available to you, the IIA is hosting a series of webinars:
  - Get to Know the New Global Internal Audit Standards
  - What the New Standards Mean to Quality Assessments.
- If you are having an external quality assessment in 2024, take the opportunity to incorporate a gap analysis against the new Standards to support your team's transition.
- Watch out for the mapping of the 2017 Standards to the 2024 Standards, coming soon from the IIA.
- Have you documented your internal audit strategy and methodology? These are both required under the new Standards.
- When reviewing your procedures, processes, and methodologies against the new Standards, take the opportunity to reflect on how you operate in practice and think about whether different approaches may be better or more effective.
- Chief audit executives should engage with (and educate) the board and chair on the content of the new Standards and enhanced responsibilities of the board. This is a requirement of the new Standards.

Cyber risk

Cybersecurity has, and will, consistently feature as one of the most dynamic and evolving risks that is assessed in many organizations' annual internal audit planning exercises (it has been voted the number one risk for the last five years in the CIIA annual risk in focus survey).

Organizations are using additional technology and means of automation than previously, such as Robotic Process Automation (RPA) and artificial intelligence (AI), potentially creating new cyber risks in the process. New mandatory requirements are being set in E.U. legislation such as the Digital Operational Resilience Act (DORA), the NIS2 Directive, the Data Act, and the Cyber Resilience Act.

Critical information assets (crown jewels) need to be well protected with defensive, monitoring, and recovery controls strengthened as far as possible. Internal audit should assess their audit plans to determine whether the audit plan will be sufficient to meet the needs of the audit committee and the organization during this period of heightened risk, rapidly emerging technologies, and new regulations.

The skill sets and sub-specialisms that are required by internal auditors and any SMEs that they bring to partner with them on cybersecurity internal audits are constantly evolving as well, in line with the changing nature of threats by cyber threat actors and changes to technology.

An alignment between internal audit teams and in-house IT security teams is becoming more commonplace in some organizations to leverage their respective expertise. This collaboration can help internal audit functions to become closer to the range of cybersecurity risks and the current state of any remediation and help ensure that audit activities align with the rapidly evolving technology landscape. The closer collaboration can also help internal audit teams to become closer to the detailed cyber risks, and help them with risk quantification of such risks, which may help to avoid a scenario whereby every cyber internal audit report receives a high rating, which may lead to fatigue from the audited parties.

Given the heavy reliance on third parties, including cloud providers and software-as-a-service providers, cybersecurity across the entire supply chain is also a focus area that we have observed with our clients. Internal audit's role is expanding in these interconnected environments to consider cybersecurity risks and controls both within the primary organization as well as the cyber security posture of any supplier that it relies upon.

As organizations continue to navigate changes to cybersecurity risks, the more recent trends indicate a shift toward proactive, collaborative, and technologically advanced approaches.

How internal audit can support

Internal audit can provide assurance and advisory services to the first line of defence in a variety of ways in order to help enhance the cybersecurity controls environment, including:

- Penetration testing
- Information security
- Cyber maturity assessments and threat modelling
- Cyber resilience, recovery, and wider business continuity
- Cyber regulation and compliance (including DORA, ISO, PCI, Cyber Essentials, etc.)
- Frequent/continuous vulnerability assessments
- Supply chain security
- Cloud security
- Incident and crisis response simulations
- Privileged access management, identity governance, and cloud access governance
- IT Security awareness education

ESG (Environment, Social, and Governance)

ESG is a mechanism to quantify and report on an organization's sustainability efforts and goals, and is increasingly important to internal and external stakeholders. This is because embedding sustainable business practices and ESG within the organizational strategy creates value, protects value, and manages risk. To achieve this, it is critical to understand what sustainability and ESG mean in the context of the organization and its mission.

2023 saw an increase in regulatory reporting requirements across the globe and the launch of the International Sustainability Standards Board's (ISSB) global sustainability standards, following the aim to increase the consistency and quality of ESG reporting, to focus on material sustainability risks and opportunities and address greenwashing concerns.

The trend of increasing regulatory and reporting requirements is expected to continue for the foreseeable future alongside an increasing demand for assurance over non-financial disclosures to add credibility to disclosures.

For organizations to create and protect value and to be able to communicate effectively, ESG should not be considered as a year-end reporting requirement but be embedded within business-as-usual activities and decision making.

Key considerations to achieve this include:

- Which ESG topics represent the greatest potential risk or opportunity to the organization and its long-term success?
- Have clear ESG and sustainability objectives and targets been set and communicated across the organization?
- Are climate and sustainability risks integrated into wider risk management activities? Have key risk indicators been identified?
- Are there robust processes, controls, and systems in place across each of the ESG priority areas?
- Is quality data readily available to enable performance to be monitored?
- Is ESG reporting transparent, balanced, credible, and fair? Does it focus on the material ESG risks to the organization's enterprise value?

ESG cont.

How internal audit can support

Internal audit has a key role to play in understanding and robustly assessing how ESG topics impact the organization's risk landscape over the short, medium, and longer term. ESG considerations and priorities should be built into assurance maps, considering the internal audit effort alongside the organization's wider assurance landscape. Specifically, internal audit can:

- Review and challenge the approach taken to identify the ESG topics which present the greatest risk to the organization, considering the extent of stakeholder engagement (internal and external).
- Throughout all internal audit work, consider how sustainability and ESG objectives are integrated across the organization, considered in decision making and risk management, and supported by an appropriate tone from the top.
- Undertake internal audit reviews focused on ESG priority areas to provide assurance over the processes and controls in place to manage the risks and exploit the opportunities. Internal audit reviews can also support organizations in preparing for independent third-party assurance over non-financial metrics
- Provide assurance over sustainability reporting, considering alignment with regulatory requirements and whether claims made are transparent and appropriately supported. There continues to be a focus on greenwashing which presents a reputational risk. Whilst there remains the ability for organizations to pick and choose what they report, internal audit has a role to play in challenging whether the content of reporting is aligned with the greatest risks to the organization and whether there are robust controls in place to prevent greenwashing or misleading and inaccurate statements. Internal audit should consider:
  - Are topics excluded material by omission?
  - Are topics and metrics included as good news stories which have limited impact on the organization's strategy or success?

Geopolitical risk

With geopolitical risk and uncertainty escalating in recent years, risk management and internal audit functions must recognize the increasing need to more closely monitor the potential impact of political, economic, and social factors on an organization's operations and investments.

Geopolitical risk can arise from a variety of sources, including changes in government policies, civil unrest, terrorism, natural disasters, and international conflicts. To respond to such swiftly changing conditions effectively, organizations need to take both a proactive and reactive approach to mitigating this risk.

With many geopolitical experts predicting 2024 to be the most dangerous and uncertain year from a global political perspective, we consider the dominant themes to keep abreast of below:

- **Continued economic uncertainty:** Operating in a subdued growth environment, affected by high interest rates and geopolitical events impacting consumption, investment, and trade trends. Coupled with a shifting labour market, this will continue to bear higher costs for businesses.
- **Military conflict:** The ongoing conflicts in Ukraine and Gaza, and tension in the South China Sea and Taiwan put key regions under further strain and potential for spillover into broader regional escalation.
- **Climate change:** The El Nino climate pattern will highlight the increasing vulnerabilities connected to climate change, and it and other natural disaster events will increase water stress, disrupt logistics, and lead to reactive policies directly impacting businesses.
- **Political regime change:** Key elections in the United States, the U.K., across Europe, India, Indonesia, and others will bring risks and opportunities as key policies shift and businesses face changing industrial policies and trade.
- **AI governance:** Breakthroughs in artificial intelligence outpace governmental efforts to regulate it. This bears risk of how AI augmentation affects labour forces, as well as its role in intensifying the likelihood and impact of cyber attacks.

Internal audit and risk management functions play a key role in building awareness around geopolitical risk and how it is mitigated, and clear guidance from boards will shape and enable assurance efforts.

Key considerations for promoting an effective approach to managing and auditing geopolitical risk include:

- Who bears the responsibility for identifying and mitigating geopolitical risk within the organization?
- How is geopolitical expertise prioritized and deployed across the organization's assurance coverage?
- What role does risk management have in driving geopolitical risk recognition via risk registers or risk assessments?
- If the organization operates across different jurisdictions, what is the strength of relationships with local stakeholders (governments, communities, suppliers)?
- Is the business (first line) aware of available geopolitical specialist expertise to draw on for strategic decision making?
- What MI and external data is readily available to guide swift decision making in relation to geopolitical risk?
- How will geopolitical risk be considered across all lines of defence to emphasize a holistic impact on the business and link back to strategic decision making?
- What contingency plans are or can be put into place to respond effectively to crystalized geopolitical risk?

Geopolitical risk cont.

How internal audit can support

Given the global escalation in geopolitical instability and the complexity of consequences, direct and indirect, internal audit can play an important role in helping organizations understand where to focus assurance.

A key starting point is to assess the organization's exposure to geopolitical risks and evaluate the effectiveness of the risk management strategies in place (reviewing key risk management policies and procedures, assessing the effectiveness of risk assessments, and evaluating the adequacy of the overall risk management approach and strategies).

Internal audit can review business continuity plans to ensure that they address potential geopolitical risks and that they are regularly tested and updated. Another key area for internal audit to review is the organization's compliance with relevant laws and regulations related to geopolitical risks, such as sanctions and export controls.

More broadly, to effectively audit geopolitical risk, internal audit needs to have a good understanding of the organization's operations and how exposure to geopolitical risks may impact them. This may involve research on political and economic developments in the regions where the organization operates, as well as consulting with subject matter experts both within and outside the organization.

People

A new horizon for workforce risk audit approach.

IA and HR professionals must look beyond traditional scope and metrics, such as staff retention and turnover, and take a broader view, focusing on mitigating the impact of intersecting human capital risks rather than trying to minimize the scope.

From a risk perspective, our quantitative and qualitative research has found that retention (47%), contingent worker arrangements (43%) and recruitment challenges (41%) are the leading human capital risks in a year.
For HR professionals to deal with these risks proactively, the intersecting risks that magnify these main challenges must be examined.

To move towards a risk-welcoming, risk-multiplier approach and succeed in this new operating environment, HR professionals must take a more holistic approach and collaborate with people across the business to understand how multiple risks affect hiring and retention. Few organizations bring together expertise from across the organization to help understand and manage risk multipliers.

Five main hot topics are vital to operating in a risk-welcoming landscape, all of which can be applied by IA professionals to manage human capital risks proactively with their HR counterparts.

Number one is the agility of mindset across leadership and the organization—if you do things the same way, why would you expect a different outcome?

The second one concerns connectivity and a clear understanding of organizational risks. Not everybody needs to be an expert on internal audit methodologies, but everybody needs better people risk awareness.

Culture is vital, so the tone from the top, psychological safety around reporting (concerns), the ability to have forums where you have discussions, and then technology as something that can drive the pace of response (to risks).

Technology is an enabler, rather than the cart that goes before the horse. The focus on data and measurement that is enabled by HR technologies - aligns well with the overall risk concepts of data-driven objectivity and transparency and opens new risks but also new opportunities.

Managing proactively reputational risks means HR professionals must consider how their organizations remain attractive to potential employees. The reputational risks intersect with other risks that can hinder recruitment, such as the effects on the talent pool of changing demographics and evolving attitudes to issues including climate, human rights, and social responsibilities.
The great resignation wave created a new risk: the overheated recruitment market. The perfect storm of insufficiently trained people and the urgent need to recruit made a lopsided situation of multiple risks where people demanded higher pay; some accepted more junior roles, while others took jobs beyond their experience.

In a market where employees, suppliers, and contractors are more discerning about where they choose to work, a company’s social capital and reputation for ethical behaviour become fundamental factors in its ability to meet its hiring needs.

Improving working capital

Following 14 consecutive increases to interest rates, the bank rate is at its highest level for 15 years. This increases the cost of funding for businesses and elevates the need to focus on effective management of cash and working capital.

From historic lows, there has been a significant risk in interest rates since 2021 to respond to high rates of inflation. This has impacted consumers, such as energy bills, the cost of food, and mortgage interest rates all increased.

The future path of interest rates is uncertain. At the time of this update, there are concerns about the Suez Canal and a spike in shipping costs resulting from the war in the Middle East but there is also a prospect of further falls in inflation driven by reductions in food and energy prices.

Not only do these factors impact funding costs but they cause disruption to global shopping routes and also create wider problems for working capital, for example, if goods spend longer in transit and do not arrive on time.

With this context in mind, more attention to cash and working capital management is increasingly a key area of focus which has the potential to materially impact financial performance.

Key considerations include:

- Has the funding and hedging strategy been reviewed taking into account the interest rate environment?
- Has your treasury function considered how to achieve a suitable return on day-to-day management of cash and investment of surplus funds?
- Have the options to improve cash positions been fully explored, for example by securing improvements to creditor days?
- Do you have robust credit policies and processes to monitor customer payments and drive improvements in cash collection practices?
- Are your inventory management policies and processes operating effectively to ensure that inventory levels are optimized? There are key performance measures for days' inventory outstanding and that inventory turnover rates are measured and understood.

FOR MORE INFORMATION:

Ziad Akkaoui
+1 416-369-6048
zakkaoui@bdo.ca

Monica Guzzo
+1 416-369-6057
mguzzo@bdo.ca

John Asher
+1 604-313-0601
jasher@bdo.ca

Sam Khoury
+1 416-369-6030
skhoury@bdo.ca

Brandon Bignell
+1 613-780-6474
bbignell@bdo.ca

Pierre Taillefer
+1 514-934-7806
ptaillefer@bdo.ca

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of
or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO Canada LLP is a leading provider of professional services to clients across a variety of sectors and segments. For over 100 years, our team has served communities across Canada through a comprehensive range of assurance, tax, and consulting services, complemented by deep industry knowledge. With over 5000 people across 100 offices in Canada, and more than 1,800 offices in 164 countries, BDO is well-positioned to assist clients with both domestic and global needs.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Canada LLP, a Canadian limited liability partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO member Firms.

http://www.bdo.ca/