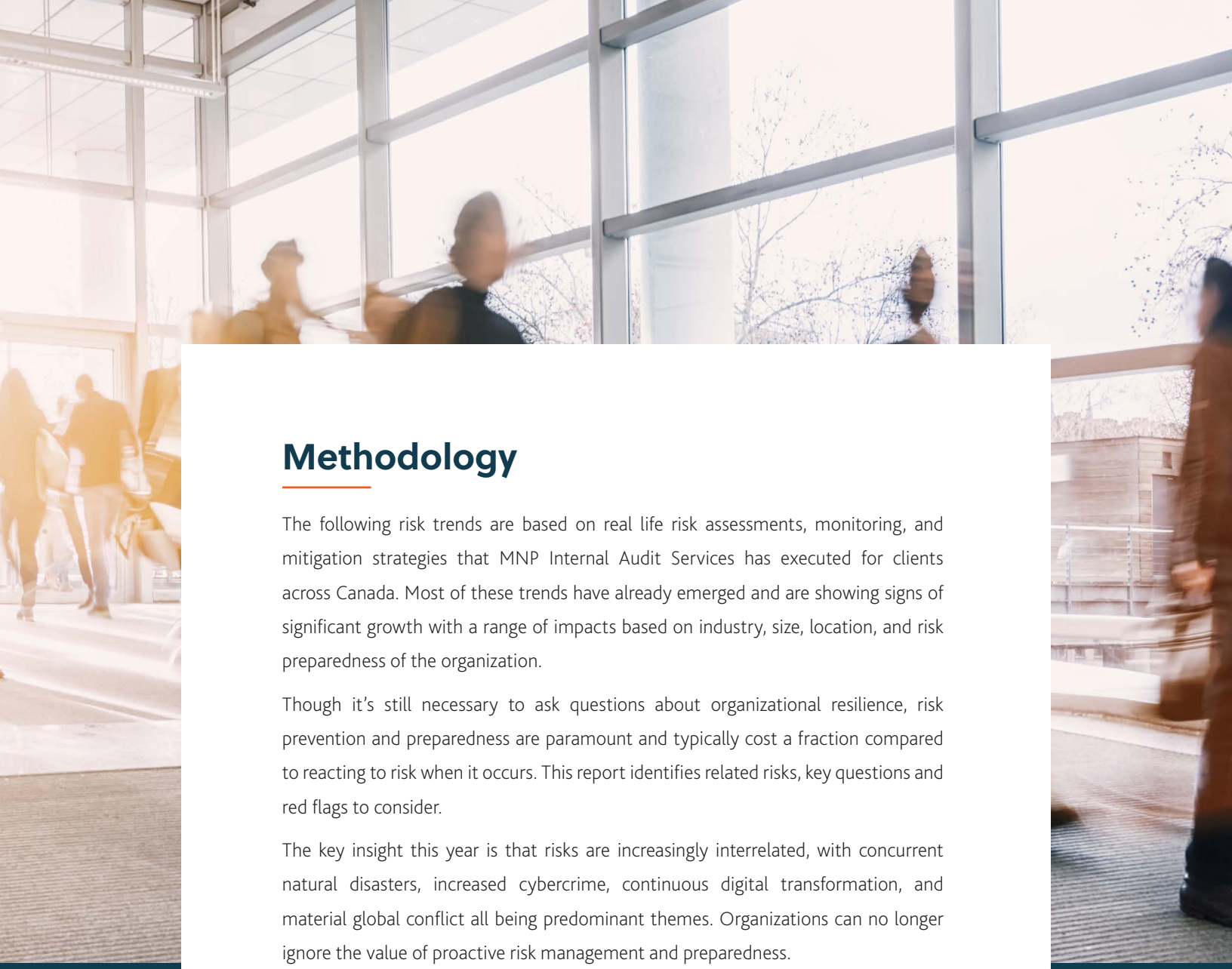
Risk Trends in 2024 and Beyond

Thought leadership for Canadians, produced by Canadian thought leaders

MNP.ca



Methodology

The following risk trends are based on real life risk assessments, monitoring, and mitigation strategies that MNP Internal Audit Services has executed for clients across Canada. Most of these trends have already emerged and are showing signs of significant growth with a range of impacts based on industry, size, location, and risk preparedness of the organization.

Though it's still necessary to ask questions about organizational resilience, risk prevention and preparedness are paramount and typically cost a fraction compared to reacting to risk when it occurs. This report identifies related risks, key questions and red flags to consider.

The key insight this year is that risks are increasingly interrelated, with concurrent natural disasters, increased cybercrime, continuous digital transformation, and material global conflict all being predominant themes. Organizations can no longer ignore the value of proactive risk management and preparedness.

Think of these risk trends as a set of dominos; each one can trigger the occurrence of any of the other risks. As each domino falls, it magnifies the financial and operational risks to the organization, making it more vulnerable to yet further risk.

As we move into the future, continuous monitoring will be instrumental to navigate and optimize for a world of integrated risks.

MNP Internal Audit Services Team

Table of Contents

Cyber Security

The dark web advantage: Can you beat the hackers at their own game?

Chris Law | Defensive Cyber Security
Adriana Gliga | PCI, Privacy, and Data Governance
Eugene Ng | Cyber Security
Drew Buhr | Cyber Security Risk

In keeping with the risk outlook over at least the past 10 years, it's almost certain that cyberattacks will grow even more aggressive and brazen in 2024. The pandemic continues to be one of the driving forces behind this uptick, as more organizations than ever before now have remote or hybrid work policies in place and operate on cloud-based technologies.

Cloud service providers are a lucrative target for hackers as the entire business model of these providers is predicated on operational servers. Even if they're not willing to pay a ransom, such a hack could also reveal a back door to thousands of other clients who may be more inclined to do so.

Remote work also provides a unique opportunity for insiders to initiate or collude with hackers to facilitate a cyberattack on their employers. These attacks have already become more common since 2020, and organizations should expect them to increase in frequency as threat actors innovate new ways to recruit and train insiders via financial or punitive (e.g., extortion) incentives.

Other transformation initiatives also have the potential to increase cyber risk. Many organizations have rapidly adopted digital platforms and tools without performing the necessary risk assessments and/or updating policies and procedures to reflect these changes. Any new hardware or software implementation could be a source of risk. One area of particular concern in the year ahead will be the ungoverned use of ChatGPT and other generative AI tools, which have a high potential for misuse and could lead to leaks of sensitive and proprietary data.

The 2022 invasion of Ukraine has also increased tensions between Russia and many developed nations, and raised questions about China's intentions with Taiwan. At the very least this should lead organizations to be more mindful of state-sponsored hacking in the coming years as both Russia and China may seek to improve their posture and establish cyber superiority. Organizations that should be especially vigilant include the public sector, major infrastructure (energy and utilities, oil and gas, etc.), those that have an outsized impact on national GDP, and those that collect and store large volumes of personal and proprietary data.

Finally, organizations should consider the possibility that they may be the target of an ongoing attack or were the victim of a past attack that hasn't yet been detected. The incident need not have resulted in a disruption to normal operations for hackers to steal sensitive data — including login credentials and employees'/customers' personal information — and sell it on the dark web. It is now possible to beat the hackers at their own game by utilizing a service that can scan the dark web and determine what might be the hacker's next move.

Related risks

- Insider threat causing cyber risk or data exfiltration
- Ransomware attack
- Deepfake social engineering
- Weak operations technology governance
- The Internet of Things creating cyber exposure
- Critical infrastructure at risk
- Controls weakened by shift to hybrid workforce
- Data privacy breach
- Supply chain risk
- Non-compliance

Key questions to ask

- What actions have you taken to verify that cloud service providers have the appropriate practices and controls in place to anticipate, respond to, and mitigate cyber risks?
- Is the frequency and intensity of cyberattacks against your organization increasing over time and/or what is the (changing) nature and vectors of these attacks? What measures has your organization taken to mitigate the likelihood and/or impact of the attacks?
- Do you complete background checks on all new employees who have access to confidential or private data?
- Do you have software to identify and escalate inappropriate access to data, attempts to transfer confidential or private data outside of your organization?
- Do you know how often confidential or private data is emailed outside your organization to private email addresses?
- Have you found ransomware on an internal server or drive? If yes, was a root cause analysis completed to determine who saved it there and when?
- Have you ever utilized a Dark Web scan to determine what the hackers are saying about your organization?
- Do you have sufficient training and tabletop exercises with leadership to discuss how to respond and manage a ransomware attack?

Red Flags

- Employees do not receive any training on cyber security risks
- Internal phishing programs continue to see multiple employees clicking on links that could be a real phishing attempt
- Your IT security function has not taken steps to obtain assurance over the security measures implemented by your cloud service provider
- The Internal Audit function has not conducted cyber security audits in an extended period
- The Dark Web identifies that hackers are discussing your organization or trading in your stolen data

Artificial Intelligence

AI is everywhere: What are your opportunities and risks?

Jason Lee | AI, Data, and Analytics

OpenAI released ChatGPT for public use in November 2022, giving many users their first eye-opening glimpse at the immense power — and disruptive potential — of generative artificial intelligence. Initial reviews marveled at how realistic computer-generated text appeared and the seemingly infinite number of cost-saving use cases, but potential stumbling blocks appeared just as quickly.

Almost everyone who has interacted with ChatGPT and similar generative artificial intelligence frameworks has experienced a so-called hallucination: The algorithm seems to go rogue and volunteer data that is incorrect, was not requested, or generally does not align with the prompt.

Subsequent updates have reduced the frequency of these hallucinations. Still, it may not be possible to eliminate them entirely. AI can interpret a question posed to it in any number of ways depending on how that question is asked, and the same prompt can result in infinite different outputs. Users, therefore, need to apply considerable scrutiny regarding how they engage with AI and the usefulness of AI text, imagery, and computer code when using these tools at scale.

Additional concerns surround the data sources used to train AI applications and the opportunities for misuse. Inputting sensitive or proprietary data (intentional or not) into AI could lead to significant privacy breaches, cases of intellectual property theft, or copyright infringement. Threat actors could deploy AI solutions to craft sophisticated and highly believable social engineering attacks. Students could use it to cheat on university papers.

Perhaps the most important takeaway from the world of AI in 2023 is that organizations and individuals will ignore it at their peril. The technology is advancing far more rapidly than anyone anticipated, and we've only just scratched the surface in understanding the myriad ways it will permeate our lives for better and worse.

Related risks

- AI bias leading to sub-optimal decisions
- Theft or loss of intellectual property or private and confidential data
- Operational issues, resulting from AI not making accurate judgments
- Cybersecurity vulnerabilities
- Plagiarism
- If ignored, loss of competitive advantage

Key questions to ask

- Do you have an inventory of all the technology, systems, processes, and job descriptions that have been — or may be — impacted by AI?
- Does the organization have a risk assessment process for all new technology or AI being considered or implemented?
- Have you asked your critical third parties and suppliers as to how they plan to incorporate AI into their technology, systems, and processes?
- What types of AI usage would be seen as unacceptable to your organization (i.e., driverless delivery vehicles)?
- Are the policies and/or guidelines that your organization has provided on the acceptable use of AI adequate?
- How are users of AI validating the recommendations, explanations, and sources put forward by AI?

Red Flags

- Projects ignoring the associated risks and implications of using AI
- Lack of measurable results related to AI usage
- AI solutions that are not scalable
- Bottlenecks caused by large volumes of AI-generated data and/or the inability to cope with the volume
- AI is unable to harness big data effectively and/or reliably
- Confidential information found on ChatGPT and similar platforms
- The ethics and bias of AI causing suboptimal decision making
- Demand forecasting/optimization failures related to the use of AI
- Negative ESG side effects resulting from reliance on AI

Privacy and Data Governance

Are you confident your data is secure and used ethically?

Adriana Gliga | PCI, Privacy, and Data Governance

Québec introduced stringent regulations in September 2022 which will have downstream impacts across Canada in the years to come. Law 25 includes numerous provisions and penalties which go far beyond the current requirements of the federal Personal Information and Electronic Documents Act (PIPEDA). Law 25 is equalled only by Europe's General Data Protection Regulation (GDPR) — widely accepted as the most robust legislation anywhere in the world.

Law 25 already has teeth beyond Québec's borders, as it applies to any organization (Canadian or international) that does business in the province or stores personal identifiable information (PII) on Québec residents. Given the trend toward greater accountability and stewardship over PII, it is only a matter of time before other provinces and the federal government follow suit with enhancing existing privacy laws.

Stricter regulations present both an obstacle and an opportunity for organizations that have come to rely on data for critical insights and market opportunities. Compliance will require significant updates to policies and procedures governing the collection, use, and transmission of data. These will need to be resilient to the numerous and often differing privacy regulations organizations are exposed to across the various jurisdictions they do business in. It will also require that organizations be more transparent with how and why they collect user data and who it will be shared with — potentially triggering some uncomfortable conversations.

Many organizations will lament the potential financial costs of hiring new privacy officer, curtailing analytics programs which are beyond the scope of why data is collected, implementing additional strategies to ensure compliance, and any regulatory fines they might face.

At the same time, it's worth noting that users are already much more aware of how much organizations value their data and the risks involved with sharing it. This is shifting the competitive edge to those entities that can demonstrate when, how, and why PII will be used, and the mechanisms they've put in place to protect it.

Related risks

- Privacy breaches due to lack of governance around AI and third-party solutions
- Emerging legislative impacts on the use of third-party data sets may increase non-compliance risk
- Impacts of transparency requirements on cross-channel management of user preferences and experience
- Increasing Insider risks due to remote/hybrid environment and turnover
- Regulatory non-compliance

Key questions to ask

- Are you confident that private and confidential data is kept in a secure location with sufficient controls?
- Do you understand which privacy laws apply to your organization and the related compliance requirements?
- Has your organization identified where all critical data is stored and how is moves between systems and jurisdictions?
- Do you know if your private and confidential data may have lost integrity and/or adequate segmentation in the transition to new digital systems (i.e., the cloud)?
- Is it possible for a third-party to gain inappropriate access to your critical data?
- Does your organization have a policy in relation to the use of AI tools such as Chat GPT and the management of confidential or personally identifiable information?

Red Flags

- Inability to isolate personal identifiable information and confidential data
- No training or policy related to data governance and controls
- No policy in relation to AI tools such as ChatGPT
- Minimal use of data analytics for decision support or risk assessment given data is private and confidential
- History of data breaches

IT/OT Governance

Are you optimizing value from limited resources and budgets?

Drew Buhr | Cyber Security Risk
Hash Qureshi | Enterprise Risk Services

Organizations have limited budgets to invest in information (IT) and operational (OT) technology , physical infrastructure, and security. Executives may be tempted to answer to this challenge by foregoing necessary upgrades and transformation initiatives. But just as there are costs to innovation, there are also risks to allowing legacy systems to continue beyond their useful lifespan.

The question isn't whether to resist or embrace digital transformation; rather, it's deciding which initiatives to prioritize right now and how to get the best return on the technology investment. Inefficient systems and processes are a drain on morale and productivity. Restricting innovation and transformation will only lead to individual departments making unilateral technology decisions without considering the impact beyond their operational silos.

Arriving at the best answer as to which technology investments should be prioritized and drive greatest value requires proper governance — with input across the organization, including IT, finance, operations, internal audit (or risk officer), and other relevant stakeholders. Conversations need to consider the current business challenges, the effectiveness of existing systems, and any threats (existing or emerging) to security and privacy. Leaders also need to have a strong grasp of the innovation pipeline and the areas where disruption and business interruption are most likely.

All infrastructure will eventually come to the end of its useful life. Every replacement option will eventually include some type of cloud solution and, eventually, AI-enabled upgrades. Recognizing this, leaders need to set a tone from the top that breeds confidence that the right updates will occur at the right time. They also need the appropriate processes in place to ensure the chosen upgrades will be the best fit for the organization, and the right advisors provide due regard to the opportunities and risks each option brings to the table.

Related risks

- Suboptimal IT/OT decisions reducing control effectiveness
- Lack of / insufficient supervision of third parties and related controls
- Insufficient policy, progress, contracts, and training on the proper/expected use of IT and OT
- Ineffective communication amongst leadership and the board

Key questions to ask

- Has your organization made sub-optimal investments in technology and has a root cause analysis been completed to determine why?
- Does your organization rely on third parties to maintain effective control over IT and OT? What is the vetting process for third party suppliers and what risks need to be managed?
- Do you have sufficient training and tabletop exercises with leadership to discuss how to respond and manage a ransomware attack?
- Is the IT/OT budget sufficient to cover the most critical needs of your organization?
- Do you foresee any big changes to your data or system architecture that might disrupt controls, process, or policy related to IT and OT?
- Has a strategy been established to guide technology investments with a view to ensuring technology is renewed on a timely basis and optimizing the business?

Red Flags

- History of sub-optimal IT/OT decision making (I.e., excessive spending)
- IT/OT third parties seen as the root cause of issues
- Employees with no knowledge of acceptable and unacceptable technology practices
- Operational issues related to system failures

Environmental, Social, and Governance (ESG)

Are you getting the balance right?

Edward Olson | ESG Leader
Mary Larson | Organizational Renewal
Len Nanjad | Organization Change Management

In 2023, the International Sustainability Standards Board (ISSB) issued two new standards related to sustainability disclosure and reporting (IFRS S1 & S2). This year also saw new Canadian legislation (Bill S-211) related to organizations' responsibility to mitigate the use of forced labour and child labour in their supply chains. These measures are only the beginning of what is likely to be an onslaught of ESG-related regulation and legislation in the years to come.

It is imperative that organizations not only be proactive in aligning with these standards, but also anticipate the environmental, social, and governance requirements around the corner. It's clear that ESG is not a passing trend, nor is it likely to be a partisan issue that waxes and wanes with the election cycle. Electors want to see businesses take more accountability for the impacts of their business decisions. Governments are responding by drafting laws with sharper teeth, and many organizations are at risk of being caught unprepared.

Most of the focus to date has been on the environment, and, to a lesser extent, social issues such as the above-mentioned problem of indentured servitude and human trafficking. In time we will see more and more focus on the social and governance elements of ESG.

Organizations have an opportunity to get ahead of the conversation. Equity, diversity, and inclusion (EDI) is one area of focus that organizations will want to be paying attention to in the year ahead (social) — especially as it relates to representation on boards and senior leadership positions (governance). It's also foreseeable that transparency around corporate donations, sustainability reporting, and executive compensation will continue to gain traction as a new area of focus for the ISSB.

At the same time, it would be ill advised to lose focus on the environmental pillar altogether considering the record-breaking heat this summer and unprecedented number of wildfires. If anything, pressure will only increase for organizations to quantify, report, and curtail their greenhouse gas emissions.

Related risks

- Rising costs and complexity related to increasing regulatory requirements and disclosures
- Physical impacts of climate change, pollution, biodiversity loss, and water scarcity
- Increased accountability for supplier and contractor practices throughout the supply chain
- Occupational health issues, unsafe working conditions
- Inadequate community engagement, particularly with Indigenous Peoples
- Lack of diversity, biased decision-making, unequal opportunities, and suboptimal organizational culture
- Corruption and fraud
- Compensation practices: Board and C-suite
- Increased scrutiny on taxes and foreign investments

Key questions to ask

- Has your organization set realistic and defendable ESG targets that are respectable in relation to peers in your industry?
- Have you assessed the impact of inaction or insufficient progress in driving ESG-related changes?
- Are you confident that you can trust the integrity of the data used to calculate your ESG metrics?
- Are any of your targets going to be difficult or even impossible to achieve? If yes, you must determine if you want to continue with this target.
- Do you know how your employees or external stakeholders view the ESG targets of your company? Are they content or disappointed? Is there risk that this could have a negative impact on the culture or perception of your organization?

Red Flags

- Lack of climate change mitigation, environment, and biodiversity strategies and detailed plans
- Weak governance architecture around emergency and incident preparedness
- Increased reports of harassment or discrimination, unwanted turnover, challenges in hiring, low/declining engagement scores
- Lack of rigorous EDI strategy (linked to corporate strategy) or failure to deliver on the strategy
- Links with suppliers or contractors involved in human rights abuses, lack of supply chain transparency
- Increased health and safety violations
- Lack of community engagement, lawsuits, public protests, negative media coverage
- Material increase in whistleblower tips (i.e., corruption and bribery)
- Lack of clarity around responsibility for fraud prevention

IT Third-Party Risk Management

How well do you really know your third parties?

Hash Qureshi | Enterprise Risk Services
Richard Arthurs | Enterprise Risk Services
Gord Chalk | Supply Chain

Canadian companies are more reliant on third parties for the provision of technology related services than at any other time in history — a trend that has been accelerated by the rate of digital innovation throughout and since the COVID-19 pandemic. The reasons for this are severalfold.

One is that many organizations are struggling to find the expertise needed to manage technology at the rate they're adopting it. This has been amplified by the ongoing labour shortage which is forcing many IT functions to split their focus between recruiting for IT needs and supporting other areas of the business.

There are also numerous instances where it makes good financial sense to outsource IT support. New roles are emerging as the sector becomes increasingly specialized. Specialist expertise is also more expensive than ever and it's hard to justify hiring an employee whose skills may not be required on a full-time basis.

Moreover, the broad definition of third parties doesn't include just the individual contractors and consultants who perform specialist work. Software-as-a-service (SaaS) providers are now ubiquitous, covering everything from day-to-day administrative tools (word processors, email, storage servers, etc.) to finance, inventory, and logistics systems.

Organizations are trusting external vendors with more information and access to their networks than ever before. While there are certainly instances where this is logical, even necessary, the sense that this has become the new status quo can easily breed complacency.

Third-party liability clauses, managing third-party access permissions, and regularly conducting cyber security threat assessments cannot become another box to tick when a new third party is brought on board. These must be reviewed and stress tested regularly with the express purpose of finding and remediating the weak links associated with those third-party dependencies.

Related risks

- Cyber security and privacy risk exposure
- Fraud
- Quality and/or project management issues
- System outages

Key questions to ask

- How many new third-party contracts has your company setup since 2020?
- Does your organization complete a detailed risk assessment before setting up contracts with third parties? Is risk mitigation accountability identified in the contract?
- Do your business resilience and disaster recovery plans take into consideration the accountabilities of specific third parties? Are these third parties prepared to act on your behalf when needed?
- Do the third parties you depend upon have appropriate response plans in place in the event of a disruption to their organizations? Have these plans been tested?
- What steps have you taken to ensure the operating effectiveness and resiliency of the third party you are relying upon?
- Do you have a customized code of conduct and training for third parties? Does this include cyber security expectations?

Red Flags

- Excessive complaints related to third parties
- Whistleblower tips
- System quality and performance issues

Merger and Acquisition (M&A) Integration

Are you aware of the risks you are inheriting with your acquisition?

Mike Reynolds | Mergers and Acquisitions Advisory
James Dyack | Valuations and Litigation Support
Johnny Earl | Due Diligence
Mark Reynolds | Mergers and Acquisitions Advisory

Following a sizable dip during the pandemic, Canadian M&A activity is back on the upswing. Private equity firms and growth-minded businesses will be eager to capitalize on the increased transaction volume, but they should also be mindful of the changing risk landscape during the due diligence process.

Major dealbreakers such as financial mismanagement or pending litigation must still be top of mind for potential buyers. However, we also know that instances of fraud and corruption spiked during the pandemic — much of which has yet to be uncovered or reported. Many organizations have also haphazardly introduced new digital platforms and tools over the past three years. Poor integrations could be costly to fix, while cyber vulnerabilities may open the door for a crippling attack if they're not quickly weeded out and remediated.

While these risk areas may not be immediately obvious, the company's approach to governance can be revealing.

Other areas that require a deeper look include the business's ESG exposures and the steps they've taken to quantify and improve exposures within the business and across their supply chain. This is especially relevant for private equity firms whose investors may be expecting progress in the areas of sustainability, diversity, and social welfare. Also, the internal climate within the business and how cultural issues have impacted its ability to attract and retain key employees is critical.

Companies that have an effective enterprise risk management and/or internal audit function will be easier to assess for potential fit and value across all risk areas. Those that don't may still be a viable M&A target; but they will require increased scrutiny — and the costs of addressing key risk areas need to be factored into the final valuation and post-merger integration plan.

Related risks

- IT/OT Governance, controls, and specifically cyber risk
- Data and system integrity issues
- Cultures in conflict
- Inability to achieve required synergies

Key questions to ask

- Does your due diligence process include IT/OT controls and governance, ability to meet investor ESG expectations, an awareness of any risk related to fraud and corruption, cultural issues, and proactive enterprise risk management activities?
- Are you clear at the outset which factors would be dealbreakers and have you set parameters for a "no-go" decision?
- Have you ever disqualified a merger or acquisition due to an unacceptable level of risk? Based on this, what do you feel is the risk appetite of the board and executive?

Red Flags

- New cyber, ESG, fraud, or corruption issues related to acquisitions or mergers
- Errors found in data
- Excessive cost and time required to achieve integration targets
- Morale issues and excessive turnover

Digital Transformation

Have you envisioned the opportunity and risks of the end state?

Jason Lee | Machine Learning and AI
Len Nanjad | Organization Change Management
Soumya Ghosh | Digital Transformation and Advisory
Wendy Gnenz | Digital Strategy and Planning

The pandemic forced many companies and governments to expedite long-term digital transformation plans. Cloud-enabled capabilities have been a common feature among transformation initiatives to accommodate enhanced e-commerce and the needs of a remote and geographically dispersed workforce. The cloud has also found its way into advanced hardware as organizations seek more data on (and how to improve the performance of) physical systems.

While many new platforms seek to replace aging and outdated infrastructure, it would be short sighted to treat these upgrades as like for like replacements. For example, a cloud enterprise resource planning platform can perform many of the same functions as on-premises accounting software, but it also introduces new processes and risk exposures.

Each cloud update introduces a new potential point of entry for cyber criminals and adds to the organization's overall third-party risk calculus. Relying on default user access settings can also increase the risk of insider threats, while poor or incomplete training can diminish data quality and the resulting return on investment. These side effects exist throughout the digital transformation value chain and compound with each new platform that is introduced.

The introduction of new software may also require updates — not just to hardware or other supporting infrastructure to ensure it is secure and operates as intended, but also to support integration with remaining legacy systems. Moreover, it is necessary to review related policies, procedures, and risk assessments that govern the use of technology and update these as required. Digital transformation can also have a material impact on an organization's strategy, business model, and human resourcing requirements — creating an increased need for specialist knowledge in some areas and making other roles redundant.

Related risks

- Cybersecurity threats
- Data privacy concerns
- Integration complexities
- Dependency on technology providers
- Cost overruns
- Resistance to change
- Skills gap
- Regulatory non-compliance
- System downtime
- Lack of digital transformation strategy
- Data quality issues

Key questions to ask

- Do you have an inventory of all the planned changes and changes already made related to digital transformation?
- Have the integration requirements with legacy systems been identified and assessed?
- Post digital transformation, do you know what controls, policies, procedures, training materials, and job descriptions need to be updated to remain effective and relevant?
- Will your organization need added resources with new capabilities to be able to effectively and efficiently use the new technology?
- How much training will be required for employees to learn how to use the new technology?
- Has the number and types of cyber attacks changed since your digital transformation started?
- How will you determine whether the intended benefits from the transformation were realized and whether there are any lessons to be learned?

Red Flags

- Increased number or complexity of cyberattacks
- Evidence of unauthorized access to systems and access to data
- System failures or downtime
- Data inaccuracies and reporting errors
- Excessive costs and service required
- User complaints
- Training, policies, and procedures out of date

Data Analytics and Continuous Monitoring

Do you feel competitors have better insights?

Ian Shaule | Advanced Analytics
Colin Wenngatz | Retail Analytics
Cameron Ollenberger | Risk Analytics
Olena Batuev | Data Analytics

Reliance on analytics has skyrocketed over the last decade with the rapid advancement of cloud-based platforms and tools. The amount and sources of data have also increased significantly with the digitization of business processes and the increased affordability of internet-connected sensors and digital twins (i.e., elaborate computer-aided simulations of physical infrastructure, often used for testing and analysis).

Analytics can add immeasurable value to internal audits by providing decision support, helping to monitor critical performance measures and targets, revealing potential fraud risks, and much more. Data-driven insights can also drive entire business models by helping to forecast consumer demand, target ads, streamline logistics and supply chains, and optimize costs throughout the value chain.

And where there are significant opportunities, there is also considerable risk.

Two opposing forces that organizations need to balance are the risks of moving too slowly or too quickly in advancing analytics capabilities. Failing to prioritize analytics will result in slower growth relative to competitors and a sharp decline in market share over the near to medium term. On the other hand, the race for better insights can lead organizations to skip critical steps in resourcing, governance, and strategy. Gaining the wrong insights from data can be even more detrimental than not having any insights.

Analytics are table stakes in 2023. However, data integrity and confidence in the quality of analytic-driven insight must be the guiding forces behind its ongoing maturity. Priority one should be to add analytic expertise at the board and operational levels — including internal audit. Next should be to assess the quality of existing data and existing policies and practices to ensure data quality. Third should be to create (or re-assess) the organization's strategy for maturing the analytics program and securing executive buy in on that roadmap.

Related risks

- Internal audit (IA) becomes redundant as business outpaces it in use of analytics and technology
- Business assumes IA only looks backwards and does not embrace innovation. IA is no longer invited to the table
- The business is losing market share to the competition
- The failure rate of innovation is higher than your peer set
- The business does not have early warning indicators of issues or negative trends

Key questions to ask

- When was the last time you tested the integrity of your data? Has anything changed that might have impacted the integrity of your data?
- Do you have a material reliance on data from third parties (I.e., ESG metrics)? Are you confident this data has integrity?
- Are you confident in the accuracy of the output of your data analytics? Especially the analytics used for material insight and decision making.
- Are you losing market share or seeing an increase in complaints because you do not have the same quality of information and insight as your competitors?

Red Flags

- Lack of data integrity
- Ambiguous findings
- Missing value proposition
- Lack of technical or industry experience
- Data analytics are too simple or too complex
- Lack of audit committee buy in

Workforce Transformation & Organizational Readiness

Are you optimizing and sustaining value from critical resources?

Mary Larson | Organizational Renewal
Len Nanjad | Organization Change Management

There has been a seismic shift in the working world over the past decade: new technologies have created new roles and increased the need for specialist expertise. The widespread adoption of remote and hybrid work arrangements during COVID is having a material impact on corporate cultures and well-established management practices. And the continued globalization of businesses and supply chains is pushing many jobs overseas, making internal teams smaller and more focused on supplier management.

Generational changes are also shifting approaches to recruitment and retention as more baby boomers retire and Gen Z continues to establish its place in the workforce. The former tended to stay with employers for the long term and follow along with organizational norms and best practices. Whereas younger professionals appear to be more open to pursuing roles with different employers and more vocal about their expectations for greater work/life balance as well as more diverse, inclusive, and socially conscious cultures.

For organizations, these trends all raise important questions about how best to attract and retain the critical resources that are needed to create operational and strategic value.

The so-called Great Resignation through 2020 and 2021 highlighted an overall lack of readiness among many organizations which quickly found themselves unable to deliver on key business priorities. While the pandemic served as an inflection point, leaders and executives will be wise to recognize that the underlying cause — inflexibility, resistance to change, stagnant culture, etc. — remains a risk area that will become more, not less, volatile in the years to come.

Organizations that recognize these challenges and take proactive steps to address their organizational readiness (i.e., increase employee morale, support health and wellness, provide competitive salary and benefits, strike the right balance between employee growth and autonomy, etc.) will find themselves in the best position to realize strategic value in an increasingly chaotic environment.

Related risks

- Getting and keeping the right people
- Misunderstanding generational needs and nuances
- Increasing use of AI applications to support change management and behavior change
- Inadequate monitoring and support of health and wellness, especially mental health and wellness
- Remote work as a right, not a privilege

Key questions to ask

- Does your culture support the optimization of strategic success, or is it making it harder to succeed?
- Is your resource turnover exceeding industry averages? Has it changed in the last three years?
- Is the morale of your workforce positive or are their reasons to be concerned?
- Do you provide sufficient compensation, benefits, training, and development?
- Is there an elevated risk of labour disruption (i.e., Unions, etc.)?
- Do you have sufficient succession planning for all critical roles in your organization?
- Do your incentive structures promote the right behaviours and do the resonate across all generations?

Red Flags

- Existing controls do not support agile change management or team member autonomy
- AI/automation tools reveal discrepancy between stated and measured engagement, wellness, and change readiness
- Increased turnover, leave, mental health usage, policy violations related to digital transformation initiatives
- Increased turnover or lack of engagement
- Increase interest in unionizing and regulatory challenges

Insurance

Read the fine print: Do you really know the current costs and benefits of insurance?

Craig Burkart | Insurance Advisory

An unprecedented number of hurricanes, floods, wildfires, droughts, and numerous cyber and privacy breaches have led to a record number of insurance claims throughout 2022 and 2023. This has led to an increase in the cost of insurance, uninsurable assets, and the complexity of terms and conditions related to acceptable claims.

As a result, organizations are finding that insurance is becoming far less affordable and far more difficult to access. And it's getting harder to make a claim even for those that are insured.

The current challenges are only the tip of the spear. 2023 is on pace to become the hottest year on record and it's likely that climate-related events will only become more severe and damaging in the coming decade. There's also reason to fear the looming impact of AI on the cyber risk landscape among other risk areas.

Organizations can no longer rely exclusively on insurance to mitigate a large percentage of risk. Those that do will find themselves increasingly at the behest of insurers to put relevant practices, policies, and governance in place. While this may lead to improved risk management, it's worth reiterating that insurers have a clear incentive to prioritize their own interests no matter the cost to the insured.

Moving forward, boards and executives must seek to gain a better understanding of their overall risk landscape — including the potential for business interruptions due to natural disasters, greenwashing, cyber attacks, pandemics, supply chain interruptions, etc. This will require some difficult decisions around which risks the company should absorb and/or mitigate independently and which to outsource to insurance.

It may also be a good time to contact an independent insurance advisor who can help to quantify coverage amounts and rates and determine whether the coverages are worth the investment.

Related risks

- Lack of oversight for renewals or amounts
- Insurance renewals not timely and/or incomplete
- Insurance program not matching the risks
- Improperly set insurance values
- Significant increase in rates and claim requirements

Key questions to ask

- How does the organization plan to navigate significant increases in insurance rates, especially those related to cyber insurance?
- Has your overall insurance coverage of risk exposure decreased over the last few years? How does this change the organization's overall risk management strategy?
- How could utilizing an insurance expert assist with optimizing insurance claims? Did you know many policies cover the cost of an insurance expert to support your claim?
- Have you ever audited the value optimization of your insurance coverage?

Red Flags

- Last-minute insurance renewal
- Claims not properly paid
- Insufficient values
- Board and senior management not aware of renewals or amounts
- Material rate increases

Economic and Financial Adversity

How has the economy impacted your business model?

Mike Reynolds | Mergers and Acquisitions Advisory
Mark Reynolds | Mergers and Acquisitions Advisory
James Dyack | Valuations and Litigation Support
Richard Arthurs | Enterprise Risk
Giovanni Worsley | Property Tax
Lee Thiessen | Real Estate and Construction

The Canadian economy remains in uncertain waters through 2023 as rising interest rates have struggled to cool stubbornly high inflation. While consumer spending has so far been resilient, there are growing fears the rising costs of food, fuel, and housing will push more households to the financial margins.

Businesses are also feeling the side effects of economic turbulence, with many choosing to hold fast until they have a better idea of whether a recession is coming and/or how severe it might be.

Capital management is a particular concern. Organizations are understandably reticent to hire, take on debt, or invest in infrastructure projects for fear of limiting cashflow if the economy contracts. On the other end, a tight labour market is keeping up the pressure to retain key employees, which includes demands to help them keep up with the rising cost of living.

Just as there are consequences to making the wrong decisions (e.g., expanding into new markets right before a downturn, downsizing just before the economy improves), doing nothing is not a better option.

Instead, organizations should be using this opportunity to pressure test business models to ensure they are resilient to any economic scenario that may arise in 2024. Where are the inefficiencies? What areas are underperforming? How will trends, technologies, and consumer behaviours shift in the next three to five years? This process can help to overcome decision making paralysis by identifying inefficiencies, opportunities, and core risk areas.

Investing in the right areas now will not only make the business more resilient to a potential recession, but also put it in a position to thrive when the economy starts growing again.

Related risks

- Increased cost of debt
- Reduced consumer demand
- Continued but decreasing inflation
- Increasing input costs
- Continued supply chain constraints

Key questions to ask

- How has the economy and decreased disposable income impacted your business model?
- Are there early signs and risk trends that you should be preparing for?
- Is your business model resilient enough to withstand ongoing economic challenge?
- Are you monitoring specific success and risk metrics?
- How are you managing your cashflow to ensure adequate funds to cover off obligations?

Red Flags

- Shrinking margins
- Low cash flow
- Decreasing customer demand

Business Resilience (Including Third Parties)

How do you respond when crisis hits?

Cliff Trollope | Business Resilience

Businesses face an ever-growing list of threats to their ability to operate, grow, and remain profitable. Serious threats over the past decade have included a global pandemic, natural disasters, significant demographic changes and shifts in consumer behaviour, disruptive technologies, a massive rise in cyber attacks, and generationally high inflation.

The next 10 years will bring even more challenges, not the least of which are increased impacts of climate change and global pressure to transition from fossil fuels, and the rapid advancement of AI.

Given the growing number and magnitude of potentially existential crises — and the shrinking timespan from one challenge to the next — it's clear that preparation is key. Leaders need to be ready to respond quickly and make decisive decisions when faced with a sudden and serious threat to the business. They also need to be confident that their vendors will be ready to respond swiftly with the right expertise at the right time.

Nobody can predict when the next pandemic or natural disaster will strike. Still, organizations can learn a lot from the outcomes and impacts of past crises on their own business and those of peer organizations. Coupled with frequent risk assessments, these lessons can inform scenario planning, tabletop exercises, and emergency response plans that cover the highest priority threats.

Ideally, these exercises will include participation from relevant third-party vendors such as cyber managed service providers, cloud vendors, co-sourced or outsourced internal auditors, business advisors, and others. The goal here isn't necessarily to successfully navigate the crisis. Rather, it is to identify critical weaknesses in existing emergency response plans such as difficulty mobilizing resources, potential safety issues, and areas where the business is most likely to lose customers and/or money.

Related risks

- Business and IT/OT disruption
- Inability to coordinate a timely response and organized communication
- In time of need, critical resources are not available or do not understand their roles
- Excessive costs required to react to needs

Key questions to ask

- Does your organization maintain a list of probable risk scenarios it should be prepared for, including plans on how it will respond to those scenarios?
- Has your leadership ever conducted mock tabletop scenarios to discuss how you would manage a crisis? If yes, do you involve an expert in this discussion?
- Has your organization experienced a real crisis or at least a material unexpected disruption? If yes, did you conduct a post analysis of this situation to discuss what worked well, what did not work well, and what you must be better prepared for?
- Do you keep track of crises that have impacted peer companies and assessed whether you are prepared to respond? Usually if it can happen to a similar organization, it could also happen to you.

Red Flags

- Insufficient preparation (training, discussions, policy, or plans)
- Third parties not aware of role in business resilience
- Business not prepared for past business disruption situations
- Competitors negatively impacted by disruption not expected by industry

Capital Projects and Operations

Are your projects being managed to mitigate the risk of budget overruns, extended timelines, and poor quality?

Richard Arthurs | Enterprise Risk
Gord Chalk | Energy and Utilities
Olena Batuev | Data Analytics
Cameron Ollenberger | Risk Analytics

Capital projects are some of the most expensive investments a company will ever make. These can range in the billions of dollars and typically carry a high risk of cost overruns, especially with inflationary pressures on labour and materials.

The expectation that capital projects almost always come in overbudget can, itself, lead organizations to pay far more — and take on more risk — than necessary.

One reason is that most capital projects see some error in billing. It is common for a project to inflate by one to three percent due to erroneous billing. That could mean up to $30 million on a billion-dollar project. Organizations that are embarking on capital projects can mitigate the risk of overpaying through the targeted use of data analytics to compare invoices and requisitions to identify inconsistencies. They could then use this data to collect back when overbilled or defend their case in court.

Other risks associated with capital projects include quality issues which can compromise both the health and safety of employees and contractors leading to costly downtime and unexpected maintenance. Addressing these issues before construction starts is the most effective way to protect people, an organization's reputation, as well as its bottom line.

Aside from the typical design, budgeting, and tendering proposals for capital projects, appropriate project management can help to ensure that timelines, materials, and costs all align with expectations. This function should be accountable for inspections and status updates throughout the project lifecycle to validate that the work is being performed as agreed, complies with relevant standards, and meets the specifications set out in engineering plans.

It is also critical that the initiative also go through a rigorous risk assessment as part of the planning process. This lens can help to identify flaws in the design, anticipate how delays and overruns will impact the business, and identify potential project management issues — including risks to safety and the environment.

Related risks

- Budget overruns and timeline delays
- Vendors who are not qualified to perform the work as required
- Poorly designed vendor contracts
- Health and safety incidents
- Vendor billing issues
- Quality concerns

Key questions to ask

- Does your organization have the requisite experience to manage large scale capital projects? If not, how will it resource the expertise required to successfully deliver the project?
- How will you monitor the timely delivery of the project ensuring it remains on budget?
- Have clear roles and responsibilities for both project delivery and project oversight been established?
- Are there unique design and implementation elements with this project, or is this something the engineering, procurement, and construction firm has done before?
- Are the vendor contracts set up as fixed fee or will they be time and materials? Do you have the contract set up with a right to audit clause and a defined dispute resolution process?

Red Flags

- Onsite health and safety issues
- Vendor billing errors
- Regulatory non-compliance instances
- Legal issues
- Material cost overruns
- Timeline extensions
- Engineering, procurement, and construction resource turnover

Fraud and Corruption

How much has the cost of living increase impacted fraud risk?

Lisa Majeau-Gordon | Forensics
Richard Arthurs | Enterprise Risk

All Canadians have experienced significant increases to the cost of living throughout 2022 and 2023 due to rampant inflation and interest rates at their highest level since before the 2008 financial crisis. Some have been particularly hard hit. MNP's July 2023 Consumer Debt Index revealed that 52 percent of households were $200 or less away from financial insolvency and more than a third already didn't make enough to cover their monthly living expenses.

While leaders are right to be concerned about their employees' wellbeing and welfare, organizations should also be keeping a watchful eye to the increased risk of theft and fraud within the business.

There are typically three factors which influence the likelihood that a fraud will occur, two of which have been significantly elevated over the past 18 months. One is pressure; the perpetrator feels compelled to commit fraud because they need the money. Another is rationalization; the perpetrator convinces themselves the ends justify the means.

Given the economic drivers and other (often personal) factors at play, senior leaders and internal auditors will find it difficult to mitigate those first two elements of the fraud triangle. However, it is still important to recognize that these are elevated right now. That makes it even more critical to understand and manage the third determinant of fraud, which is opportunity.

Remote work, incomplete policies, poor training, and ineffective controls can all lead to increased opportunity for fraud to occur. Regular risk assessments should seek to identify additional opportunity-related fraud risks unique to the organization.

Taking steps like requiring dual signatures for large transactions, using AI tools to monitor for suspicious activity, restricting login access to the smallest number of individuals can all help to reduce fraud. Providing fraud training and encouraging team members to report suspicious activity has also proven to be extremely effective.

Related risks

- Financial loss
- Legal and regulatory issues
- Fines
- Business interruption
- Negative impact on reputation

Key questions to ask

- Are you aware of how much pressure the current economic conditions have had on your employees and third parties? Is there anything you can do proactively to help reduce this pressure related to cost of living (allow remote working, etc.)?
- Have your organization or peers experienced an increase in fraudulent activities?
- Have you conducted a fraud risk assessment recently?
- Do you have experts in fraud investigation? Often forensic experts are engaged to assist with investigations. Do not assume internal audit has this expertise.
- Have you ever used advanced data analytics to detect fraud risk or to find real incidence of fraud in your organization?

Red Flags

- Employees living beyond their means
- Growing morale issues
- Employees who never take time off or work at odd times (I.e., stat holidays and weekends)
- Excessive overtime, sales returns, damaged product, refunds, coupon redemption, etc.
- Third parties with cash flow issues
- Excessive manual transactions or transactions off the books
- No code of conduct or expense reporting policy, or controls (i.e., training)
- Doing business in highly corrupt countries

Internal Audit Project Opportunities

This section lists the opportunites for internal audit projects in each area of risk discussed in the previous section.

Cyber Security | The dark web advantage: Can you beat the hackers at their own game?

- **Information Security Policy and Procedure Audit:** This audit reviews the organization's information security policies and procedures to ensure they are comprehensive, up-to-date, and aligned with industry best practices.
- **Access Controls Audit:** This audit assesses the effectiveness of access controls in place to protect sensitive information and systems from unauthorized access.
- **Network Security Audit:** This audit examines the organization's network infrastructure to identify potential security weaknesses and ensure the implementation of appropriate security measures.
- **Vulnerability Assessment and Penetration Testing Audit:** This audit reviews the results of vulnerability assessments and penetration tests conducted on the organization's systems and applications to identify and remediate potential vulnerabilities.
- **Security Patch Management Audit:** This audit assesses the organization's processes for identifying, testing, and applying security patches to address known vulnerabilities.
- **Data Protection and Encryption Audit:** This audit evaluates the organization's data protection measures, including data encryption, to ensure that sensitive information is adequately safeguarded.
- **Incident Response Preparedness Audit:** This audit assesses the organization's readiness to handle cybersecurity incidents effectively, including the existence of incident response plans and the training of staff to respond to incidents.
- **Security Awareness Training Audit:** This audit examines the effectiveness of cybersecurity awareness training provided to employees to reduce the risk of human-related security incidents.
- **Physical Security Audit:** This audit reviews the physical security measures in place to protect critical infrastructure, data centers, and other sensitive areas.
- **Endpoint Security Audit:** This audit evaluates the security controls implemented on endpoints (e.g., laptops, desktops, mobile devices) to protect against malware and unauthorized access.
- **Data Backup and Disaster Recovery Audit:** This audit ensures that data is regularly backed up, data restoration has been tested and disaster recovery plans are in place to restore critical systems and data in case of a cybersecurity incident or natural disaster.
- **Identity and Access Management (IAM) Audit:** This audit examines the organization's IAM processes and technologies to ensure that user access is appropriately managed and monitored.
- **Third-Party Vendor Security Audit:** This audit assesses the security practices of third-party vendors and service providers who have access to the organization's systems or data.
- **Regulatory Compliance Audit:** This audit reviews the organization's compliance with relevant cybersecurity laws, regulations, and industry standards.
- **Cybersecurity Governance Audit:** This audit evaluates the effectiveness of the organization's cybersecurity governance structure and oversight processes.

Artificial Intelligence | AI is everywhere! What are your opportunities and risks?

- **AI Model Performance Audit:** This audit assesses the accuracy, efficiency, and reliability of AI models deployed by the organization. It ensures that the models are producing accurate and meaningful results.
- **Data Quality for AI Audit:** This audit examines the quality, completeness, and relevance of data used to train AI models. It ensures that the data is of high quality and that any biases are identified and addressed.
- **AI Governance and Oversight Audit:** This audit evaluates the organization's governance structure and oversight processes related to AI development and deployment. It ensures that there are clear responsibilities and accountability measures in place.
- **AI Ethics and Fairness Audit:** This audit focuses on assessing the ethical implications of AI systems and whether they are designed to treat all individuals and groups fairly, without bias or discrimination.
- **AI Security and Privacy Audit:** This audit reviews the security measures implemented to protect AI systems and the data they process. It ensures that AI systems do not pose security risks and that privacy concerns are adequately addressed.
- **AI Transparency Audit:** This audit examines whether AI models and their decisions can be explained and understood. It ensures that AI systems are not operating as "black boxes" and that their reasoning is transparent.
- **AI Compliance Audit:** This audit assesses whether AI systems comply with relevant laws, regulations, and industry standards, such as data protection regulations or ethical guidelines.
- **AI Training and Testing Data Audit:** This audit evaluates the data used to train and test AI models, ensuring it is representative and appropriate for the intended use.
- **AI Vendor Management Audit:** This audit focuses on the organization's management of third-party AI vendors, ensuring that vendor selection, contracts, and performance are in line with the organization's requirements and standards.
- **AI Incident Response and Contingency Audit:** This audit reviews the organization's preparedness to respond to AI-related incidents, such as system failures, biases, or ethical violations, and the measures in place to handle such situations.
- **AI Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees regarding AI ethics, usage, and potential risks.
- **AI ROI (Return on Investment) Audit:** This audit evaluates the financial and strategic value derived from AI implementations, ensuring that AI projects align with the organization's goals and provide tangible benefits.

Artificial Intelligence | AI is everywhere! What are your opportunities and risks?

- **AI Model Performance Audit:** This audit assesses the accuracy, efficiency, and reliability of AI models deployed by the organization. It ensures that the models are producing accurate and meaningful results.
- **Data Quality for AI Audit:** This audit examines the quality, completeness, and relevance of data used to train AI models. It ensures that the data is of high quality and that any biases are identified and addressed.
- **AI Governance and Oversight Audit:** This audit evaluates the organization's governance structure and oversight processes related to AI development and deployment. It ensures that there are clear responsibilities and accountability measures in place.
- **AI Ethics and Fairness Audit:** This audit focuses on assessing the ethical implications of AI systems and whether they are designed to treat all individuals and groups fairly, without bias or discrimination.
- **AI Security and Privacy Audit:** This audit reviews the security measures implemented to protect AI systems and the data they process. It ensures that AI systems do not pose security risks and that privacy concerns are adequately addressed.
- **AI Transparency Audit:** This audit examines whether AI models and their decisions can be explained and understood. It ensures that AI systems are not operating as "black boxes" and that their reasoning is transparent.
- **AI Compliance Audit:** This audit assesses whether AI systems comply with relevant laws, regulations, and industry standards, such as data protection regulations or ethical guidelines.
- **AI Training and Testing Data Audit:** This audit evaluates the data used to train and test AI models, ensuring it is representative and appropriate for the intended use.
- **AI Vendor Management Audit:** This audit focuses on the organization's management of third-party AI vendors, ensuring that vendor selection, contracts, and performance are in line with the organization's requirements and standards.
- **AI Incident Response and Contingency Audit:** This audit reviews the organization's preparedness to respond to AI-related incidents, such as system failures, biases, or ethical violations, and the measures in place to handle such situations.
- **AI Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees regarding AI ethics, usage, and potential risks.
- **AI ROI (Return on Investment) Audit:** This audit evaluates the financial and strategic value derived from AI implementations, ensuring that AI projects align with the organization's goals and provide tangible benefits.

Privacy and Data Governance | Are you confident your data is secure and used ethically?

- **Data Privacy Compliance Audit:** This audit ensures that the organization is complying with relevant data privacy laws and regulations, including the General Data Protection Regulation (GDPR) in Europe, Quebec's Law 25, and/or the California Consumer Privacy Act (CCPA) in the United States.
- **Data Access and Authorization Audit:** This audit reviews the access controls and authorization mechanisms in place to ensure that data is only accessible by authorized personnel and that data access rights are appropriately managed.
- **Data Quality Audit:** This audit examines the quality and accuracy of the data maintained by the organization. It includes assessing data validation, cleansing processes, and data documentation practices.
- **Data Retention and Deletion Audit:** This audit assesses whether the organization is retaining data for the appropriate periods of time and is following proper procedures for data destruction when it is no longer required.
- **Data Security Audit:** This audit focuses on evaluating the security measures in place to protect sensitive data from unauthorized access, breaches, or cyberattacks.
- **Data Governance Policy and Procedures Audit:** This audit ensures that the organization has well-defined data governance policies and procedures in place and that they are effectively implemented and followed.
- **Data Classification and Handling Audit:** This audit reviews how data is classified based on its sensitivity and criticality, and whether appropriate handling measures are in place for each classification level.
- **Data Lifecycle Management Audit:** This audit examines how data is collected, stored, used, and eventually archived or deleted throughout its entire lifecycle.
- **Data Governance Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees regarding data governance policies and best practices.
- **Data Governance Metrics and Reporting Audit:** This audit reviews the organization's data governance metrics and reporting mechanisms to ensure that they effectively measure the success and performance of data governance initiatives.
- **Data Governance Committee Effectiveness Audit:** This audit evaluates the effectiveness and efficiency of the data governance committee or similar governance bodies responsible for overseeing data management activities.
- **Data Governance Communication and Stakeholder Engagement Audit:** This audit assesses how effectively the organization communicates its data governance initiatives to stakeholders and engages them in data management efforts.

IT/OT Governance | Are you optimizing value from limited resources and budgets?

- **IT/OT Strategy and Alignment Audit:** This audit assesses how well the IT and OT strategies align with the overall business objectives and goals of the organization.
- **IT/OT Asset Management Audit:** This audit reviews the organization's processes for managing and maintaining IT and OT assets, including hardware, software, and industrial control systems.
- **IT/OT Change Management Audit:** This audit evaluates how changes to IT and OT systems are managed, documented, and approved to minimize risks and disruptions.
- **IT/OT Security Audit:** This audit focuses on assessing the security measures implemented for both IT and OT systems, ensuring protection against cyber threats and unauthorized access.
- **IT/OT Risk Management Audit:** This audit examines the organization's risk management practices related to IT and OT, including risk identification, assessment, and mitigation strategies.
- **IT/OT Incident Response and Business Continuity Audit:** This audit assesses the organization's preparedness to respond to IT and OT incidents, as well as its ability to maintain critical operations during disruptions.
- **IT/OT Compliance Audit:** This audit reviews whether IT and OT practices comply with relevant laws, regulations, and industry standards.
- **IT/OT Vendor Management Audit:** This audit evaluates the management of IT and OT vendors, including contracts, security assessments, and performance monitoring.
- **IT/OT Performance Measurement and Reporting Audit:** This audit examines the organization's metrics and reporting mechanisms to measure the performance and effectiveness of IT and OT activities.
- **IT/OT Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees regarding IT and OT governance, security, and best practices.
- **IT/OT Integration Audit:** This audit focuses on evaluating the integration between IT and OT systems to ensure seamless communication and cooperation between the two domains.
- **IT/OT Budget and Resource Allocation Audit:** This audit reviews the allocation of budget and resources to IT and OT initiatives to ensure alignment with business priorities.
- **IT/OT Documentation and Documentation Management Audit:** This audit examines the documentation practices for IT and OT systems, including policies, procedures, and system documentation.
- **IT/OT Governance Committee Effectiveness Audit:** This audit evaluates the effectiveness and efficiency of governance committees responsible for overseeing IT and OT activities.
- **IT/OT Cloud and Third-Party Services Audit:** This audit assesses the use of cloud services and third-party providers for IT and OT functions, including security and compliance considerations.

ESG | Are you getting the balance right?

Environment (E)

- **Carbon Footprint Audit:** This audit assesses the organization's carbon emissions across its operations, including direct emissions (Scope 1), indirect emissions from purchased energy (Scope 2), and other indirect emissions along the value chain (Scope 3).
- **Energy Efficiency Audit:** This audit reviews the organization's energy consumption patterns and identifies opportunities for energy efficiency improvements to reduce greenhouse gas emissions.
- **Waste Management Audit:** This audit evaluates the organization's waste generation, disposal practices, and recycling efforts to identify ways to minimize waste and its impact on the environment.
- **Water Usage Audit:** This audit assesses the organization's water consumption and identifies strategies to conserve water resources.
- **Green Procurement Audit:** This audit examines the organization's procurement practices to ensure environmentally sustainable sourcing and supplier selection.
- **Sustainable Supply Chain Audit:** This audit reviews the environmental impact of the organization's supply chain activities and identifies opportunities for sustainability improvements.
- **Environmental Compliance Audit:** This audit assesses the organization's compliance with environmental laws, regulations, and permits relevant to its operations.
- **Environmental Management System (EMS) Audit:** This audit evaluates the effectiveness of the organization's EMS, such as ISO 14001, and its implementation of environmental policies and procedures.
- **Renewable Energy Usage Audit:** This audit reviews the organization's utilization of renewable energy sources and its progress toward renewable energy targets.
- **Carbon Offsetting and Compensation Audit:** This audit assesses the organization's efforts to offset or compensate for its carbon emissions through initiatives such as reforestation projects or investing in carbon credits.
- **Climate Change Resilience and Adaptation Audit:** This audit examines the organization's strategies for adapting to climate change impacts and building resilience against climate-related risks.
- **Reporting and Communication Audit:** This audit evaluates the organization's transparency in reporting its environmental performance and progress toward carbon footprint reduction targets.
- **Environmental Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees regarding environmental sustainability and carbon reduction efforts.
- **Green Building and Infrastructure Audit:** This audit reviews the environmental impact of the organization's buildings and infrastructure, including energy-efficient designs and sustainable construction practices.
- **Environmental Performance Monitoring and Measurement Audit:** This audit ensures that the organization has appropriate metrics and systems in place to monitor its environmental performance regularly.

ESG | Are you getting the balance right?

Social (S)

- **Diversity and Inclusion Audit:** This audit assesses the organization's efforts to promote diversity and inclusion in its workforce, ensuring fair employment practices and equal opportunities for all employees.
- **Employee Welfare and Well-being Audit:** This audit reviews the organization's initiatives and policies to support employee well-being, health, safety, work-life balance, and professional development.
- **Human Rights Compliance Audit:** This audit evaluates the organization's adherence to human rights principles, ensuring that its activities do not infringe upon the rights of individuals or communities.
- **Labour Practices Audit:** This audit assesses the organization's compliance with labour laws and regulations, including fair wages, working hours, and appropriate labour conditions.
- **Supplier and Vendor Social Responsibility Audit:** This audit reviews the social responsibility practices of the organization's suppliers and vendors to ensure ethical and responsible sourcing.
- **Community Engagement and Impact Audit:** This audit examines the organization's efforts to engage with and positively impact the communities in which it operates.
- **Social Impact Assessment Audit:** This audit assesses the organization's activities and projects to measure their social impact and alignment with social responsibility targets.
- **Corporate Social Responsibility (CSR) Reporting Audit:** This audit evaluates the accuracy and transparency of the organization's CSR reporting, ensuring that social targets and achievements are properly disclosed.
- **Philanthropic Initiatives Audit:** This audit reviews the organization's charitable and philanthropic activities to ensure they align with the organization's social responsibility goals.
- **Supplier Diversity Audit:** This audit assesses the organization's efforts to promote supplier diversity and engage with minority-owned, women-owned, or small businesses.
- **Social Accountability and Ethical Practices Audit:** This audit examines the organization's commitment to ethical business practices and social accountability throughout its operations.
- **Social Performance Metrics and Reporting Audit:** This audit ensures that the organization has appropriate metrics and systems in place to monitor and report on its social performance.
- **Employee Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees regarding social responsibility and the organization's social targets.
- **Social Governance and Oversight Audit:** This audit evaluates the effectiveness of the organization's governance structure and oversight processes related to social responsibility.
- **Impact Measurement and Evaluation Audit:** This audit reviews the organization's methods for measuring and evaluating the impact of its social programs and initiatives.

ESG | Are you getting the balance right?

Governance (G)

- **Corporate Governance Audit:** This audit assesses the overall governance framework, including the roles and responsibilities of the board of directors, management, and committees, and the effectiveness of the oversight provided.
- **Compliance Audit:** This audit reviews the organization's compliance with laws, regulations, and internal policies relevant to its operations.
- **Code of Conduct and Ethics Audit:** This audit examines the organization's code of conduct and ethics policies to ensure they are communicated effectively and followed by employees and stakeholders.
- **Risk Management Audit:** This audit assesses the organization's risk management processes and the effectiveness of risk identification, assessment, and mitigation strategies.
- **Internal Control Audit:** This audit reviews the organization's internal control environment to ensure that appropriate controls are in place to mitigate operational, financial, and compliance risks.
- **Financial Reporting and Accounting Audit:** This audit evaluates the accuracy and reliability of the organization's financial reporting and accounting practices.
- **Board Independence and Composition Audit:** This audit assesses the independence and composition of the board of directors to ensure effective oversight and avoid conflicts of interest.
- **Executive Compensation Audit:** This audit examines the organization's executive compensation policies to ensure alignment with the company's performance and shareholder interests.
- **Whistleblower Program Audit:** This audit reviews the organization's whistleblower program to ensure that it provides a confidential and effective means for reporting concerns.
- **Succession Planning and Talent Management Audit:** This audit evaluates the organization's succession planning and talent management strategies to ensure leadership continuity and employee development.
- **Cybersecurity Governance Audit:** This audit focuses on evaluating the organization's cybersecurity governance practices and the board's oversight of cybersecurity risks.
- **IT Governance Audit:** This audit assesses the alignment of IT strategies and initiatives with the organization's overall objectives and the effectiveness of IT oversight.
- **Data Governance Audit:** This audit reviews the organization's data governance practices to ensure proper management, security, and compliance with data-related policies.
- **Governance Training and Awareness Audit:** This audit assesses the training and awareness programs provided to employees and stakeholders regarding governance principles and practices.

Third-Party Risk Management | How well do you really know your third parties?

- **Vendor Management Audit:** This audit assesses how the organization selects, monitors, and manages its vendors to ensure they meet specific criteria, provide quality products or services, and adhere to contractual obligations.
- **Supplier Compliance Audit:** This audit evaluates whether the organization's suppliers comply with relevant regulations, standards, and contractual requirements.
- **Due Diligence Audit:** This audit examines the process of evaluating and selecting third-party vendors or partners to identify potential risks and assess the suitability of these relationships.
- **Contract Compliance Audit:** This audit reviews the contracts with third parties to ensure that both parties are fulfilling their obligations and that the agreements align with legal and regulatory requirements.
- **Information Security and Data Privacy Audit:** This audit focuses on how the organization's third-party vendors handle sensitive information and data, ensuring that appropriate security measures are in place and that privacy regulations are followed.
- **Anti-Corruption and Bribery Audit:** This audit investigates the organization's third-party relationships to ensure compliance with anti-corruption laws and regulations, safeguarding against unethical practices.
- **Financial Audit of Third-Party Transactions:** This audit examines the financial transactions and payments made to third parties to detect any irregularities or potential fraud.
- **Performance and Service Level Audit:** This audit assesses the performance of third-party vendors in delivering products or services as per agreed-upon service level agreements (SLAs).
- **Business Continuity and Disaster Recovery Audit:** This audit evaluates whether third-party vendors have adequate plans and measures in place to ensure business continuity and recovery in case of emergencies or disasters.
- **Ethics and Social Responsibility Audit:** This audit reviews third-party vendors' policies and practices regarding ethical and social responsibility aspects, such as labor practices, environmental sustainability, and diversity.
- **Third-Party Risk Assessment and Management Audit:** This audit analyzes how the organization identifies, evaluates, and mitigates risks associated with its third-party relationships.

Merger and Acquisition Integration | Are you buying a corruption fine, cyber issues, or the wrong culture?

- **Financial Due Diligence:** This audit focuses on assessing the financial health and performance of the target company. It involves a thorough examination of the target company's financial statements, cash flow, assets, liabilities, and financial projections.
- **Tax Due Diligence:** This audit examines the target company's tax compliance history, potential tax liabilities, and the effectiveness of its tax strategies.
- **Legal and Regulatory Compliance Audit:** This audit ensures that the target company complies with all relevant laws and regulations, including industry-specific regulations, environmental laws, labor laws, and corporate governance requirements.
- **IT Systems and Cybersecurity Audit:** This audit assesses the target company's IT infrastructure, information security measures, and data privacy practices to identify potential vulnerabilities and risks.
- **Human Resources and Employee Benefits Audit:** This audit reviews the target company's HR policies, employment contracts, benefits plans, and potential labor issues that may arise during the integration process.
- **Intellectual Property Audit:** This audit evaluates the target company's intellectual property portfolio, including patents, trademarks, copyrights, and trade secrets, to ensure they are properly protected and documented.
- **Contract and Agreement Audit:** This audit examines the target company's contracts and agreements with customers, suppliers, and partners to identify any unfavorable terms or potential legal issues.
- **Environmental and Sustainability Audit:** This audit assesses the target company's environmental impact and sustainability initiatives to identify any potential liabilities or risks associated with environmental compliance.
- **Cultural Alignment Audit:** This audit evaluates the cultural compatibility between the two companies to identify potential challenges in integrating their workforces and operations.
- **Synergy Assessment Audit:** This audit analyzes the potential synergies and cost savings that can be achieved through the merger or acquisition and assesses the feasibility of achieving those targets.
- **Post-Merger Integration Audit:** This audit evaluates the effectiveness of the integration process after the merger or acquisition has taken place, identifying any issues or areas that require further attention.
- **Benefits Realization Audit:** This audit determines if benefits expected have been realized post implementation.

Digital Transformation | Have you envisioned the opportunities and risk of the end state?

- **Project Management Audit:** This audit assesses the planning, execution, and control of the digital transformation project. It ensures that project management practices are in place, timelines and budgets are adhered to, and potential risks are being managed effectively.
- **Technology Infrastructure Audit:** This audit focuses on evaluating the organization's existing technology infrastructure and its readiness to support the digital transformation initiatives. It examines factors such as scalability, security, data storage, and network capabilities.
- **Data Governance and Management Audit:** This audit reviews how the organization collects, stores, processes, and protects data during the digital transformation. It ensures compliance with data protection regulations and assesses data quality and integrity.
- **Cybersecurity Audit:** This audit examines the organization's cybersecurity measures and evaluates the robustness of its defenses against cyber threats, especially as new digital solutions are implemented.
- **Vendor and Third-Party Management Audit:** This audit assesses the selection and management of third-party vendors involved in the digital transformation project, ensuring that they meet security and compliance requirements.
- **Change Management Audit:** This audit evaluates the change management strategies used during the digital transformation to assess the impact on employees, identify potential resistance, and ensure effective communication.
- **User Experience and Customer Journey Audit:** This audit reviews the user experience design and customer journey for digital products and services, ensuring they meet the intended objectives and provide a seamless experience.
- **IT Governance Audit:** This audit assesses the governance structure for IT decision-making and the alignment of digital transformation projects with the organization's overall IT strategy.
- **Compliance and Regulatory Audit:** This audit ensures that digital transformation projects comply with relevant industry regulations, data protection laws, and other legal requirements.
- **Training and Skill Development Audit:** This audit examines the training programs and skill development initiatives put in place to equip employees with the necessary capabilities to adopt and leverage digital tools effectively.
- **Return on Investment (ROI) Audit:** This audit assesses the financial performance and ROI of digital transformation projects to determine their impact on the organization's bottom line.

Data Analytics and Continuous Monitoring | Do you feel competitors have better insight?

- **Data Quality Audit:** This audit assesses the quality, completeness, and accuracy of data used for analytics. It verifies if data sources are reliable and whether data is properly collected, stored, and processed.
- **Data Governance Audit:** This audit evaluates the organization's data management practices, policies, and procedures to ensure that data is handled securely, ethically, and in compliance with relevant regulations.
- **Data Privacy Audit:** This audit focuses on assessing the organization's adherence to data privacy laws and regulations. It ensures that personal and sensitive data is handled appropriately and that proper consent mechanisms are in place.
- **Data Security Audit:** This audit examines the organization's data security measures, including access controls, encryption, and vulnerability assessments, to protect data from unauthorized access and cyber threats.
- **Data Analytics Process Audit:** This audit reviews the end-to-end data analytics process, including data collection, preprocessing, analysis, and reporting. It ensures that the analytical methods and models are accurate, reliable, and aligned with the organization's objectives.
- **Model Validation Audit:** For organizations using predictive models and algorithms for decision-making, a model validation audit verifies the accuracy and reliability of these models and checks if they are producing valid and actionable results.
- **Data Retention and Deletion Audit:** This audit assesses the organization's data retention policies to ensure compliance with data retention regulations and evaluates the proper deletion of data when it is no longer needed.
- **Data Access Audit:** This audit examines the access controls and permissions granted to users who interact with data analytics tools and systems. It ensures that access is granted based on the principle of least privilege.
- **Vendor Management Audit:** For organizations relying on third-party data analytics vendors, this audit evaluates the vendor's data handling practices, security measures, and compliance with contractual agreements.
- **Compliance Audit:** This broader audit assesses the organization's compliance with relevant laws, regulations, and internal policies related to data analytics, including data protection, consumer rights, and industry-specific guidelines.
- **Data Visualization Audit:** This audit focuses on the accuracy and clarity of data visualizations and reports, ensuring that they present insights in a comprehensible and unbiased manner.
- **Data Ethics Audit:** An audit of data ethics evaluates the organization's practices related to the ethical use of data, including transparency, fairness, and the avoidance of bias in data analytics.

Workforce Transformation & Organizational Readiness | Are you optimizing and sustaining value from critical resources?

- **Strategic Planning Audit:** This audit evaluates the organization's strategic planning process, ensuring that it is comprehensive, aligned with the organization's mission and vision, and involves key stakeholders.
- **Change Management Audit:** This audit assesses the organization's change management processes, including how it plans, implements, and communicates changes to employees and other stakeholders.
- **Leadership and Talent Audit:** This audit reviews the organization's leadership capabilities and talent development strategies to ensure that it has the right people in the right positions to drive success.
- **Training and Development Audit:** This audit examines the organization's training and development programs to determine if they are sufficient to equip employees with the necessary skills and knowledge.
- **Organizational Culture Audit:** This audit assesses the organization's culture, values, and norms to ensure they align with the strategic objectives and support desired behaviors.
- **Communication Audit:** This audit evaluates the organization's communication processes to determine if information flows effectively among employees, departments, and management.
- **Risk Management Audit:** This audit assesses the organization's risk management practices to identify potential threats and weaknesses in its ability to respond to risks.
- **Financial Preparedness Audit:** This audit reviews the organization's financial stability, budgeting practices, and contingency plans to ensure it is financially prepared for various scenarios.
- **Resource Allocation Audit:** This audit examines how the organization allocates its resources (financial, human, and technological) to support its objectives and initiatives.
- **IT Audit:** This audit assesses the organization's information technology infrastructure, systems, and cybersecurity measures to ensure they support the organization's needs and protect against threats.
- **Project Management Audit:** This audit reviews the organization's project management processes to determine if projects are effectively planned, executed, and monitored.
- **Operational Efficiency Audit:** This audit evaluates the efficiency of the organization's operational processes, identifying areas for improvement and streamlining.
- **Supplier and Vendor Audit:** This audit assesses the organization's relationships with suppliers and vendors to ensure they meet quality and reliability standards.
- **Business Continuity and Disaster Recovery Audit:** This audit examines the organization's plans for business continuity and disaster recovery, ensuring it can respond effectively to disruptions.
- **Regulatory Compliance Audit:** This audit assesses the organization's compliance with relevant laws, regulations, and industry standards.

Insurance | Read the fine print: Do you really know the current cost/benefit of insurance?

- **Underwriting Audit:** This audit reviews the underwriting process to ensure that insurance policies are issued in accordance with established guidelines, and risks are properly assessed and priced.
- **Claims Management Audit:** This audit assesses the claims handling process, ensuring that claims are processed efficiently, accurately, and in compliance with the insurance policy terms.
- **Compliance Audit:** This audit examines the insurance company's adherence to regulatory requirements, industry standards, and internal policies.
- **Risk Management Audit:** This audit evaluates the effectiveness of the insurance company's risk management practices, including risk identification, assessment, and mitigation strategies.
- **Reinsurance Audit:** For insurance companies that use reinsurance, this audit reviews reinsurance arrangements and ensures they align with the company's risk management objectives.
- **Premium Audit:** This audit reviews the premium calculation and collection process to ensure accuracy and compliance with policy terms.
- **Policyholder Services Audit:** This audit assesses customer service processes, policyholder communications, and complaint handling to ensure high levels of customer satisfaction.
- **Financial Controls Audit:** This audit examines the financial controls, accounting practices, and financial reporting of the insurance company to ensure accuracy and integrity of financial information.
- **Information Security Audit:** This audit assesses the company's information security measures, including data protection, access controls, and cybersecurity practices.
- **Product Development Audit:** This audit reviews the process of designing and introducing new insurance products to ensure they meet regulatory requirements and align with the company's risk appetite.
- **Sales and Marketing Practices Audit:** This audit assesses the sales and marketing practices of the insurance company to ensure they are fair, transparent, and compliant with relevant regulations.
- **Claims Reserving Audit:** This audit evaluates the adequacy of claims reserves set aside by the insurance company to cover future claim payments.
- ***Actuarial Audit:*** For companies using actuaries to assess risks and set insurance premiums, this audit reviews actuarial practices and compliance with professional standards.
- **IT Systems Audit:** This audit assesses the insurance company's information technology systems and infrastructure to ensure they support the organization's operations securely and efficiently.
- **Agency and Broker Management Audit:** This audit reviews the relationship and performance of insurance agents and brokers to ensure proper oversight and compliance.

Economic and Financial Adversity | How has the economy impacted your business model?

- **Financial Risk Management Audit:** This audit assesses the organization's financial risk exposure, including liquidity risk, market risk, credit risk, and operational risk. It evaluates risk management practices to identify vulnerabilities during adverse economic conditions.
- **Business Continuity and Disaster Recovery Audit:** This audit examines the organization's plans and preparedness to continue critical operations during economic and financial crises, ensuring that business continuity and disaster recovery plans are robust.
- **Stress Testing Audit:** This audit reviews the organization's stress testing methodologies and scenarios to assess how the company's financial position would be affected under adverse economic conditions.
- **Expense Management Audit:** This audit evaluates the organization's expense management practices to identify opportunities for cost reduction and efficiency improvements during economic challenges.
- **Financial Reporting Integrity Audit:** This audit ensures the accuracy and integrity of financial reporting during economic adversity, helping to maintain transparency and confidence in the organization's financial statements.
- **Debt and Credit Management Audit:** This audit assesses the organization's debt and credit management practices to identify potential risks related to debt levels and credit exposures during economic downturns.
- **Revenue Recognition Audit:** This audit reviews the organization's revenue recognition policies and practices to ensure they align with accounting standards and accurately reflect revenue during economic challenges.
- **Supply Chain and Vendor Risk Audit:** This audit examines the organization's supply chain and vendor relationships to identify potential risks and vulnerabilities related to disruptions in the supply chain.
- **Working Capital Management Audit:** This audit evaluates the organization's working capital management practices, including inventory management, accounts receivable, and accounts payable, to optimize liquidity during economic adversity.
- **Investment Management Audit:** This audit reviews the organization's investment portfolio and investment management practices to assess risks and potential impacts on investment values during economic downturns.
- **Cost of Capital Audit:** This audit assesses the organization's cost of capital and capital structure to ensure it remains sustainable during economic challenges.
- **Credit Underwriting and Monitoring Audit:** For financial institutions, this audit examines credit underwriting and monitoring processes to identify potential credit risks and assess the quality of the loan portfolio.
- **Credit Loss Provisioning Audit:** This audit reviews the organization's credit loss provisioning practices to ensure they are in line with regulatory requirements and reflect the economic conditions accurately.
- **Regulatory Compliance Audit:** This broader audit assesses the organization's compliance with relevant financial and economic regulations, ensuring the company meets its obligations during challenging economic times.

Business Resilience (Including Third Parties) | Who do you rely on when crisis hits?

- **Business Continuity Planning Audit:** This audit assesses the organization's business continuity plans, ensuring they are comprehensive, up-to-date, and aligned with the organization's critical functions and priorities.
- **Disaster Recovery Audit:** This audit reviews the organization's disaster recovery plans and measures, including data backup and restoration processes, to ensure the organization can quickly recover from IT-related disruptions.
- **Crisis Management Audit:** This audit evaluates the organization's crisis management strategies, protocols, and decision-making processes to ensure effective responses to emergencies and unexpected events.
- **Risk Assessment and Management Audit:** This audit assesses the organization's risk assessment practices, including the identification and evaluation of potential risks and the implementation of risk mitigation strategies.
- **Supply Chain Resilience Audit:** This audit examines the organization's supply chain resilience, identifying vulnerabilities and ensuring contingency plans are in place to address disruptions in the supply chain.
- **IT Resilience Audit:** This audit reviews the organization's IT infrastructure, systems, and processes to ensure they are resilient to cyber threats, data breaches, and other IT-related risks.
- **Employee Continuity Audit:** This audit assesses the organization's plans and measures to ensure the safety and well-being of employees during disruptions, including remote work capabilities and employee support programs.
- **Financial Resilience Audit:** This audit evaluates the organization's financial preparedness to withstand adverse economic conditions, including stress testing, liquidity management, and contingency funding plans.
- **Vendor and Outsourcing Resilience Audit:** This audit examines the organization's relationships with vendors and outsourced service providers to ensure they have robust business continuity and disaster recovery plans.
- **Communication and Stakeholder Management Audit:** This audit assesses the organization's communication strategies and stakeholder management during crises to maintain trust and transparency.
- **Regulatory Compliance Audit:** This audit ensures the organization complies with relevant regulations and standards related to business resilience and continuity planning.
- **Incident Response Audit:** This audit reviews the organization's incident response procedures to ensure they are well-defined, understood, and regularly tested.
- **Physical Security Audit:** This audit evaluates the organization's physical security measures to protect assets and facilities from potential threats.
- **Training and Awareness Audit:** This audit assesses the organization's training and awareness programs related to business resilience, ensuring employees are adequately prepared to respond to disruptions.
- **Testing and Simulation Audit:** This audit examines the organization's testing and simulation exercises for business resilience plans, ensuring they are conducted regularly and effectively to identify areas for improvement.

Capital Projects and Operations | Are you confident you were billed fairly?

- **Capital Expenditure Audit:** This audit examines the organization's capital expenditure process to ensure that investments are aligned with strategic objectives, adequately planned, and appropriately authorized.
- **Project Management Audit:** This audit reviews the organization's project management practices, including planning, execution, monitoring, and control of capital projects, to identify potential risks and areas for improvement.
- **Cost Control and Cost Estimation Audit:** This audit assesses the accuracy and reliability of cost estimates for capital projects and examines cost control measures to identify cost overruns and deviations.
- **Contract Management Audit:** This audit evaluates the organization's contract management processes for capital projects, ensuring compliance with contract terms and conditions, and verifying that vendors and contractors deliver as per agreements.
- **Schedule Compliance Audit:** This audit examines the adherence to project schedules and timelines to identify delays and potential impacts on project outcomes.
- **Quality Assurance and Quality Control Audit:** This audit reviews the organization's quality assurance and quality control processes for capital projects to ensure that deliverables meet established standards.
- **Procurement and Vendor Audit:** This audit assesses the organization's procurement practices, vendor selection, and performance evaluation to ensure transparency and compliance with procurement policies.
- **Health, Safety, and Environment (HSE) Audit:** This audit evaluates the organization's HSE practices during capital projects to identify potential risks and ensure compliance with safety regulations and environmental standards.
- **Resource Allocation and Utilization Audit:** This audit examines the allocation and utilization of resources, including labour and equipment, to ensure efficient use during capital projects.
- **Change Order and Variance Analysis Audit:** This audit reviews change orders and variance analysis for capital projects to assess the impact on project budgets and schedules.
- **Internal Controls Audit:** This audit assesses the effectiveness of internal controls in place to manage risks related to capital projects and operations.
- **Compliance with Regulatory and Legal Requirements Audit:** This audit ensures that capital projects and operations comply with relevant regulatory and legal requirements, permits, and licenses.
- **Asset Management Audit:** This audit examines asset management practices, including maintenance and disposal strategies, to optimize the life cycle of capital assets.
- **Data and Documentation Management Audit:** This audit assesses the organization's data and documentation management related to capital projects and operations to ensure accuracy and accessibility of information.
- **Project Closure and Lessons Learned Audit:** This audit reviews the closure of capital projects and analyzes lessons learned to identify best practices and areas for improvement in future projects.

Fraud and Corruption | How much has the cost of living increase impacted fraud risk?

- **Fraud Risk Assessment Audit:** This audit assesses the organization's vulnerability to fraud by identifying areas where fraud is more likely to occur and evaluating the effectiveness of existing fraud prevention measures.
- **Anti-Corruption Compliance Audit:** This audit evaluates the organization's compliance with anti-corruption laws and regulations, such as the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act.
- **Whistleblower Program Audit:** This audit reviews the organization's whistleblower program to ensure that employees can report fraud and corruption anonymously and without fear of retaliation.
- **Expense Reimbursement Audit:** This audit examines employee expense reimbursements to detect any instances of fraudulent or inappropriate claims.
- **Vendor and Supplier Audit:** This audit assesses the relationships with vendors and suppliers to identify potential conflicts of interest and instances of corruption.
- **Employee Background Checks Audit:** This audit reviews the organization's procedures for conducting background checks on employees to ensure that potential risks of fraud and corruption are adequately assessed before hiring.
- **Procurement Fraud Audit:** This audit examines the procurement process to identify any fraudulent activities, such as bid rigging or kickbacks.
- **Conflicts of Interest Audit:** This audit assesses the organization's policies and procedures for managing conflicts of interest among employees and key stakeholders.
- **Gifts, Entertainment, and Hospitality Audit:** This audit reviews the organization's policies and practices regarding gifts, entertainment, and hospitality to prevent potential corrupt practices.
- **Asset Misappropriation Audit:** This audit examines the organization's assets and inventory to detect any instances of theft or misappropriation.
- **Internal Controls Audit:** This audit assesses the effectiveness of internal controls in place to prevent and detect fraudulent activities.
- **Compliance with Code of Conduct and Ethics Policies Audit:** This audit ensures that the organization's code of conduct and ethics policies are communicated effectively, understood by employees, and followed throughout the organization.
- **Financial Statement Fraud Audit:** This audit examines financial transactions and records to identify any indications of fraudulent financial reporting.
- **Data Analytics for Fraud Detection Audit:** This audit uses data analytics techniques to identify patterns and anomalies indicative of potential fraud and corruption.
- **Investigative Audit:** In response to specific fraud allegations or suspicions, this audit involves detailed investigations to gather evidence and determine the extent of fraudulent activities.
- **Workplace Investigations:** In response to specific allegations of harassment, misconduct, etc., this audit assesses the allegations for validity and the extent of misconduct, providing recommendations for enhancing the workplace.

Contributors

Richard Arthurs
National Internal Audit Leader

Olena Batuev
Business Intelligence Developer

Drew Buhr
National Cyber Security Assessment Lead

Craig Burkart
National Leader, Insurance Advisory

Gord Chalk
Consulting Leader, Energy and Utilities

James Dyack
Southern Alberta Lead, Valuations and Litigation Support

Johnny Earl
Managing Director, Corporate Finance

Soumya Ghosh
Director, Digital Transformation and Advisory

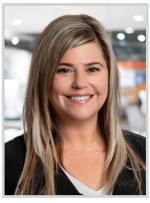
Adriana Gliga
Privacy Lead

Wendy Gnenz
Partner, Digital Strategy and Planning

Mary Larson
Leader, Organizational Renewal

Chris Law
Partner, Cyber Security

Jason Lee
Partner, Data and Analytics



Lisa Majeau-Gordon
National Leader, Forensics and Litigation Support

Len Nanjad
Partner, Organization Change Management

Contributors

Eugene Ng
Central Canada Lead,
Cyber Security

Cameron Ollenberger
Senior Manager,
Enterprise Risk Services

Edward Olson
ESG Leader

Hash Qureshi
Partner, Enterprise Risk Services

Mark Reynolds
Managing Director,
Corporate Finance

Mike Reynolds
Managing Director,
Corporate Finance

Ian Shaule
Director, Advanced Analytics

Lee Thiessen
National Leader, Real
Estate and Construction

Cliff Trollope
National Leader,
Business Resilience
Services

Colin Wenngatz
Leader, Enterprise Analytics

Giovanni Worsley
Partner, Property Tax
Services

About MNP

National in scope and local in focus, MNP is one of Canada's leading professional services firms — proudly serving individuals, businesses, and organizations since 1958. Through the development of strong relationships, we provide client-focused accounting, consulting, tax, and digital services. Our clients benefit from personalized strategies with a local perspective to fuel success wherever business takes them.

For more information, contact:

Richard Arthurs, FCPA, FCMA, MBA, CFE, CIA, CRMA, QIAL
National Leader, Internal Audit
richard.arthurs@mnp.ca

Mariesa Fett, CPA, CA, ABCP, CRMA, ICD.D
National Enterprise Risk Services Leader
mariesa.fett@mnp.ca

PRAXITY™
Empowering Business Globally