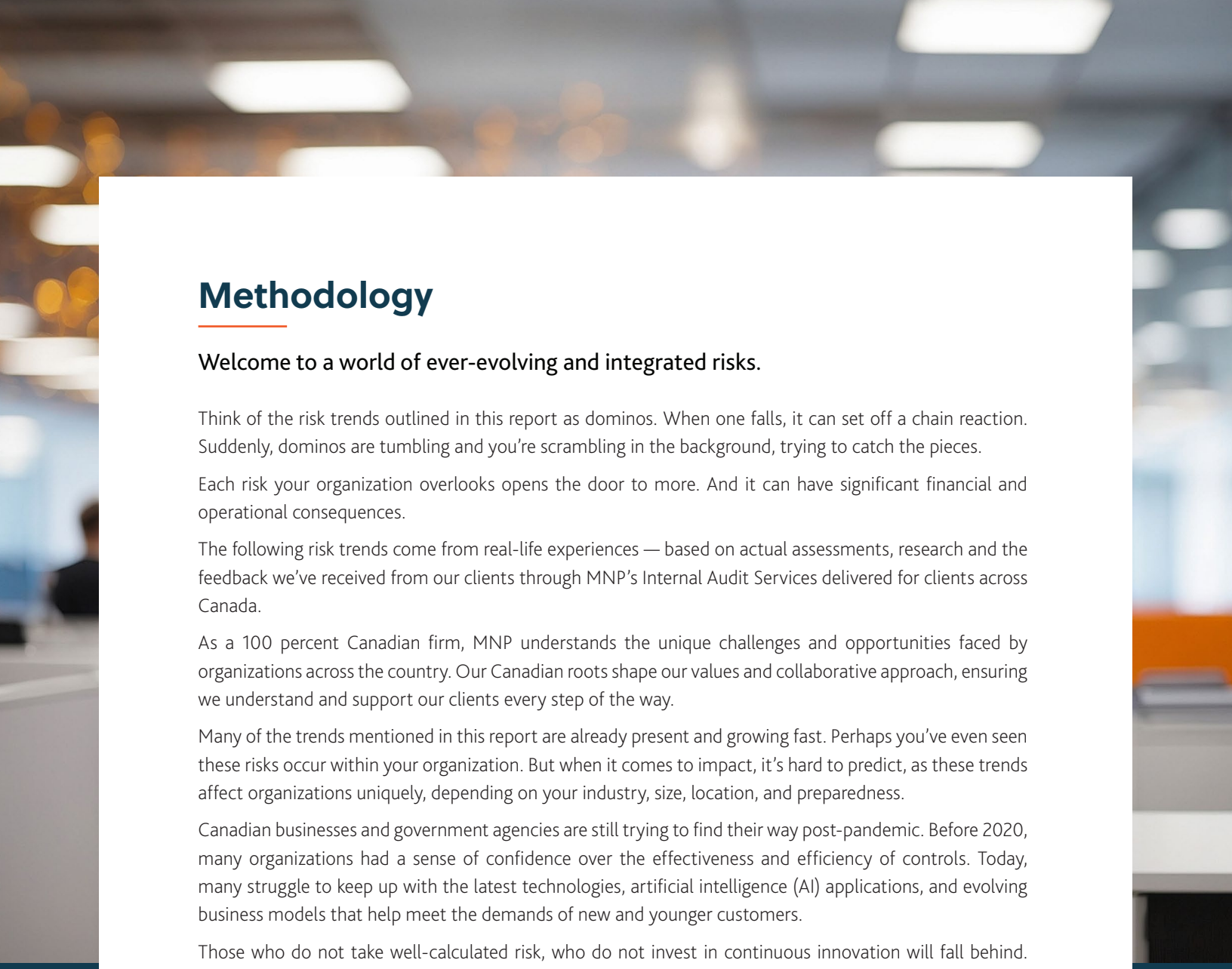
Risk Trends in 2025 and Beyond

A leader's guide to navigating Canada's uncertain digital future

MNP.ca



Methodology

Welcome to a world of ever-evolving and integrated risks.

Think of the risk trends outlined in this report as dominos. When one falls, it can set off a chain reaction. Suddenly, dominos are tumbling and you're scrambling in the background, trying to catch the pieces.

Each risk your organization overlooks opens the door to more. And it can have significant financial and operational consequences.

The following risk trends come from real-life experiences — based on actual assessments, research and the feedback we've received from our clients through MNP's Internal Audit Services delivered for clients across Canada.

As a 100 percent Canadian firm, MNP understands the unique challenges and opportunities faced by organizations across the country. Our Canadian roots shape our values and collaborative approach, ensuring we understand and support our clients every step of the way.

Many of the trends mentioned in this report are already present and growing fast. Perhaps you've even seen these risks occur within your organization. But when it comes to impact, it's hard to predict, as these trends affect organizations uniquely, depending on your industry, size, location, and preparedness.

Canadian businesses and government agencies are still trying to find their way post-pandemic. Before 2020, many organizations had a sense of confidence over the effectiveness and efficiency of controls. Today, many struggle to keep up with the latest technologies, artificial intelligence (AI) applications, and evolving business models that help meet the demands of new and younger customers.

Those who do not take well-calculated risk, who do not invest in continuous innovation will fall behind. But at the same time, they must not allow hackers or fraudsters to cause losses or disruption. The most successful will invest proactively in risk trend awareness, enterprise risk management, balanced internal controls, a high-value internal audit function, and good governance.

The findings in this report highlight essential practices and drive home the importance of the basics. Asking the right questions is important, but prevention and preparedness are more critical — and are often less costly than reacting to problems once they arise.

This report digs into these risks, highlights key questions, and points out red flags you should watch for.

The only certainty seems to be living with uncertainty. Though, with uncertainty comes opportunity.

MNP Internal Audit Services Team

Table of Contents

The Digital Minds of Future Leaders

Do your future leaders understand your critical technology?

Jason Lee | Machine Learning and AI
Soumya Ghosh | Digital Transformation and Advisory
Wendy Gnenz | Digital
Mary Larson | Organizational Renewal

In today's fast-paced world, the future of leadership hinges on digital transformation and retaining the digital-minded leaders required to succeed. It's not just about being tech-savvy — it's about leveraging technology to drive innovation, efficiency, and growth. The COVID-19 pandemic fast-tracked digital transformation plans, with many companies rushing to adopt new technologies. But now, they're realizing they might not have the right people to maximize these advancements.

Demographic shifts and workforce implications

Consider this: Canada has an aging population with an average life expectancy of 82.3 years, one of the highest in the world. According to the most recent Canadian Census, between 2016 and 2021, more than 1.4 million Canadians joined the ranks of those aged 55 and older. In 2021 alone, one in five working-age individuals were aged 55 to 62, marking an all-time high.

This demographic shift delays retirements and limits opportunities for the leaders of tomorrow, impacting business operations. To achieve sustainable success in the rapidly changing digital landscape, your organization must leverage the digital intelligence of the next generation.

A 2023 report from the Canadian Federation of Independent Business (CFIB) highlighted that 76 percent of business owners plan to exit their businesses within the next decade. That's more than $2 trillion worth of business assets changing hands. The question is, can Canadian businesses survive, or will they be acquired, without digital-minded future leaders?

Organizations must prepare future leaders to manage and grow these enterprises while managing associated risks. One of the primary risks is the shortage of necessary skills. Many companies lack employees with the specialized skills needed for the future, making continuous learning and development essential to remain competitive.

Competing for the top digital minds

Another significant risk is talent competition. The race for top talent, especially those with specific skill sets, is fierce. Enterprises face talent shortages and higher recruitment costs. Future leaders must develop strategic recruitment and retention plans to attract and retain the top digitally minded talent.

To reduce turnover, businesses must create a positive work environment, and a culture of engagement and loyalty. Flexible work arrangements will go far in retaining the leaders of tomorrow.

Why stop there? Here are other risks to consider:

- Toxic Culture
- Weak leadership
- Inadequate succession planning
- Inadequate workforce diversity and lack of inclusivity
- Remote work challenges
- Reduced productivity due to employee well-being issues
- Impact of automation and AI creating new risks

Questions to ask:

- Are you recruiting, developing, and retaining the digital minds your organization requires to be successful?
- Are your organizational structure and job descriptions designed to optimize value from your digital assets?
- Are you confident in sourcing future leaders who can compete and deliver strategic value in a digital world?

Red flag risks:

- Employees haven't received training on new and advanced digital technologies
- The organizational structure and job descriptions have not been fine tuned to leverage the digital technology needed to achieve strategic targets
- The culture is toxic and is seeing high turnover of high potential leaders

Cyber security

Are you prepared to detect and defend against human hackers, especially those leveraging AI?

Chris Law | Defensive Cyber Security
Adriana Gliga | Payment Card Industry, Privacy and Data Governance
Eugene Ng | Cyber Security
Drew Buhr | Cyber Security Risk
Ian Shaule | Advanced Analytics
Colin Wenngatz | Retail AnalyticsCameron Ollenberger | Risk Analytics

Cyber security is a hot topic that's here to stay. Every year, hackers get more sophisticated, and their attacks more damaging. According to the Canadian Centre for Cyber Security, in 2023 alone, over 70,000 cyber incidents were reported in Canada, a 25 percent increase from the previous year. It cost Canadian cyber victims more than $3 billion in mitigation, recovery, and long-term damage control.

The growing threats

Picture this: you get an email that looks like it's from your bank, asking you to update your password. You click the link, type in your old password and create a new one. Little do you know; a hacker is using your old password to access your credit card. This is a classic phishing attack.

The introduction of generative artificial intelligence (AI) is making it harder to distinguish between legitimate and fraudulent communications. To combat this, organizations should implement robust email filters and educate employees to recognize phishing attempts. Multi-factor authentication can add an extra layer of security.

Ransomware attacks are another major threat. Hackers can lock an organization out of its own systems, denying access to data, and demand a ransom to restore access. Keeping software updated with the latest security patches is crucial to fend off these attacks. Also, having a data storage strategy, that maintains timely and reliable backups, may allow you to bypass paying the ransom. The most important control is optimizing your employees' cyber awareness, so they know how to avoid phishing and insider risk situations. Insiders should be guided by cyber-related policy, which would also outline the acceptable and not acceptable use of AI.

Addressing key vulnerabilities

The rise of remote work has introduced new vulnerabilities. Without the structured security of an office environment, employees' home networks can be weak points. Using virtual private networks (VPNs), keeping security software updated, and educating employees on safe remote work practices can help secure these environments.

As AI and machine-learning systems are being manipulated by hackers in new ways to commit cyber crime, regular audits, strict data validation, and contingency plans can help address potential AI-related vulnerabilities. Additionally, the National Institute of Standards and Technology has developed technical standards — including international ones — that promote trust in AI technologies and systems.

While it's common to outsource tasks and services, it comes with risks. Third-party vendors can be entry points for cyber attacks. Thorough security assessments and enforcing strict access controls for these partners are essential.

In this ever-evolving trend, proactive measures, continuous monitoring, and employee education are key. By understanding and addressing these key risk trends, your business can better safeguard its assets and ensure long-term stability.

Why stop there? Here are other risks to consider:

- Deepfake AI voice and video manipulation
- Data breaches
- Cloud security threats
- IoT (Internet of Things) vulnerabilities
- Mobile security threats

Questions to ask:

- What information technology (IT) changes have been made recently or are planned over the next three years? Could these changes weaken or remove controls?
- Can employees initiate large financial transactions remotely? Do you have a policy for how and where large financial transactions need to occur?
- Do you conduct background checks on all employees and third-party individuals who are given privileged access rights to your systems?
- How effective are your training and tools for preventing phishing attacks?

Red flag risks:

- Employees consistently do not detect cyber threats
- Extensive period since the internal audit function conducted cyber security audits
- Your IT security function hasn't kept up with evolving security measures implemented by your cloud service provider
- No policies in place around the ethical use of AI

Artificial Intelligence Ethical Dilemmas

Can you say with confidence that AI will be more of an opportunity than a risk?

Jason Lee | AI, Data and Analytics

The Canadian AI market is booming. Current projections have it reaching US$4.13 billion in 2024 and growing to US$18.5 billion by 2030, according to Statista. AI is transforming businesses, making them smarter and more efficient. But AI brings a whole host of ethical dilemmas that organizations must navigate.

One of the biggest concerns is bias and discrimination. AI systems are often programmed with distinct biases. For example, an AI system might favour one group over another simply because the programmer influenced the code to prioritize certain options, or the training data was biased.

To combat this, businesses must ensure that AI is programmed and trained on diverse and representative data sets. Also, the AI may need complementary technology to help it make better decisions, such as facial recognition scanners. Regular audits and testing can also help detect and correct these unwanted biases.

Privacy is a significant issue with AI's data collection and analysis capabilities, which can threaten individual privacy by identifying people and predicting personal attributes. This can lead to misuse of personal information, such as inadequately protected health data from a smart watch. Strong governance practices are essential to protect privacy and ensure ethical data use.

Be prepared, not sorry

Misinformation and deepfakes are also raising concerns. AI can create convincing content to spread misinformation or commit fraud. Organizations need to develop tools to detect and counteract deepfakes, ensuring the integrity of their information and their systems.

There is also a need to educate individuals to be skeptical about who is establishing contact. For example, if someone suspects the person calling is not who they claim to be, they should ask a complex question that only the genuine person would know the answer to.

AI systems are not immune to attacks. Adversarial attacks can manipulate AI inputs to produce incorrect outputs, leading to security breaches or bad decisions. Implementing robust security measures, like adversarial training and continuous monitoring, can help keep AI systems safe and functioning as intended.

The rise of AI-driven surveillance systems raises concerns about mass surveillance and its impact on civil liberties. Organizations must ensure that their surveillance practices are transparent, ethical, and protective of individual rights to maintain public trust.

Lastly, AI can be used to enhance cyber attacks, create persuasive misinformation campaigns, and automate spam and phishing. To protect against these threats, businesses need to stay vigilant and proactive in developing controls and countermeasures.

Why stop there? Here are other risks to consider:

- Misuse of autonomous drones and weapons
- Job displacement when technology replaces manual labour
- Lack of explainability due to user ignorance of code biases
- Everyday technologies that, unbeknownst to individuals, copy, store and use data from their laptop, smartphone, or watch

Questions to consider:

- How is AI impacting your organization and what are you doing to get ahead of it?
- Do you have an inventory of all the ways you're using AI? Has your organization created a policy identifying how to use it correctly?
- Have you asked your software and hardware providers how they intend to use AI?
- Can you turn off unacceptable AI use?

Red flag risks:

- Embedded AI technology is found to be allowing unwanted access to private or confidential data
- The ethics and biases of AI result in suboptimal decision making or increasing the potential for future risks to occur
- Misuse of AI creates negative or inaccurate data that may be shared publicly (i.e. ESG metrics)

High-value, Sensitive, Private and Confidential Data

Who knows where your private and confidential data resides, and can you trust your controls?

Adriana Gliga | Payment Card Industry, Privacy and Data Governance

As organizations uncover the potential of their data, they're learning how to harness it for incredible benefits. But safeguarding this data is more critical than ever.

Consider the example of healthcare providers. By integrating patient data from electronic health records with real-time health monitoring devices, they can predict and prevent health issues, reduce re-admissions, and improve patient outcomes. This showcases the transformative power of data while highlighting the importance of data protection.

Recent legislative changes like Bill C-27, amendments to Québec's Law 25, and mandatory privacy programs in B.C.'s public sector underscore the growing importance of data protection. Non-compliance can lead to serious consequences, including legal penalties and fines. Regularly updating data protection policies and training employees are crucial steps for maintaining compliance.

Manage data like a pro

Proper data lifecycle management ensures data is classified correctly, stored securely, and disposed of properly. Automated tools can help track data throughout its lifecycle, mitigating risks at every stage. Vendors and partners with access to data must also uphold strict privacy standards. Conducting due diligence on third parties and establishing clear data protection requirements in contracts are vital steps to prevent vulnerabilities. Regular audits ensure partners remain compliant.

Data quality is another significant concern. Inaccurate data can lead to poor decision-making and regulatory violations. Implementing data quality management processes, such as data validation and cleansing, keeps your data accurate and reliable.

Despite the best precautions, data breaches can still occur. Having an effective incident response plan is essential. Regularly updated plans and mock drills ensure all employees know the procedures in case of a breach.

Addressing these data risks requires a proactive approach. By staying informed about legislative changes and investing in security technologies, organizations can comply with legislation, build trust with stakeholders, and protect their valuable data assets.

Why stop there? Here are other risks to consider:

- Data breaches
- Internal threats (e.g. manipulating data for personal gain)
- Inadequate data security measures
- Lack of training and awareness
- Data residency and sovereignty issues

Questions to consider:

- Are you confident your data is secure and used in an ethical manner?
- As data increases in demand and drives material value, will your data governance practices keep pace?
- Who has access to your data, and can you trust them?

Red flag risks:

- No training, policy, or program in place regarding data lifecycle management and governance
- History of data breaches and data being shared without consent
- Sub-optimal decision making, and strategies based on poor quality and inaccurate data

Information and Operations Technology Governance

What will you do when the current cost of your IT/OT needs exceeds the allowable budget?

Cameron Ollenberger | Risk Analytics
Drew Buhr | Cyber Security Risk
Hash Qureshi | Enterprise Risk Services

In today's digital world, the convergence of IT and operational technology (OT) has pros and cons. Both the integration and poor governance of either can create risk.

Cyber criminals are targeting IT and OT systems at an accelerating rate to increase downtime and disrupt industrial processes and customers. The Canadian government and regulators emphasize protecting critical infrastructure, especially OT systems like power grids and water management systems.

State-sponsored actors also pose a serious threat, targeting infrastructure to gather information through espionage. They use this information to prepare and position themselves for future conflicts. The risk of cyber attacks on both IT and OT systems is a top concern. As these systems become more integrated, vulnerabilities in IT can impact OT environments, such as industrial control systems, which are often less resilient to disruptions.

Today's landscape has a shortage of skilled professionals with expertise in both IT and OT cyber security. This skills gap could lead to governance issues and increased vulnerability to attacks. Effective IT change management is crucial. Without it, organizations risk operational disruptions, security weaknesses, and compliance issues.

Bridging the divide

Physical security measures are also important. Insufficient physical security for OT infrastructure can lead to unauthorized access and tampering with systems. Organizations need to take a proactive stance to address these risks. This may include investing in training for teams, thorough security measures, and detailed IT change management processes. Regular risk assessments and audits can help identify and prevent vulnerabilities.

One major challenge is that smaller companies often struggle to keep their technology up to date due to budget constraints, while larger companies can afford the latest innovations. This creates a divide, making smaller businesses more vulnerable to cyber threats.

Ultimately, IT and OT leaders must prioritize investments in information and operations technology based on strategy and the needs of the business. They need to be agile, moving as fast as their strategy to protect against ever-evolving threats. By staying focused on strategic goals and minimizing risk exposure, they can ensure their systems remain secure and effective.

Why stop there? Here are other risks to consider:

- Non-compliance to related regulation and laws
- Data governance and privacy
- Supply chain vulnerabilities
- Outsourcing that causes controls to weaken or no longer exist

Questions to consider:

- Is it possible to adapt and change IT and OT priorities as quickly as your strategy, while not exceeding your budget?
- Can IT and OT leaders anticipate what needs to change and when, while aligning to long term strategy?
- Does your organization's IT- and OT-related change management consider how it may impact cyber security exposure?

Red flag risks:

- Operational issues related to system failures or a data breach
- Excessive operational disruption costs due to old or unmaintained IT and OT equipment
- Failing to meet strategic goals because of existing IT or OT systems

Environment, Social, and Governance (ESG)

Are you aware of both the opportunity and risk — like greenwashing — related to ESG?

Mary Larson | Organizational Renewal
Edward Olson | ESG Leader

As a business leader, you're likely used to adapting to new laws that require you to track and report on everything from carbon emissions to labour practices in distant countries. Welcome to the world of ESG, where the pressure to meet sustainability targets is mounting, and the rules are constantly changing.

Many businesses are under scrutiny to make real progress on ESG goals, but the reality is, they often lack the time, money, or resources to do everything they'd like. Prioritizing is key, but it's no easy task, especially when the government introduces new regulations like Bill S-211. This law requires companies to issue a public report on their risk assessment related to forced child labor. Miss the deadline and you may face a fine as high as $250,000. For many companies, especially those dealing with thousands of products, this is a massive challenge.

Tackle ESG challenges head on

Climate change and carbon emissions are significant risks. Businesses must adapt to extreme weather events and transition to low-emission operations, which can be costly and complex. Yet, this shift is essential for long-term sustainability. To survive, businesses need to brace for changes but also recognize the necessity of these adjustments.

Adopting sustainable practices and efficient technologies early on can help businesses mitigate risks related to resource scarcity, as well as waste and pollution management. Strong corporate governance is essential for managing ESG risks, ensuring compliance with regulations to maintain legal standing, investor trust, and a positive reputation. Additionally, businesses must avoid greenwashing, where ESG data is misrepresented to appear more favorable. The new Canadian Bill C-59 has been created to target greenwashing; however, it will also target those whose might not have evidence to support ESG claims and unintentionally could be violating this bill. Ensuring the accuracy of ESG reports is crucial, and data analytics can help verify this information.

In a world where ESG awareness and compliance are increasingly demanding, staying agile and proactive is key. By prioritizing these efforts and embracing sustainable practices, businesses can navigate challenges and build a resilient future.

Why stop there? Here are other risks to consider:

- Reliance on potentially inaccurate or unavailable third-party data
- Social inequality and community impacts
- Employee well-being and diversity not meeting industry expectations
- Supply chain management being disrupted by climate change
- Regulatory and policy changes leading to new fines
- Customer and stakeholder ESG expectations not being achieved

Questions to consider:

- If the risk and return associated with ESG needed to change, how fast can your organization act? Has your board established its risk appetite related to ESG?
- What are your top ESG priorities, and do they align with your stakeholders' expectations? Have you assessed the risks in relation to these strategies?
- Are you at risk of losing competitive advantage because you are not meeting customer ESG expectations?

Red flag risks:

- No knowledge of evolving ESG-related laws and policies
- Absence of prioritized ESG goals or established base lines against which to measure progress
- Lack of understanding of risks related to ESG goals

Disinformation Confusion

There is false information everywhere — how much false information do your employees, customers, partners, regulators, and competitors believe is true?

Chris Law | Defensive Cyber Security
Adriana Gliga | Payment Card Industry, Privacy and Data Governance
Eugene Ng | Cyber Security
Drew Buhr | Cyber Security Risk
Mark Reynolds | Mergers and Acquisitions Advisory

Canadians are growing more concerned about false, misleading, and inaccurate information online.

A recent Statistics Canada report highlights this trend: 59 percent of respondents say they're worried about the rising threat of misinformation, while 43 percent say they increasingly struggle to separate fact from fiction on the internet.

This is the first time disinformation confusion has been included in this report, reflecting its increasing impact on society and business. The spread of false or misleading information can lead to confusion, panic, and harm to individuals, corporations and communities. Disinformation campaigns, which intend to mislead, can manipulate public opinion and influence major decisions.

The impact on business

The implications for businesses are serious. Reputational damage from disinformation, malicious attacks on social media, or the promotion of fraud, scams, or phishing attacks can lead to financial losses and a loss of public trust.

The risk of disinformation is not just about reputational damage; it's also about the potential for financial harm and lost opportunities. Consider a scenario where false information spreads online about the safety of an airline. Even if completely unfounded, these rumours can cause people to avoid flying with the airline, leading to financial losses.

Similarly, during competitive bidding for government contracts, a false claim about a vendor's integrity can sway decisions, possibly costing the vendor the contract. Even if these claims are later proven untrue, the damage to the company's reputation could be long-lasting.

As disinformation continues to evolve, businesses need to stay vigilant and develop strategies to maneuver through the complexities of online information. To navigate these challenges, businesses must develop methods to verify the information they use and disseminate. This might include forming a communication verification team to ensure the accuracy of all public statements. Think of it as having a dedicated group that checks facts before they are shared, maintaining the company's credibility and trustworthiness.

Verifying the accuracy of information is imperative to maintaining public trust and integrity in the digital age.

Why stop there? Here are other risks to consider:

- Health misinformation
- Polarization and division
- Erosion of trust
- Manipulation of public discourse
- Cyber security threats
- Compliance challenges and legal liabilities

Questions to consider:

- How would you know if and prevent your organization from making critical decisions based on false information?
- Do you have effective controls to verify what is factual and what's not?
- Are you scanning social media to see if you are the victim of someone trying to spread false information about your business?

Red flag risks:

- No crisis response strategy in place for handling disinformation, misinformation, or reputation damage
- No mechanism in place to identify misinformation
- Lack of consumer confidence and trust

Third-Party Risk Management

Have you risk assessed your third-party vendors and mitigated the risks through contracts?

Cameron Ollenberger | Risk Analytics
Hash Qureshi | Enterprise Risk Services
Phil Racco | Enterprise Risk Services
Gord Chalk | Supply Chain

You think you know your third-party partners, but do you really?

Managing third-party risk is critical to protecting an organization's security and compliance. Yet, some businesses are still playing it fast and loose.

An October 2021 Statista survey of Canadian tech and security executives found that only about half of the organizations audited or verified their third-party service providers' security and compliance. A mere 43 percent refined their criteria for onboarding and ongoing risk assessments of outside vendors and partners. Only 27 percent terminated partnerships so they could improve their risk management framework.

When it comes to regulations and industry standards, it's not enough for a business to ensure its own compliance — third parties must comply as well. If not, the organization could face legal penalties and reputational damage. Regular audits and compliance checks can help confirm that your partners are adhering to necessary regulations.

Say an organization partners with an IT provider who, due to a lapse in their security measures, suffers a data breach. This breach could expose sensitive information and compromise the systems of any of the companies relying on the third-party IT provider. Every risk a business faces also applies to its third parties, making their vulnerabilities shared vulnerabilities.

Operational hiccups and talent gaps

Operational risks arise when third parties face disruptions that affect service delivery. Think about issues like bankruptcy, business interruptions, or performance failures. For instance, if a vendor goes out of business, your organization might face unexpected fees or lose an important service, impacting its financial health. Assessing the operational stability and financial well-being of vendors ensures a reliable partnership.

Third-party risks extend beyond the typical concerns. For example, if a vendor lacks proper training for emergency scenarios, like wildfire response for a pipeline project, the consequences could be catastrophic. Or consider the impact of using a third party to support your digital needs. If that partner fails to retain top talent, it could mean a loss of valuable knowledge and expertise, affecting the company's innovation and growth.

Outsourcing can also leave a business without a pipeline of young leaders to develop into future executives. Relying heavily on third parties might mean that the next generation of talent is not being groomed within an organization, creating a leadership vacuum down the line.

A proactive approach to third-party risk management goes a long way in protecting your business. Regular risk assessments, clear contracts, and ongoing open communication are key. Remember, the integrity of operations depends on the reliability of an organization and its partners. So, even if you think you know your third parties well, it's worth getting to know them even better.

Why stop there? Here are other risks to consider:

- Ethics, fraud, and reputation risk driven by third parties
- ESG data and project risk due to unreliable third-party information
- Insider cyber risk driven by third parties with access to systems
- Procurement risk driven by suboptimal decisions made by third parties
- Quality risk due to third parties not meeting standards

Key questions to ask

- Do you have the right framework and tools to assess the risk associated with all your vendors and business partners?
- Do you currently do background checks on vendors and their key resources based on risk (e.g., vendors with access to confidential data and critical systems should be considered high risk)?
- What strategies do you have in place to mitigate a disruption to your business due to a third-party outage and do you know what they are doing to minimize the disruption to you?
- Do you have a vendor code of conduct and mandatory training third parties must review annually?

Red flag risks:

- Whistleblower tips — from employees and vendors — regarding third parties
- Third party has a history of data breaches
- Excessive quality or cost complaints from your team or customers about work completed by your third-party partners

Merger and Acquisition (M&A) Integration

Does your due diligence accurately assess and mitigate the risk that could destroy the value expected from M&A?

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

Considering acquiring or merging with a company? The potential for growth and new markets is exciting, but the integration process can be riddled with hidden risks that could derail even the most promising deals. As we move towards 2025, M&A activities come with emerging areas of risk that must be addressed.

Consider the increased federal and provincial regulatory scrutiny of foreign investments, especially those involving sectors like minerals, infrastructure, manufacturing, personal data, and advanced technology.

It may sound grim, but organizations need to consider any possible connection to forced child slavery, as per Canada's Bill S-211, especially during M&A activity. This heightened scrutiny can lead to delays and increased compliance requirements. Organizations must fully understand these rules and regulations to avoid costly setbacks. Due diligence in M&A should include assessing the risk of acquiring a company involved in forced child slavery, ensuring that all potential liabilities are identified and addressed.

Activist investor campaigns are also on the rise in Canada, targeting M&A activities. These campaigns can be tricky to navigate, forcing businesses to address stakeholders' concerns and maybe even alter deal structures to gain approval. It's essential to have a clear strategy for managing these potential disruptions.

ESG factors are increasingly influencing M&A transactions. Organizations today must take ESG efforts seriously and demonstrate progress in achieving ESG performance targets and meeting the expectations of its stakeholders. Don't acquire a company that derails your ability to achieve your ESG targets, such as a net zero target by a certain date. Having a clear plan for how the deal will fit into an ESG strategy is important for long-term success.

Integrating tech and managing cultural clashes

When it comes to technology, ensure that the technology systems, especially related to AI, cyber security, and data privacy, are secure and compatible with the existing infrastructure. Protecting sensitive information and maintaining smooth operations is paramount during the integration process.

Cross-border deals come with their own set of challenges. Make sure to conduct thorough legal checks to avoid expensive lawsuits or fines down the road. For example, buying a company with a history of bribing public officials could lead to being implicated in a foreign corrupt practices act (FCPA) violation. Understanding the legal landscape in different countries can prevent significant headaches down the road.

Beyond these broader concerns, specific integration risks can trip up M&A efforts. Cultural clashes between merging companies can lead to conflicts and disrupt the ability to achieve strategic targets. Integrating systems and processes can be time-consuming and expensive. And losing key employees from the acquired company due to uncertainty or dissatisfaction with the new management or culture can cost valuable talent and knowledge.

The world of M&A is more complex than ever. The risks of today go far beyond what companies faced in the past. Due diligence, risk assessment, clear communication, and careful planning are essential to successfully navigate these challenges.

Why stop there? Here are other risks to consider:

- Regulatory and anti-trust issues
- Bribery and corruption risk
- Adverse customer, partner, and supplier reactions
- Reputation risk
- Legal, ethics, and compliance risks

Questions to consider:

- Are you buying a corruption fine, cyber issue, or the wrong culture?
- Do you have experts who can accurately assess the risks associated with the M&A deal — especially in foreign country operations?
- If you decide to pursue an acquisition or merger, do you have a plan to mitigate the risks associated with the company you will be acquiring?

Red flag risks:

- ESG, fraud, or corruption issues related to M&A deals
- Inaccurate or incompatible data
- Employee morale issues and cultural incompatibilities
- Lost customers and/or third-party suppliers

Digital Transformation

The technology is ready, but is your organization?

Jason Lee | Machine Learning and AI
Caitlin Crowley | Business Transformation
Denise Gigova| Business Transformation
Soumya Ghosh | Digital Transformation and Advisory
Wendy Gnenz | Digital

Digital transformation has surged since the pandemic as Canadian businesses rushed to stay afloat. Many feared that without upgrading their digital capacities, they'd soon be out of business. This urgency was felt across many sectors, from retail chains needing to expand their online presence to manufacturers grappling with disrupted supply chains.

But this digital transformation rush brought its own set of risks and challenges.

One of the biggest issues is resistance to change. When new technologies and processes are introduced, a workforce can be resistant because they prefer the status quo or fear job displacement. This resistance can slow down, or even halt, the transformation. Leaders need to clearly communicate the benefits of new technologies and involve employees in the transition to ease fears.

Are you ready for it?

Another risk is the lack of a skilled workforce. In 2023, more than half of Canadian businesses reported that their current workforce wasn't fully proficient in the necessary skills, including many digital skills. Without training and development, staff may not keep up with advancements in technology, leading to an unemployment crisis as tech outpaces talent development.

Effective leadership and a clear digital transformation strategy are vital to maneuvering through such a significant change, including modelling the end state with a clear plan for required resources and capabilities. Without a solid change management plan, organizations can struggle to implement new processes and realize the benefits associated with the transformation, leading to wasted resources and stalled progress.

One example comes from an organization that spent millions on new technologies but didn't engage their unions early in the process. And when it came time to train employees on the new systems, the unions resisted, fearing job losses. As a result, the new systems sat unused, wasting time and money, and halting transformation. In the end, by the time natural turnover occurs and the needed digital expertise is in place, the new systems may already be out of date.

So, why not engage a third-party vendor? Overdependence on outsourced IT vendors for digital transformation holds its own risks — as mentioned in the Third-Party Risk Trend section. Relying too much on outsourced IT can lead to issues with cost, quality, and control, especially if they fail to deliver. By developing in-house teams, you can maintain control over digital transformation efforts, as well as train future leaders who have innovative, digital minds.

Why stop there? Here are other risks to consider:

- Cyber security threats
- Data privacy non-compliance
- Technology misalignment
- Scalability issues
- Siloed data and systems
- Project cost and schedule overrun

Questions to consider:

- Is your organization ready to embrace and leverage new digital technology?
- Do you have the resources and capabilities needed to manage the end state and deliver on the expected benefits?
- If not, how much time and money is needed to manage the change to be prepared?

Red flag risks:

- Poor change management strategies
- A workforce not capable of managing new digital systems
- Employees resisting change out of fear of losing their jobs
- Ineffective integration, leading to excessive downtime or network incompatibilities

Data Analytics and Continuous Monitoring

Knowing how to optimize value from data is the starting point, but do you have the expertise to do so?

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

In the current business landscape, data analytics and continuous monitoring are driving significant value for many industries — a foundational element of staying ahead of the curve.

The value of data in Canada is projected to reach $1 trillion before 2030, and to stay competitive, businesses need to consider investing in data, databases, and data science. Statistics Canada reported a 400 percent growth in these investments since 2005, highlighting their importance. However, leveraging these analytics isn't without risk.

Here's the thing, the more value businesses see in data, the more they start relying on it, and the more they generate. And the more data generated, the greater the chance of mistakes, inaccuracies or a data breach. Data integrity is critical to data value and the ability to capitalize upon it.

Poor quality data can lead to misleading results, which can result in deployment of incorrect strategies and poor decision-making. Keep in mind that it's not only about collecting data, it's about making sure it's clean and reliable.

Clean data, smart moves

Different systems and formats can lead to unreliable data sets, making it a challenge to integrate data from a variety of sources. To combine all the pieces into a cohesive set, organizations need to seamlessly integrate data — this is key to making informed, confident decisions.

While automation in analytics can improve efficiency, try not to over rely on them. Algorithms are handy but might miss the nuances or errors that human oversight could catch. By balancing automation with human review, it helps make sure nothing slips through the cracks and supports more accurate outcomes.

Human review of data can also help keep workplaces physically safe. Consider the enormous dump trucks in the oil sands that are controlled by AI sensors. These trucks rely on these sensors to prevent accidents. If these sensors fail, the consequences could be severe, possibly causing harm to staff or damage to the worksite. Human oversight helps to mitigate these physical risks.

Without the right expertise in place, businesses may struggle to interpret the data correctly. By investing in training and hiring skilled professionals, organizations can leverage the full potential of data analytics. A knowledgeable team can be the difference between actionable insights and suboptimal decisions.

They can also help overcome any cultural resistance within an organization. If the culture resists data-driven decision-making, it can lead to a lack of support for these projects. Nurturing a culture that understands the value of data can drive more informed decisions across the business.

Why stop there? Here are other risks to consider:

- Data privacy and security breaches
- Cyber security vulnerabilities enabling hacker success
- IT and OT control weakness impacting critical infrastructure
- Weak data management and storage controls leading to breaches
- Increased risk of ethics violations, fraud, and corruption due to ineffective controls

Questions to consider:

- Do you feel your competitors have better insights from data, enabling them to gain market share?
- Does your strategy optimize value from data, and do you have sufficient expertise to unlock this value?
- Have you used advanced data analytics and continuous monitoring to prevent and detect fraud?

Red flag risks:

- Misleading or erroneous insights driven by data without integrity
- Systems crashing while running analytics, possibly due to not using appropriate analytic systems
- Lack of buy-in from board, leadership, employees, and stakeholders
- Lack of necessary skills, resulting in errors and the inability to create timely insights

Organization Design and Readiness

Is your organization ready for the future — or even for today — and how resilient will you be as critical resources retire or quit?

Caitlin Crowley | Business Transformation
Mary Larson | Organizational Renewal

Continuous transformation is happening everywhere, driven mostly by rapid technological advancements. With that in mind, adapting your organization to be future-ready is critical. However, a lack of vision and strategy is a big risk that can hinder an organization's ability to evolve. Many system transformations, for instance, don't consider the changes needed in organizational design, job descriptions, processes, and policy.

Setting up a business to support its goals while quickly responding to new challenges and opportunities is essential. Even without a major digital overhaul, businesses need to consider how emerging technologies can impact how they deliver products and services.

Without clear goals, aligning systems, processes, and resources becomes difficult. Poor communication of new initiatives can leave employees confused and investments misaligned. Everyone in the organization needs to understand the direction and goals to increase the chances of success. Therefore, leaders need to understand technology well enough to communicate effectively to all resources, even their technology experts.

Leading the charge

Inadequate leadership support can derail change efforts. Change requires strong commitment from the top. Without executive backing, there won't be enough direction or resources to drive change forward. Leaders need to champion and provide clear guidance.

Resistance to change is a common hurdle. Employees often prefer the comfort of the familiar and fear the unknown. They may even be scared they'll be replaced by new technology or more digital-minded colleagues. This resistance can stop change in its tracks. Leaders must communicate the benefits of new initiatives and involve employees in the transition to alleviate concerns.

Failing to address resistance and cultural issues can lead to misalignment of corporate values and, at its worst, lead to conflict. Organizational culture impacts how changes are perceived and adopted. Ignoring the potential for resistance and cultural issues can create a divided workforce. Categorizing employees into three groups: those who will never change, those who want to change but need help, and those who are ready and able to change can make change management efforts more effective.

Ultimately, even if a business hasn't undergone a massive digital transformation, it's important to consider how technology will drive leadership, product development, and service delivery. Proactively addressing these key points will help organizations adapt to future changes and ensure long-term success.

Why stop there? Here are other risks to consider:

- Poor communication — especially from leadership
- Insufficient resource capability to adopt critical technology
- Insufficient training while skill gaps exist
- Inadequate infrastructure and systems
- Ineffective monitoring, support, and feedback mechanisms

Questions to consider:

- Is your organization prepared for tomorrow? What about the next three years?
- If not, are you prepared to remove the barriers in the way of required change?
- Is there a need for a major reorganization to be better aligned with critical technology needs — like knowing which resources have required technology capabilities.
- Are you able to recruit and retain the talent you require to support the company's continued evolution? If not, what is standing in your way?
- How do you compare to your greatest competitors?

Red flag risks:

- Organizational design hinders optimal use of critical digital systems and data
- Leaders aren't respected due to insufficient tech knowledge and evolving skills to support change
- Existing controls don't support change management or transparency
- Lack of employee engagement, morale, and/or knowledge
- High turnover of high value employees

Insurance Mirage

Have you read the fine print, and will you meet the requirements for a claim?

Craig Burkart | Insurance Leader

Insurance is key to protecting businesses against unexpected events — or is it? It's becoming increasingly complicated and expensive as natural disasters, cyber security breaches, and technological advancements have created a world full of risks. Insurance companies are struggling to keep up, and it impacts everyone who relies on their coverage.

Take cyber security, for instance. The cost of cyber insurance has skyrocketed, and policies come with so many conditions that filing a claim can feel nearly impossible. Imagine paying $1 million each year for a cyber insurance policy with almost zero chance of getting a payout. It's a harsh reality for many businesses.

And this isn't limited to cyber insurance. After a major wildfire or flood, getting affordable insurance that covers these disasters becomes unfeasible, leaving people and businesses vulnerable. This situation forces organizations to rethink their reliance on insurance altogether.

Unveiling policy complexities

Another factor is the complexity of insurance policies. One real-life scenario involved a kids' sports team that was paying $30,000 each year in travel insurance only to find out their policy didn't cover sports teams. This oversight could have led to a disaster if an accident had happened. It's become critical to read the fine print to make sure policies cover what needs protecting.

Reliable insurance coverage shouldn't be an illusion. As the world of risk evolves, businesses must be proactive in understanding their insurance policies and make sure they offer real protection.

For their part, insurance companies must adapt to the changing landscape and balance affordability, relevance and comprehensive coverage.

Why stop there? Here are other risks to consider:

- Catastrophic events not covered by insurance
- Technology risk is not cost-effective to insure
- Use of new technology — like AI — that can prove incident cause
- Claims inflation driving rate increases
- Climate change raising insurance costs

Questions to consider:

- Read the fine print — do you understand the current cost and benefit of your insurance?
- What are the terms and conditions you must meet to be able to be eligible for a claim payout?
- Are you doomed to not meet terms and conditions before you even begin?
- Does it make sense to not buy insurance?

Red flag risks:

- Claims not paid on time or paid at all
- Last-minute, rushed insurance renewal with very little customer support
- Rate increases due to industry or corporate claims history
- Number of terms and conditions is continuously increasing

The Economic Rollercoaster

How will economic volatility impact your business, and is your business model resilient enough for the future?

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

In 2024, Canada's economy feels like an amusement park ride, filled with ups and downs that bring uncertainty and challenges. High interest rates, slow economic growth, and rising unemployment make it hard for businesses to succeed, or even to maintain the status quo.

It's a bumpy ride, but one that can be navigated by understanding and mitigating some key risk factors.

Our economy relies on commodities, like energy (e.g. oil, gas, renewables, and other natural resources). And when prices fluctuate, it creates a ripple effect, impacting exports, investments, and overall economic well-being. A drop in oil prices can hurt the economy by reducing the revenue generated by exports, which leads to decreased investment in the energy sector and a decline in the overall spending power in society.

The housing market continues to be an area of concern. High levels of household debt, high interest rates, and soaring housing prices — think of cities like Vancouver and Toronto — pose the risk of a market correction. This means that housing prices could suddenly drop, impacting consumer spending and financial stability. This may have dire consequences for a business, especially when losing customers because of the increasing cost of living.

Interest rate impacts

Interest rates impact borrowing costs for consumers and businesses. Higher rates result in reduced consumer spending and housing market activity as household manage increased debt servicing costs.

To navigate this risk trend, businesses may want to focus on reducing debt and avoid over-leveraging in real estate. This risk can be managed by locking in low-interest rates on loans. A healthy flow of cash can help cover these higher costs, but sometimes this is more easily said than done.

Domestic policy decisions and political dynamics add yet another layer of uncertainty, impacting investment climates and economic priorities. To prevent these risks, stay informed on policy changes and be prepared to adapt quickly. You may also want to consider engaging in advocacy yourself. This can help make sure the interests of your business are represented.

Why stop there? Here are other risks to consider:

- Trade dependencies and disruptions
- Global economic/market volatility
- Climate change and environmental risks
- Cyber security threats
- Demographic challenges — like an aging workforce of leaders who will retire at a later age
- Geopolitical tensions and uncertainties, including the impact of wars

Questions to consider:

- How has the economy and an interdependent global market impacted your business model, customers, and/or third parties?
- Can your business model survive the changes expected in the next three years?
- Will inflation and increasing prices help or hurt your value proposition?
- Do you have sufficient cash flow to be resilient to further fluctuations in the economy?

Red flag risks:

- Low cash flow and the risk of insolvency
- Falling margins as inflation increases costs
- Reducing diversity of income
- Shrinking target customer spending and demand

Business Resilience (Including Third Parties and the Impact of Cyber Attacks)

Practice makes perfect, so how has your leadership and board practiced for a real crisis?

Phil Racco | Third-Party Risk Management
Gustavo Meschler | Business Resilience Planning
Cliff Trollope | Business Resilience Planning

In the face of growing emerging risks, resilience has become an important focus for Canadian businesses.

And it's top of mind. A recent corporate risk survey from Canadian Underwriter 2024, found that 57 percent of respondents identified business interruption as their top enterprise risk. It was followed by cyber incidents (46 percent) and natural catastrophes (43 percent). And all three of these are interrelated or integrated risks.

Strong strategies can mitigate these risks. By withstanding — and swiftly recovering from — threats and disruptions, organizations stand to gain operational continuity and long-term stability.

Changes in global and domestic economic conditions can impact businesses, particularly those reliant on international trade and commodity prices. In the case of an oil and gas operation, a sudden drop in oil prices can hurt Canada's energy sector, lowering the revenue generated by the organization, which in turn lowers investments in the business. Many businesses have resilience plans for times when there is a sharp decline in margins.

Global supply chain disruptions can result in delays, added costs, and operational challenges. During the COVID-19 pandemic, many businesses struggled to get the materials they needed from their suppliers. To mitigate this and build resilience, organizations need to consider developing relationships with multiple suppliers. Local suppliers can also help ensure a steady flow of goods, even when global supply chains are disrupted.

Since March 2020, global supply chains have become more resilient. However, the size and quality of digital logistics networks will usually dictate how resilient they have become or have the potential to become.

Weathering the storm

Extreme weather events like wildfires, floods, mudslides, and storms can damage infrastructure and disrupt operations — so try not to underestimate the damage potential of climate change and environmental disasters. A thorough and proactive disaster recovery plan and resilient infrastructure can help withstand unexpected environmental impacts.

And to build business resilience, the right talent is imperative. But labour market complexities — like skills shortages, demographic shifts, and changing workplace expectations — can affect recruitment and retention of specialized skill sets. To attract and keep top talent, businesses need to offer competitive salaries, flexible work arrangements, and opportunities for professional development. This is a win for your workforce and a win for your business.

To prepare, leadership teams can conduct table-top training exercises to practice relevant and probable scenarios, like ransomware attack simulations, to discuss teamwork and sequence steps in an emergency management plan.

Why stop there? Here are other risks to consider:

- Regulatory and non-compliance risks
- Geopolitical instability
- Pandemic and health crises
- Financial market risks
- Cyber security threats
- Technological change and obsolescence
- Climate change and related natural disasters

Questions to consider:

- What role and associated responsibilities do your outsourced partners have in business resilience (e.g., disaster recovery, business continuity, etc.)?
- Do you include outsourced partners or third parties in the table-top training exercises?
- Are the roles and responsibilities of business resilience built into vendor and key stakeholder contracts and training?

Red flag risks:

- Third parties not keeping up with industry disruptions and unaware of their role in establishing resilience
- Lack of critical incident planning and preparation
- A competitor is impacted by an unexpected disruption — you could be next

Supply Chain, Capital Projects, and Operations

Are you prepared to detect and prevent risk trends that disrupt facility operations, and cause significant cost and schedule overruns?

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

Imagine you're managing a major construction project. Everything is going smoothly until unexpected expenses start piling up, a critical shipment of materials gets delayed, and suddenly the project is weeks behind schedule and possibly overbudget.

This scenario highlights the fragile nature of managing supply chains and capital projects, especially without the right technological controls in place. While sometimes the root cause is the lack of an experienced project manager, often it is something outside the control of the project manager — like an unexpected material delay or poor weather conditions.

Statistics Canada reports that 40 percent of Canadian industries are highly vulnerable to external demand and supply shocks. These industries, which account for a quarter of Canada's economic output, face risks in global supply chains, which need to be carefully managed.

Major disruptions in supply chain often leads to very costly downtime in production facilities.

Mitigate disruptions

Cost overruns are one of the biggest risks for significant projects. Unexpected expenses, scope changes, or inaccurate cost estimates can blow budgets out of the water. This puts immense strain on your resources and jeopardizes the completion of the project.

These resource constraints can delay project timelines, as can factors like adverse weather, regulatory approvals, and/or technical challenges. So, if a shipment of materials is delayed because of a storm, the project schedule can be drawn out, increasing costs and pushing back completion dates. Resource constraints — including a lack of skilled labour, materials, equipment, and funding — can halt your business' work in its tracks.

Scope creep is a sneaky cause of inflated timelines and budgets. The inflow of continual change orders leads to added costs and delays — causing the initial plan to spiral into a financial and logistical nightmare.

Supply chain disruptions are a constant threat. Natural disasters, geopolitical events, or supplier issues can delay materials and drive price increases. Consider developing relationships with multiple suppliers, especially local ones, to avoid disrupting production operations in the case of a political conflict or a major wildfire. Often, experienced project managers plan for high-risk resource and material issues and have contingency plans in place.

By leveraging technology controls like project management software, real-time tracking systems, and predictive analytics, businesses can help prevent these operational challenges. These tools allow for better monitoring of costs, timelines, and resource availability, so you can respond more quickly to unexpected issues.

Why stop there? Here are other risks to consider:

- Health and safety incidents
- Regulatory non-compliance
- Quality control issues
- Technology failures
- Adverse environmental impacts

Questions to consider:

- How do you anticipate and detect quality, cost, and material supply issues?
- Are data analytics being used to prevent, detect, and monitor billing (like duplicate payments) or construction quality issues in supply chain, capital projects, and operations?
- How will you monitor the external risks — like extreme weather or permit delay — that may disrupt the project?

Red flag risks:

- Timeline extensions
- Excessive amount of change orders
- Change in prime contractor
- Resource shortages or turnover during projects
- Non-compliance issues
- Onsite health and safety issues

Climate Crisis Fallout

How predictable are the negative side effects of climate change on your organization and how prepared are you to deal with them?

Edward Olson | Enterprise Risk and ESG

By 2025, the previous 10 years of climate change will have reduced Canada's GDP by $25 billion, according to the Canadian Climate Institute.

That's a big number. One that demonstrates the frequency and impact of weather-related disasters.

The increased frequency and severity of extreme weather events — like floods, wildfires, and storms — comes with physical risks. These events can damage infrastructure, potentially stall operations, and lead to costly rebuilding efforts.

Furthermore, these climate-related disruptions — like crop failures, transportation delays, or water scarcity — impact supply chains, which can hinder production, distribution, and access to raw materials.

Navigating the operational and economic storm

Governments across the globe are implementing climate-related regulations, like carbon pricing and emissions standards. And these changes, like a new carbon tax, can make it more costly to produce goods, squeezing profit margins.

Financial risks are closely linked to climate change. As the world shifts away from fossil fuels, business models may become less viable, leading to the repricing of financial assets. Even the banks, pension funds, and investment firms that finance businesses could feel the financial squeeze. Additionally, rising insurance costs and reduced access to funding can put a strain on financial performance.

Operational risks also arise from climate-related interruptions. Sudden changes in weather patterns can affect energy supply, water availability, and infrastructure stability. For instance, a factory might face power outages during a heatwave or water shortages during a drought, impacting its ability to operate smoothly.

Why stop there? Here are other risks to consider:

- Insurance excluding claims related to the impact of climate change
- Market risks from climate-related supply chain disruptions
- Reputational risks from inaction on high-probability climate risks
- Legal risks for insufficient employee protection
- Human capital risks from high turnover due to safety concerns

Questions to consider:

- Does your organization project, model, and prepare for the impact of extreme weather events and global warming on your operations?
- If you lost your top supplier — do you have others to call upon?
- Have you trained your employees and onsite third parties to mitigate the relevant risks related to climate change scenarios?

Red flag risks:

- Lack of critical climate incident planning and preparation
- Shrinking profit margins due to increased climate-related fees, taxes, and insurance
- No knowledge of your organization's emission (carbon footprint) output

Fraud and Corruption

Fraud issues have doubled in Canada over the last decade. Have you doubled the effectiveness of your fraud risk assessment along with your preventative and detective controls?

Lisa Majeau-Gordon | Forensics
Richard Arthurs | Enterprise Risk

Fraud cases have nearly doubled over the past decade, surging from 79,000 in 2012 to 150,000 in 2022, according to Statistics Canada. This dramatic increase underscores the growing sophistication of fraudsters, who are now leveraging cutting-edge technology like AI to enhance their illicit activities.

How can you protect your business and your future?

By knowing and proactively addressing the risks.

Consider third-party vendors and service providers who may have the opportunity to steal or misuse company funds, inventory, or other assets for personal gain. This asset misappropriation could look like embezzling money, or even something like selling company products for personal profit. These actions erode trust and, potentially, the financial well-being of an organization.

Alongside this, bribery and kickbacks present another potential danger. This involves offering, soliciting, or accepting illicit payments to influence decisions, contracts, or regulatory outcomes.

As we dive deeper, conflicts of interest add another layer of complexity. When employees or executives engage in activities or relationships that could compromise their objectivity, it can lead to biased decisions that aren't in the best interest of the company.

The new age of fraud

The digital age brings its own set of risks, with cyber fraud being a major threat. Enhanced by AI, cyber fraud includes phishing, ransomware, identity theft, and payment fraud. Consider a cyber criminal hacking into company systems to steal sensitive information or tricking employees into making unauthorized payments. In 2024, cases of deepfake AI fraud skyrocketed — this involves using AI to look and sound like an actual person and then requesting a payment.

As we navigate 2024 and move into 2025, vendor fraud becomes a growing concern. This type of fraud occurs when vendors work with an organization's employees to artificially inflate prices, deliver sub-standard goods or services, or give kickbacks in exchange for business. These fraudulent activities can be expensive and damaging to reputations and bottom lines.

Why stop there? Here are other risks to consider:

- Financial statement fraud
- Employee fraud
- Insider trading
- Money laundering
- Non-compliance with anti-corruption laws

Questions to consider:

- How aware are your leaders of the most common types of fraud and corruption techniques being used today?
- Are your leaders aware of how to effectively prevent and detect these issues?
- Is your organization aware of the most advanced crimes committed using artificial intelligence, like deepfake impersonation tools?
- Do you have a formal and effective internal controls framework in place? Has it been tested?

Red flag risks:

- Absence of a fraud risk assessment, and/or use of data analytics to prevent or detect fraud
- Employees living lifestyles beyond what their compensation could afford
- Third parties with cash flow issues, continuous requests for change orders, or those with known close relations with leaders
- No clear guidelines, training, policies, or code of conduct for effective fraud controls

Internal Audit Project Opportunities

A comprehensive list of potential internal audit projects for each emerging risk area detailed in this report, including relevant laws and regulations.

The digital minds of future leaders

- **Recruitment process audit:** Evaluating the efficiency and effectiveness of the recruitment process, including sourcing methods, interview procedures, candidate evaluation, and onboarding practices to ensure they attract high-quality digital talent.
- **Compliance with employment laws audit:** Verifying that recruitment and employment practices are compliant with relevant laws and regulations, such as non-discrimination, right to work, and data protection legislation.
- **Talent acquisition cost audit:** Analyzing the costs associated with the talent acquisition process, including advertising, recruitment agencies, background checks, and other related expenses to ensure they are optimized and provide a good return on investment.
- **Diversity and inclusion audit:** Assessing the organization's efforts to recruit and retain a diverse workforce and create an inclusive environment, which is critical for fostering innovation and attracting digital leaders.
- **Employee turnover and retention audit:** Investigating the causes of employee turnover, especially among digital talent, to identify patterns and develop strategies to improve retention rates.
- **Performance management system audit:** Reviewing the performance management system to ensure it is effectively identifying, rewarding, and developing high-potential digital leaders.
- **Leadership development and succession planning audit:** Evaluating the processes in place for identifying, developing, and preparing potential future leaders for advancement within the organization, ensuring a pipeline of digital leadership talent.
- **Compensation and benefits audit:** Analyzing the competitiveness of the organization's compensation and benefits packages in attracting and retaining digital talent, including salary, bonuses, stock options, and other perks.
- **Training and professional development audit:** Assessing the availability, quality, and effectiveness of training and professional development programs aimed at enhancing the skills and knowledge of digital leaders.
- **Cultural alignment and employee engagement audit:** Examining the organizational culture and its alignment with the expectations and values of digital professionals, as well as measuring employee engagement levels, which are critical for retention.

Relevant laws and regulations

- **Human rights legislation:** The Canadian Human Rights Act and provincial human rights codes (e.g., the Ontario Human Rights Code) prohibit discrimination in employment practices on grounds such as race, national or ethnic origin, color, religion, age, sex, sexual orientation, marital status, family status, disability, and a conviction for which a pardon has been granted.
- **Employment Equity Act:** This federal law applies to federally regulated industries and aims to eliminate employment barriers for four designated groups: women, Indigenous peoples, persons with disabilities, and members of visible minorities.
- **Employment standards legislation:** Each province and territory has its own Employment Standards Act, which sets out the minimum standards for conditions of employment, such as hours of work, minimum wage, holidays, leaves, notice of termination, and severance pay.

The digital minds of future leaders

- **Labour Relations Legislation:** This set of laws governs the collective bargaining process between employers and unions, which may impact the recruitment and retention of all employees, including digital leaders, in unionized environments.
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** This federal privacy law sets out the rules for how businesses must handle personal information in the course of commercial activity, which includes recruitment and HR management practices.
- **Accessibility legislation:** Laws such as the Accessibility for Ontarians with Disabilities Act (AODA) set requirements for organizations to create more accessible environments, which can help in recruiting and retaining employees with disabilities, including those in leadership roles.
- **Pay equity legislation:** Federal and provincial pay equity laws require that employers provide equal pay for work of equal value, which is relevant for ensuring fair compensation practices are in place for digital leaders.
- **Canada Labour Code:** For federally regulated employers, the Canada Labour Code outlines a range of employment standards, including those related to hours of work, employee entitlements, and leaves of absence.
- **Immigration and Refugee Protection Act:** For organizations looking to recruit digital leaders from abroad, this act sets the regulations for obtaining the necessary work permits and visas for international candidates.
- **Provincial occupational health and safety acts:** These acts require employers to ensure a safe working environment, which includes considerations for ergonomic setups that are often important in digital workspaces.

Cyber Security

- **Risk assessment audits:** Evaluating the organization's cyber risk profile, including identifying and assessing potential threats, vulnerabilities, and the impact of potential cyber incidents.
- **Network security audits:** Reviewing network infrastructure for security weaknesses, including the management of firewalls, intrusion detection systems, and network segmentation.
- **Access control audits:** Ensuring that access to systems and data is restricted based on the principle of least privilege and that user accounts are managed securely with appropriate authentication mechanisms.
- **Data protection and privacy audits:** Verifying that personal and sensitive data is handled in compliance with applicable data protection laws (like GDPR, PIPEDA) and that data encryption, anonymization, and other protective measures are in place.
- **Incident response and recovery audits:** Evaluating the organization's incident response plan for preparedness in the event of a cyber security breach, including response procedures, communication plans, and recovery processes.
- **Change management audits:** Assessing the processes for managing changes to IT systems and software to ensure that they don't introduce new vulnerabilities and that they are documented and authorized.
- **Third-party and vendor risk audits:** Examining the security policies and controls of third-party vendors and service providers, especially those who handle sensitive data or have access to the organization's IT systems.
- **Compliance audits:** Checking adherence to relevant cyber security standards and frameworks such as ISO 27001, NIST Cybersecurity Framework, or industry-specific regulations like HIPAA for healthcare, or PCI DSS for payment card processing.
- **Patch management audits:** Ensuring that software patches and updates are being managed effectively to mitigate the risk of exploiting known vulnerabilities.
- **Physical security audits:** While often considered separate from cyber security, physical security can impact IT security. Audits in this area ensure that physical access to critical infrastructure is controlled and monitored.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents act (PIPEDA):** This federal law sets out the rules for how private-sector organizations must handle personal information in their commercial activities.
- **Privacy Act:** Governs how federal government institutions handle personal information. It is complemented by PIPEDA for the private sector.
- **Canadian Anti-Spam Legislation (CASL):** Designed to protect Canadians from spam and other electronic threats, CASL regulates the sending of commercial electronic messages and the installation of computer programs on another person's computer system.
- **Canadian Cyber Incident Response Centre (CCIRC):** Part of Public Safety Canada, CCIRC is responsible for mitigating and responding to cyber threats to Canada's critical infrastructure.
- **National Strategy for Critical Infrastructure:** Establishes a strategic framework for strengthening the resilience of critical infrastructure against cyber threats.
- **Digital Privacy Act (Bill S-4):** Amends PIPEDA to include mandatory breach reporting, notification, and record-keeping requirements for organizations in the case of a data breach.

Cyber Security

- **The Cyber Security Strategy:** Canada's vision for cyber security and how the government plans to secure government systems and work with industries to secure vital cyber systems outside the federal government.
- **Bill C-59: An Act respecting national security matters:** Enacts new authorizations and processes for certain security and intelligence operations and introduces measures to increase transparency and accountability.
- **Bill S-4, the Digital Privacy Act:** Amends PIPEDA to create new obligations for organizations to report breaches of security safeguards that pose a real risk of significant harm to individuals.
- **Secure Air Travel Act:** Part of Canada's anti-terrorism strategy, this act regulates the protection and handling of passenger information as well as the no-fly list.

Artificial intelligence ethical dilemmas

- **Governance and oversight:** Audit the governance structure for AI initiatives, including roles and responsibilities, decision-making processes, and oversight mechanisms.
- **Data governance:** Assess the data quality, integrity, and security measures in place to ensure that data used by AI systems is accurate, reliable, and compliant with regulations.
- **Model development and validation:** Review the process of developing AI models, including data preprocessing, model selection, hyperparameter tuning, and validation techniques to ensure accuracy and reliability.
- **Algorithmic bias and fairness:** Audit AI systems for potential bias and discrimination by examining the fairness of data sources, model training, and decision-making outputs.
- **Cyber security and data privacy:** Evaluate the cyber security measures and data privacy controls implemented to protect AI systems from cyber threats and ensure compliance with privacy regulations.
- **Ethical use of AI:** Assess whether AI systems adhere to ethical guidelines and principles, including transparency, accountability, and fairness in decision-making processes.
- **Compliance and regulatory requirements:** Review AI systems to ensure compliance with relevant laws and regulations governing data protection, consumer rights, and industry-specific requirements.
- **Monitoring and performance management:** Audit the monitoring mechanisms in place to track the performance of AI systems, detect anomalies or errors, and ensure ongoing compliance with established standards.
- **Vendor management:** Evaluate the controls in place for managing third-party vendors and service providers involved in AI development or deployment to mitigate risks associated with external dependencies.
- **Incident response and continuity planning:** Assess the organization's incident response procedures and business continuity plans for AI-related disruptions, including data breaches, system failures, or ethical issues.

Relevant laws and regulations

- **Personal information protection and electronic documents act (PIPEDA):** PIPEDA sets out rules for the collection, use, and disclosure of personal information in the course of commercial activities. It may apply to AI systems that process personal data.
- **Canadian Charter of Rights and Freedoms:** The Charter guarantees fundamental rights and freedoms, including privacy and equality rights, which are relevant when considering the impact of AI on individuals.
- **Privacy laws:** Provincial privacy laws, such as the Alberta Personal Information Protection Act (PIPA) and the British Columbia Personal Information Protection Act (PIPA), may also apply to the handling of personal information by AI systems.
- **Anti-discrimination laws:** Laws like the Canadian Human Rights Act and provincial human rights codes prohibit discrimination on grounds such as race, gender, and disability, which are important considerations in AI systems to prevent bias and discrimination.
- **Competition Act:** The Competition Act regulates anti-competitive practices and misleading advertising, which may be relevant in the context of AI-driven pricing algorithms and marketing strategies.
- **Telecommunications Act:** This legislation governs the provision of telecommunications services in Canada and may impact the use of AI in telecommunications networks and services.

Artificial intelligence ethical dilemmas

- **Criminal Code of Canada:** The Criminal Code contains provisions related to fraud, hacking, and other cybercrimes that may be relevant in cases involving AI systems.
- **Copyright Act:** The Copyright Act governs the protection of intellectual property rights in Canada, including issues related to the ownership and infringement of AI-generated content.
- **Consumer protection laws:** Various federal and provincial laws protect consumers from unfair practices, which may be relevant when AI is used in customer service, advertising, or product recommendations.
- **Emerging technologies and innovation policies:** While not laws per se, government policies and initiatives promoting innovation and responsible AI development, such as the Pan-Canadian Artificial Intelligence Strategy, may influence the regulatory landscape for AI in Canada.

High-value, sensitive, and privacy data

- **Data governance audit:** Evaluate the data governance framework to ensure that policies, procedures, and standards for managing sensitive data are in place and effective.
- **Access control audit:** Assess the effectiveness of access controls and user permissions to ensure that only authorized personnel have access to sensitive data.
- **Data protection and privacy audit:** Review the organization's compliance with applicable data protection and privacy laws, such as PIPEDA in Canada, GDPR in Europe, or any other relevant legislation.
- **IT security audit:** Conduct a comprehensive review of IT security controls, including firewalls, intrusion detection systems, anti-malware measures, and security incident management processes.
- **Encryption and data masking audit:** Verify that encryption standards are robust and that encryption keys are managed securely. Ensure proper data masking practices are in place where necessary.
- **Data lifecycle management audit:** Examine the processes for data creation, storage, archiving, and destruction to ensure data is managed securely throughout its lifecycle.
- **Third-party vendor and service provider audit:** Assess the risks associated with third-party vendors who handle sensitive data, ensuring that they have adequate security controls and comply with contractual agreements.
- **Incident response and breach notification audit:** Review the incident response plan and past incident reports to ensure that the organization can effectively respond to data breaches and comply with breach notification requirements.
- **Data transfer and sharing audit:** Evaluate the controls surrounding data transfer and sharing, both internally and externally, to prevent unauthorized data disclosure or leaks.
- **Employee training and awareness audit:** Assess the effectiveness of employee training programs on data protection and privacy to ensure staff are aware of their responsibilities and best practices.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** This is Canada's federal privacy law for private-sector organizations. It sets out the rules for the collection, use, and disclosure of personal information in the course of commercial activity.
- **Digital Privacy Act (Bill S-4):** An amendment to PIPEDA, this act introduces mandatory breach reporting, notification, and record-keeping requirements.
- **Privacy Act:** Governs how federal government institutions handle personal information.
- **Canadian Anti-Spam Legislation (CASL):** Sets the rules for electronic communications, including requirements for obtaining consent to send commercial electronic messages, and the handling of personal information.
- **Access to Information Act:** Provides the right of access to information in federal government records, which can include sensitive and high-value data.
- **An act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities (Canada's anti-spam law):** This law, often referred to as CASL, includes provisions related to the installation of computer programs on another person's computer system, in the course of a commercial activity, without express consent.

High-value, sensitive, and privacy data

- **Health information custodians in the province of Ontario — Personal Health Information Protection Act (PHIPA):** Governs the collection, use, and disclosure of personal health information within the province of Ontario.
- **Act Respecting the Protection of Personal Information in the Private Sector (Quebec):** This is Quebec's private-sector privacy law that regulates the collection, use, and disclosure of personal information.
- **Personal Information Protection Acts (PIPA) — Alberta and British Columbia:** These acts are for the private sector and are similar to PIPEDA but are applicable in their respective provinces.
- **Cyber security and critical infrastructure protection:** While not a single act, there are various initiatives and proposed regulations aimed at protecting critical infrastructure and ensuring cyber security, which can involve sensitive and privacy data.

Information and operations technology governance

- **Data governance audit:** Evaluate the data governance framework to ensure that policies, procedures, and standards for managing sensitive data are in place and effective.
- **Access control audit:** Assess the effectiveness of access controls and user permissions to ensure that only authorized personnel have access to sensitive data.
- **Data protection and privacy audit:** Review the organization's compliance with applicable data protection and privacy laws, such as PIPEDA in Canada, GDPR in Europe, or any other relevant legislation.
- **IT security audit:** Conduct a comprehensive review of IT security controls, including firewalls, intrusion detection systems, anti-malware measures, and security incident management processes.
- **Encryption and data masking audit:** Verify that encryption standards are robust and that encryption keys are managed securely. Ensure proper data masking practices are in place where necessary.
- **Data lifecycle management audit:** Examine the processes for data creation, storage, archiving, and destruction to ensure data is managed securely throughout its lifecycle.
- **Third-party vendor and service provider audit:** Assess the risks associated with third-party vendors who handle sensitive data, ensuring that they have adequate security controls and comply with contractual agreements.
- **Incident response and breach notification audit:** Review the incident response plan and past incident reports to ensure that the organization can effectively respond to data breaches and comply with breach notification requirements.
- **Data transfer and sharing audit:** Evaluate the controls surrounding data transfer and sharing, both internally and externally, to prevent unauthorized data disclosure or leaks.
- **Employee training and awareness audit:** Assess the effectiveness of employee training programs on data protection and privacy to ensure staff are aware of their responsibilities and best practices.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** This is Canada's federal privacy law for private-sector organizations. It sets out how businesses must handle personal information in the course of commercial activities across Canada.
- **Privacy Act:** Governing the federal public sector, this act regulates how the Government of Canada collects, uses, stores, discloses, and disposes of personal information.
- **Canadian Anti-Spam Legislation (CASL):** This law protects Canadians while ensuring that businesses can continue to compete in the global marketplace. It sets the rules for the sending of commercial electronic messages and the installation of computer programs.
- **Digital Privacy Act (Bill S-4):** This act amended PIPEDA to include mandatory breach reporting, notification, and record-keeping requirements for private-sector organizations.
- **An Act to support the Digital Economy:** This act may refer to various legislative efforts aimed at protecting personal information and encouraging digital commerce, including potential amendments to PIPEDA or new laws enacted to protect digital privacy.
- **Access to Information Act:** This act provides a process for individuals to request access to information in federal government records, which may include sensitive or high-value data.

Information and operations technology governance

- **Provincial health information acts:** Such as Ontario's Personal Health Information Protection Act (PHIPA), Alberta's Health Information Act (HIA), and British Columbia's E-Health (Personal Health Information Access and Protection of Privacy) Act, these laws regulate the handling of personal health information within their respective provinces.
- **Provincial private sector privacy acts:** Alberta, British Columbia, and Quebec have their own private sector privacy laws that are considered substantially similar to PIPEDA, meaning they apply in place of PIPEDA within those provinces.
- **Quebec's Act Respecting the Protection of Personal Information in the Private Sector:** This is a comprehensive privacy law that governs the collection, use, and disclosure of personal information by private businesses in Quebec.
- **Canada's cyber security strategy:** While not a law or regulation, the strategy outlines how Canada plans to protect against cyber threats and promote safe and secure online services, which includes the protection of sensitive and high-value data.

Environment, social and governance

- **Environmental compliance audit:** Assesses adherence to environmental laws and regulations. Evaluates waste management, pollution control, and resource usage.
- **Health and safety audit:** Ensures compliance with occupational health and safety regulations. Examines workplace safety protocols and employee wellness programs.
- **Social responsibility audit:** Reviews policies related to labor practices, human rights, and community impact. Evaluates stakeholder engagement and corporate philanthropy initiatives.
- **Supply chain audit:** Assesses the sustainability and ethical practices of suppliers. Reviews adherence to fair labor standards and environmental impact mitigation in the supply chain.
- **Corporate governance audit:** Ensures that the governance structure aligns with best practices and regulatory requirements. Assesses board independence, diversity, executive compensation, and shareholder rights.
- **Ethics and compliance audit:** Evaluates the effectiveness of the organization's code of conduct and ethics policies. Reviews mechanisms for reporting and addressing unethical behavior.
- **Energy management audit:** Reviews energy use and efficiency measures. Assesses initiatives for reducing the carbon footprint and improving sustainability.
- **Information disclosure and transparency audit:** Ensures that ESG reporting is accurate, complete, and transparent. Assesses adherence to reporting standards such as GRI, SASB, or TCFD.
- **Diversity and inclusion audit:** Evaluates recruitment, retention, and promotion practices to ensure diversity and equal opportunity. Assesses training and development programs focused on inclusivity.
- **Climate risk and resilience audit:** Assesses the organization’s exposure to climate-related risks. Evaluates adaptation and resilience strategies for potential climate change impacts.

Relevant laws and regulations

- **Canadian Environmental Protection Act (CEPA):** CEPA is the principal federal law for preventing pollution and protecting the environment and human health.
- **Species at Risk Act (SARA):** This act aims to prevent wildlife species from becoming extinct and provides for the recovery of endangered or threatened species.
- **Fisheries Act:** One of Canada's oldest laws, it provides the framework for the protection and sustainable use of Canada's fisheries resources, including habitat protection.
- **Impact Assessment Act:** This act, which replaced the Canadian Environmental Assessment Act in 2019, provides the process for assessing the potential environmental, social, economic, and health impacts of designated projects.
- **Greenhouse Gas Pollution Pricing Act:** This legislation establishes a federal pricing benchmark for carbon emissions, aimed at reducing greenhouse gas emissions in compliance with international commitments.
- **Canada Labour Code:** Governs labor relations and fair work practices in federally regulated industries, including provisions for occupational health and safety, labor standards, and employment equity.
- **Employment Equity Act:** Aims to achieve equality in the workplace so that no person is denied employment opportunities for reasons unrelated to ability, and to correct the conditions of disadvantage in employment experienced by women, Indigenous peoples, persons with disabilities, and members of visible minorities.

Environment, social and governance

- **Canadian Human Rights Act:** Prohibits discrimination on grounds such as race, gender, and disability, and applies to federal agencies and businesses.
- **Corruption of Foreign Public Officials Act:** This is Canada's law that criminalizes the bribery of foreign officials in order to obtain or retain an advantage in the course of international business.
- **Accessible Canada Act:** The act aims to make Canada barrier-free by 2040. This legislation requires organizations under federal jurisdiction to ensure that public spaces, workplaces, employment service delivery, and information be accessible to everyone.

Disinformation dynamics

- **Content management audit:** Reviews the policies and procedures for managing content on platforms owned by the organization to ensure that disinformation is identified and addressed appropriately.
- **Compliance audit with laws and regulations:** Assesses whether the organization complies with applicable laws and regulations concerning disinformation, such as election laws, advertising standards, and data protection regulations.
- **Information security audit:** Evaluates the security measures in place to protect against cyber threats that could lead to the spread of disinformation, such as hacking or unauthorized access to systems.
- **Communication and response audit:** Examines the organization's crisis communication plan and response procedures to ensure they are effective in addressing disinformation incidents.
- **Third-party management audit:** Assesses the risk management processes related to third parties, such as vendors and partners, to ensure they are not sources or amplifiers of disinformation.
- **Training and awareness audit:** Reviews the training programs and awareness initiatives in place to educate employees about disinformation risks and their role in preventing it.
- **User reporting systems audit:** Evaluates the mechanisms for users to report disinformation, ensuring that these systems are user-friendly, effective, and result in timely action.
- **Data analytics and monitoring audit:** Assesses the tools and processes used for monitoring and analyzing data to detect patterns indicative of disinformation campaigns.
- **Editorial and fact-checking audit:** Reviews the policies and practices of editorial teams and the use of fact-checking services to validate the accuracy of content before publication.
- **Incident management and recovery audit:** Assesses the organization's preparedness to manage and recover from a disinformation incident, including the effectiveness of incident management teams and processes.

Relevant laws and regulations

- **Criminal Code of Canada:** The Criminal Code contains provisions against hate speech, libel, and slander, which can be applicable in cases where disinformation crosses into these territories.
- **Canadian Charter of Rights and Freedoms:** Although this document protects freedom of expression, it also allows for reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society, which could pertain to harmful disinformation.
- **Canada Elections Act:** This Act contains provisions to protect the electoral process from false statements that could affect the outcome of an election, which includes the spread of disinformation about candidates.
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA governs how private sector organizations collect, use, and disclose personal information in the course of commercial business, which can be relevant if disinformation involves the misuse of personal data.
- **Canadian Anti-Spam Legislation (CASL):** CASL might be used to tackle disinformation in cases where misleading information is spread via electronic messaging, including email and social media.
- **Competition Act:** This Act contains provisions against misleading representations and deceptive marketing practices, which can be applied to disinformation campaigns that affect competition.

Disinformation dynamics

- **Broadcasting Act:** The CRTC (Canadian Radio-television and Telecommunications Commission) enforces this Act, which includes provisions related to the content that is broadcasted in Canada, potentially encompassing the spread of disinformation through media channels.
- **Act Respecting the Protection of Personal Information in the Private Sector (Quebec):** Similar to PIPEDA but applicable in Quebec, this Act could also be relevant in cases of disinformation involving personal data.
- **Bill C-76 (Elections Modernization Act):** This act, which amended the Canada Elections Act, introduced transparency requirements for political advertising, which could also apply to certain types of disinformation.
- **Digital Charter Implementation Act, 2020:** If passed, this proposed legislation would update PIPEDA and introduce new regulations to increase control and transparency in digital and data practices, which could impact the dissemination of disinformation.

Third-party risk management

- **Vendor management policy audit:** Review and assess the organization's vendor management policy to ensure it aligns with industry best practices, regulatory requirements, and the organization's risk appetite.
- **Vendor due diligence audit:** Evaluate the effectiveness of the vendor due diligence process, including how vendors are selected, assessed, and monitored for compliance with security and privacy requirements.
- **Contract management audit:** Review vendor contracts to ensure they include necessary clauses related to data protection, security measures, compliance requirements, service levels, and incident response procedures.
- **Risk assessment audit:** Assess the organization's process for conducting risk assessments of vendors, including how risks are identified, analyzed, and rated to determine the level of oversight required.
- **Security controls audit:** Evaluate the effectiveness of security controls implemented by vendors to protect the organization's data and systems. This may include reviewing security assessments, penetration testing results, and compliance with security standards.
- **Incident response audit:** Review the organization's incident response plan and assess how it integrates with vendors' incident response procedures to ensure a coordinated response to security incidents or data breaches.
- **Compliance audit:** Verify that vendors comply with relevant laws, regulations, and industry standards, such as GDPR, HIPAA, or PCI DSS. Ensure that vendors provide necessary attestations and certifications to demonstrate compliance.
- **Business continuity and disaster recovery audit:** Evaluate vendors' business continuity and disaster recovery plans to assess their ability to maintain services during disruptions and recover from disasters effectively.
- **Performance monitoring audit:** Assess the organization's process for monitoring vendor performance, including service level agreements (SLAs), key performance indicators (KPIs), and regular vendor reviews to ensure service quality and compliance.
- **Exit strategy audit:** Review the organization's procedures for terminating vendor relationships, including data retrieval, contract termination clauses, transition planning, and ensuring continuity of services if switching to a new vendor or bringing services in-house.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA sets out rules for how private-sector organizations must handle personal information in the course of commercial activities. It includes requirements for obtaining consent, safeguarding data, and notifying individuals of data breaches.
- **Digital Privacy Act (Bill S-4):** This amendment to PIPEDA introduced mandatory data breach notification requirements, compelling organizations to report certain breaches to the Privacy Commissioner of Canada and affected individuals.
- **Privacy Act:** The Privacy Act regulates the federal government's collection, use, and disclosure of personal information. It outlines individuals' rights to access their personal information held by federal government institutions.
- **Canadian Anti-Spam Legislation (CASL):** CASL regulates the sending of commercial electronic messages, including email, text messages, and social media messages. Organizations must obtain consent before sending commercial messages and provide an opt-out mechanism.

Third-party risk management

- **Bank Act:** The Bank Act governs banking regulations in Canada and includes provisions related to privacy and the protection of customer information held by financial institutions.
- **Personal Health Information Protection Act (PHIPA):** PHIPA regulates the collection, use, and disclosure of personal health information by health care providers and others involved in the delivery of health care services in Ontario.
- **Alberta Personal Information Protection Act (PIPA):** PIPA establishes rules for the collection, use, and disclosure of personal information by private sector organizations operating in Alberta.
- **British Columbia Personal Information Protection Act (PIPA):** Similar to Alberta's PIPA, this legislation in British Columbia governs the collection, use, and disclosure of personal information by private sector organizations in the province.
- **Digital Charter Implementation Act:** Proposed legislation that aims to modernize Canada's privacy laws and enhance individuals' control over their personal information. It includes provisions related to data portability, the right to be forgotten, and algorithmic transparency.
- **Cyber security frameworks (e.g., NIST, ISO 27001):** While not specific laws, organizations in Canada often reference internationally recognized cyber security frameworks such as NIST Cybersecurity Framework or ISO 27001 to guide their cyber security practices, including third-party risk management.

Merger and acquisition integration

- **Financial controls audit:** Review financial controls, accounting processes, and reporting systems to ensure accuracy, reliability, and compliance with regulatory requirements.
- **Operational process audit:** Assess operational processes and workflows to identify inefficiencies, redundancies, and opportunities for optimization in the integrated organization.
- **IT systems audit:** Evaluate IT systems, infrastructure, and data security measures to ensure seamless integration, data integrity, and protection against cyber threats.
- **Compliance audit:** Verify compliance with legal, regulatory, and contractual obligations to mitigate risks and ensure adherence to applicable laws and industry standards.
- **Risk management audit:** Identify and assess risks associated with the integration process, including strategic, financial, operational, and compliance risks, and develop mitigation strategies.
- **Vendor and contract audit:** Review vendor contracts, service agreements, and procurement processes to optimize vendor relationships, control costs, and ensure compliance with contractual terms.
- **Human resources audit:** Evaluate HR policies, employee benefits, compensation structures, and talent management practices to address workforce integration challenges and ensure employee engagement.
- **Cultural integration audit:** Assess organizational culture, values, and communication practices to facilitate cultural alignment between the merging entities and promote collaboration and teamwork.
- **Data privacy and security audit:** Audit data privacy practices, security protocols, and compliance with data protection regulations to safeguard sensitive information and prevent data breaches.
- **Post-integration audit:** Conduct a post-merger audit to evaluate the effectiveness of the integration process, measure key performance indicators, identify lessons learned, and make continuous improvement recommendations.

Relevant laws and regulations

- **Competition Act:** The Competition Act regulates mergers and acquisitions to prevent anti-competitive practices, including mergers that substantially lessen competition in the marketplace.
- **Securities laws:** Securities laws in Canada, such as those administered by provincial securities commissions, regulate disclosure requirements, shareholder approvals, and other aspects of M&A transactions involving publicly traded companies.
- **Corporate laws:** Each province and territory in Canada has its own corporate laws governing the formation, operation, and dissolution of corporations, including regulations related to mergers, acquisitions, and other corporate transactions.
- **Tax laws:** Canadian tax laws, including the Income Tax Act, have implications for M&A transactions, including tax treatment of transactions, such as capital gains taxes and tax implications for shareholders.
- **Employment Standards Legislation:** Employment standards legislation at the provincial and federal levels governs issues such as employee rights, termination, and severance pay, which are relevant in M&A transactions that involve employee transfers.

Merger and acquisition integration

- **Privacy laws:** Canada has stringent privacy laws, such as the Personal Information Protection and Electronic Documents Act (PIPEDA), which regulate the collection, use, and disclosure of personal information in M&A transactions.
- **Foreign Investment laws:** The Investment Canada Act regulates foreign investments in Canadian businesses, including acquisitions by foreign investors, and may require approval for certain transactions.
- **Environmental laws:** Environmental regulations at the federal, provincial, and municipal levels in Canada may impact M&A transactions, particularly in industries with potential environmental liabilities.
- **Intellectual Property laws:** Intellectual property laws in Canada protect patents, trademarks, copyrights, and other intellectual property rights, which are important considerations in M&A transactions involving technology or innovation-driven companies.
- **Antitrust laws:** In addition to the Competition Act, antitrust laws in Canada regulate mergers to prevent anti-competitive behavior and ensure fair competition in the marketplace.

Digital transformation

- **Digital strategy audit:** Evaluate the organization's digital strategy to assess alignment with business objectives, identify key initiatives, and ensure that the strategy supports the organization's overall goals.
- **IT governance audit:** Review the organization's IT governance framework to assess the effectiveness of decision-making processes, risk management practices, and resource allocation related to digital transformation projects.
- **Cyber security audit:** Assess the organization's cyber security measures, including data protection controls, access management, threat detection, incident response preparedness, and compliance with cyber security best practices and regulatory requirements.
- **Data governance and privacy audit:** Review data governance policies and practices to ensure the quality, integrity, security, and compliance of data used in digital transformation initiatives, including data privacy and protection measures.
- **Vendor and third-party risk management audit:** Evaluate the organization's vendor management processes to assess risks associated with third-party relationships, ensure compliance with contractual agreements, and mitigate vendor-related risks in digital transformation projects.
- **IT infrastructure audit:** Review the organization's IT infrastructure, including networks, systems, and cloud services, to assess scalability, reliability, performance, and security measures supporting digital initiatives.
- **Change management audit:** Assess the organization's change management processes to evaluate how changes related to digital transformation projects are planned, communicated, implemented, and monitored to minimize disruptions and maximize adoption.
- **Digital skills and talent audit:** Evaluate the organization's digital skills and talent management practices to identify gaps, assess training needs, and ensure that the workforce has the necessary capabilities to support digital transformation initiatives.
- **Compliance audit:** Review regulatory requirements, industry standards, and internal policies to ensure that digital transformation projects comply with applicable laws and regulations, including data protection, privacy, and cyber security requirements.
- **Performance measurement and monitoring audit:** Establish key performance indicators (KPIs) and metrics to measure the effectiveness of digital transformation initiatives, track progress towards goals, and identify areas for improvement through ongoing monitoring and evaluation.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA is Canada's federal privacy law that governs the collection, use, and disclosure of personal information in the private sector, including during digital transformation initiatives.
- **Digital Privacy Act (Bill S-4):** Part of Canada's federal privacy legislation, the Digital Privacy Act amended PIPEDA to strengthen privacy protections, introduce mandatory data breach reporting requirements, and enhance consent rules for the collection of personal information.
- **Canadian Anti-Spam Legislation (CASL):** Canada's Anti-Spam Legislation regulates commercial electronic messages, including email marketing, and requires organizations to obtain consent before sending electronic communications.

Digital transformation

- **Cyber security frameworks:** While not a specific law, organizations in Canada must adhere to cybersecurity best practices and frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to protect digital assets and systems from cyber threats.
- **Canada's Anti-Counterfeiting Trade Agreement (ACTA):** ACTA aims to combat the trade of counterfeit goods and pirated products, including digital content, by establishing international standards for intellectual property protection and enforcement.
- **Electronic transactions acts:** Provinces and territories in Canada have electronic transactions acts that recognize and regulate electronic signatures, contracts, and records, facilitating digital transactions and e-commerce activities.
- **Banking regulations:** Financial institutions in Canada must comply with banking regulations, such as the Bank Act and regulations issued by the Office of the Superintendent of Financial Institutions (OSFI), when implementing digital banking and fintech solutions.
- **Canadian Radio-television and Telecommunications Commission (CRTC) Regulations:** The CRTC regulates telecommunications and broadcasting services in Canada, including rules related to data privacy, net neutrality, and telecommunications infrastructure.
- **Accessibility laws:** The Accessibility for Ontarians with Disabilities Act (AODA) and similar legislation in other provinces mandate digital accessibility standards to ensure that digital services and content are accessible to individuals with disabilities.
- **Consumer Protection laws:** Various consumer protection laws, such as the Competition Act and provincial consumer protection legislation, regulate advertising practices, pricing transparency, and consumer rights in digital commerce.

Data analytics and continuous monitoring

- **Data governance audit:** Review the organization's data governance framework to assess the effectiveness of policies, procedures, and controls related to data management, including data quality, data security, and data privacy.
- **Data analytics process audit:** Evaluate the organization's data analytics processes, including data collection, data analysis techniques, data validation, and data visualization practices to ensure accuracy and reliability of insights derived from data.
- **Continuous monitoring audit:** Assess the organization's continuous monitoring processes, including the monitoring of key risk indicators, performance metrics, and compliance requirements to identify potential issues in a timely manner.
- **Data quality audit:** Audit the organization's data quality management processes to ensure that data used for analytical purposes is accurate, complete, and reliable.
- **Anomaly detection audit:** Review the organization's anomaly detection methods and algorithms to identify and investigate unusual patterns or outliers in data that may indicate errors, fraud, or other anomalies.
- **Model validation audit:** Evaluate the organization's model validation processes to ensure that data models used for analysis are accurate, reliable, and appropriate for the intended purposes.
- **Data privacy and security audit:** Assess the organization's data privacy and security controls to ensure that sensitive data is protected from unauthorized access, disclosure, or misuse.
- **Audit trail review:** Review the organization's audit trail practices to ensure that there is a clear record of data analysis processes, including data sources, transformations, and calculations for transparency and accountability.
- **Compliance audit:** Conduct audits to ensure that data analytics and continuous monitoring activities comply with relevant laws, regulations, industry standards, and internal policies.
- **Risk-based audit approach:** Apply a risk-based audit approach to prioritize internal audit activities related to data analytics and continuous monitoring, focusing on areas of highest risk or impact to the organization.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA sets out rules for how private sector organizations must handle personal information in the course of commercial activities. It governs the collection, use, and disclosure of personal information.
- **Privacy Act:** The Privacy Act regulates how federal government institutions collect, use, and disclose personal information. It applies to federal government departments and agencies.
- **Canadian Anti-Spam Legislation (CASL):** CASL regulates the sending of commercial electronic messages, including email, text messages, and other forms of electronic communication. It also covers the installation of computer programs.
- **Digital Privacy Act (Bill S-4):** The Digital Privacy Act introduced important changes to PIPEDA, including mandatory breach notification requirements and enhanced consent provisions.
- **Alberta Personal Information Protection Act (PIPA):** PIPA governs the collection, use, and disclosure of personal information by private sector organizations in Alberta.

Data analytics and continuous monitoring

- **British Columbia Personal Information Protection Act (PIPA):** Similar to Alberta's PIPA, this legislation governs the collection, use, and disclosure of personal information by private sector organizations in British Columbia.
- **Quebec Act Respecting the Protection of Personal Information in the Private Sector:** This Quebec legislation sets rules for the collection, use, and disclosure of personal information by private sector organizations in the province.
- **Ontario Personal Health Information Protection Act (PHIPA):** PHIPA regulates the collection, use, and disclosure of personal health information by health information custodians in Ontario.
- **Canada's Competition Act:** The Competition Act addresses false or misleading representations and deceptive marketing practices, which can be relevant to data analytics and monitoring activities.
- **Securities regulations:** Various securities regulations in Canada may have implications for data analytics and monitoring activities, especially in the context of financial services and investment activities.

Organization Design and Readiness

- **Governance structure audit:** Evaluates the effectiveness of the governance framework, including the roles and responsibilities of the board of directors, committees, and executive management.
- **Strategic planning process audit:** Assesses the processes used for strategic planning to ensure that they are robust, involve the appropriate stakeholders, and are aligned with the organization's mission and objectives.
- **Risk management audit:** Reviews the organization's risk management strategies and practices to ensure that risks are properly identified, assessed, mitigated, and monitored.
- **Compliance audit:** Ensures that the organization complies with relevant laws, regulations, and internal policies, reducing the risk of legal or regulatory penalties.
- **Human resources audit:** Examines HR policies and practices, including recruitment, onboarding, training, performance evaluation, succession planning, and adherence to labor laws.
- **Change management audit:** Reviews the effectiveness of change management processes to ensure that organizational changes are managed in a controlled and systematic manner.
- **Operational efficiency audit:** Evaluates the efficiency and effectiveness of operational processes, looking for ways to improve productivity, reduce waste, and optimize resource allocation.
- **IT governance and infrastructure audit:** Assesses IT governance structures and the IT infrastructure to ensure that they support the organization's strategic goals and are resilient against cyber threats.
- **Financial management and control audit:** Examines financial controls, budgeting, forecasting, and financial reporting processes to ensure accuracy and integrity in financial management.
- **Culture and ethics audit:** Surveys organizational culture, ethical practices, and employee engagement to ensure they align with the organization's values and contribute to a positive work environment and public image.

Relevant laws and regulations

- **Canada Business Corporations Act (CBCA):** Governs the incorporation and operation of federal corporations, including corporate governance, director responsibilities, and shareholder rights.
- **Employment Equity Act:** Aims to achieve equality in the workplace so that no person is denied employment opportunities for reasons unrelated to ability, and to correct the conditions of disadvantage in employment experienced by women, Aboriginal peoples, persons with disabilities, and members of visible minorities.
- **Canadian Human Rights Act:** Prohibits discrimination in employment and services within federal jurisdiction.
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** Governs the collection, use, and disclosure of personal information in the course of commercial activities.
- **Canada Labour Code:** Covers labor standards, industrial relations, occupational health and safety, and employment equity for federally regulated employees.
- **Accessibility for Ontarians with Disabilities Act (AODA):** Requires organizations in Ontario to ensure that their business and employment practices are accessible to individuals with disabilities.
- **Employment standards acts (Provincial/Territorial):** Each province and territory has its own legislation governing employment standards such as hours of work, minimum wage, leave entitlements, and termination procedures.

Organization Design and Readiness

- **Pay equity acts (Provincial/Federal):** Designed to ensure that female and male employees receive equal pay for work of equal value.
- **Workplace safety and insurance acts (Provincial/Territorial):** Establishes systems for workplace injury and insurance for workers. In Ontario, this is administered by the Workplace Safety and Insurance Board (WSIB).
- **Competition Act:** Ensures that Canadian businesses operate in a competitive marketplace by prohibiting certain business practices that can harm competition, such as price fixing, market allocation, and abuse of dominant position

Insurance mirage

- **Risk management process audit:** Evaluates the effectiveness of the organization's overall risk management framework and its ability to identify, assess, and mitigate insurance-related risks.
- **Insurance coverage adequacy audit:** Reviews insurance policies to ensure that coverage is adequate, appropriate, and aligned with the organization's risk exposure.
- **Claims management audit:** Assesses the efficiency and effectiveness of the claims management process, including timeliness of claims processing, accuracy of settlements, and compliance with policy terms.
- **Compliance with insurance regulations audit:** Ensures that the organization is compliant with all relevant insurance laws and regulations at both the federal and provincial/territorial levels.
- **Policy and procedure review audit:** Examines the internal policies and procedures related to insurance procurement, renewal, and management to ensure they are up to date and followed consistently.
- **Premium payment and allocation audit:** Verifies that insurance premiums are paid on time, properly allocated, and accurately recorded in the organization's financial statements.
- **Insurance vendor management audit:** Evaluates the processes for selecting and managing relationships with insurance brokers, agents, and underwriters to ensure they deliver value and service quality.
- **Underwriting and pricing audit:** Reviews the underwriting standards and pricing models of the organization's insurance providers to ensure they are reasonable and competitive.
- **Subrogation and recovery audit:** Assesses effectiveness in identifying opportunities for subrogation or pursuing recoveries from third parties who may be responsible for causing losses.
- **Contractual risk transfer audit:** Evaluates the adequacy of risk transfer mechanisms within contracts and agreements, such as hold harmless and indemnification clauses, and the requirement for third parties to carry insurance.

Relevant laws and regulations

- **Insurance Companies Act:** This federal act regulates insurance companies in Canada. It establishes the framework for the operation of insurance companies, including capital requirements, ownership, and governance.
- **Provincial insurance acts:** Each province and territory has its own Insurance Act, which regulates the conduct of insurance business within their jurisdictions, including licensing, solvency, and market conduct.
- **Bank Act:** Governs how banks and federally regulated trust and loan companies operate in all financial sectors, including insurance.
- **Office of the Superintendent of Financial Institutions (OSFI) Act:** Establishes the OSFI, which supervises and regulates federally registered insurers, banks, and trust companies.
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** A federal law relating to data protection, which sets out how businesses must handle personal information, including that held by insurance companies.
- **Automobile insurance acts:** Provincial/territorial laws that regulate car insurance, which is mandatory across Canada. These laws dictate the minimum coverage requirements and often establish a framework for handling claims and disputes.

Insurance mirage

- **Property and Casualty Insurance Compensation Corporation (PACICC):** While not a law, PACICC is an industry-funded protection fund that provides protection to policyholders if their insurer fails.
- **Provincial health insurance acts:** Each province and territory has its own act that governs public health insurance, affecting private health insurers by determining what is covered publicly and what can be insured privately.
- **Life and health insurance business practices regulations:** Provincial and territorial regulations that set standards for life and health insurance business practices.
- **Financial Consumer Agency of Canada (FCAC) Act:** Establishes the FCAC, which enforces consumer protection legislation and monitors the conduct of federally regulated financial entities, including insurance companies

Economic rollercoaster

- **Cash flow and liquidity management:** Evaluating the organization's cash flow projections, liquidity position, and working capital management to ensure the organization can meet its short-term obligations.
- **Cost control and reduction:** Ensuring that cost-saving measures are effective and do not compromise critical operations. Auditing procurement, operational efficiencies, and discretionary spending.
- **Revenue assurance:** Verifying that all revenue streams are captured, billed accurately, and collected in a timely manner, and ensuring that the organization is not losing revenue due to inefficiencies or fraud.
- **Supply chain resilience:** Assessing the robustness of the supply chain, including the reliability of suppliers, the risks of supply chain disruption, and the effectiveness of contingency plans.
- **Credit risk management:** Reviewing the credit policies, especially regarding accounts receivables and credit exposure, to ensure that credit risk is being effectively managed.
- **Compliance with financial covenants:** Ensuring the organization complies with all financial covenants associated with its debt agreements, which can be important to avoid defaults during economic downturns.
- **IT systems and cyber security:** Evaluating the reliability and security of IT systems, which are critical for maintaining operations, especially with the increased risk of cyber threats during economic instability.
- **Strategic alignment and business continuity:** Examining whether the organization's strategic initiatives are aligned with the changing economic environment and whether there are robust business continuity plans in place.
- **Human resources and workforce management:** Assessing the risks associated with workforce planning, including the potential for layoffs, furloughs, and the need to retain key talent during economic downturns.
- **Fraud risk assessment:** Increasing vigilance for fraudulent activity that often rises during economic downturns, including assessing the effectiveness of anti-fraud controls and the organization's fraud response plan.

Business resilience (including third parties)

- **Business continuity planning (BCP) audit:** Evaluate the effectiveness of the organization's BCP in ensuring the continuity of critical business functions during disruptions. Review the plan's scope, documentation, testing, and alignment with business objectives.
- **Crisis management audit:** Assess the organization's crisis management framework, including incident response procedures, communication protocols, and decision-making processes during emergencies. Identify gaps and opportunities for improvement.
- **Risk management audit:** Review the organization's risk management practices to identify, assess, and mitigate risks that could impact business resilience. Evaluate the effectiveness of risk assessment processes and risk treatment strategies.
- **Incident response audit:** Evaluate the organization's incident response capabilities, including detection, containment, eradication, and recovery procedures for cyber security incidents, data breaches, natural disasters, and other disruptions.
- **IT disaster recovery audit:** Assess the organization's IT disaster recovery plan to ensure the timely recovery of critical IT systems and data. Review backup strategies, recovery time objectives (RTOs), and testing procedures.
- **Supply chain resilience audit:** Evaluate the resilience of the organization's supply chain by assessing dependencies, vulnerabilities, and contingency plans for key suppliers. Identify risks and develop strategies to mitigate supply chain disruptions.
- **Data protection and privacy audit:** Review the organization's data protection and privacy practices to ensure compliance with relevant laws and regulations. Assess data security controls, data governance processes, and incident response capabilities.
- **Training and awareness audit:** Assess the organization's training and awareness programs related to business resilience, cyber security, and emergency response. Evaluate employee readiness and knowledge of business continuity procedures.
- **Physical security audit:** Evaluate the organization's physical security measures to protect people, assets, and facilities during emergencies. Review access controls, surveillance systems, emergency evacuation plans, and security incident response procedures.
- **Testing and exercise audit:** Review the organization's testing and exercise programs for business resilience. Assess the frequency and effectiveness of drills, tabletop exercises, simulations, and post-exercise evaluations to validate preparedness and identify areas for improvement.

Relevant laws and regulations

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA sets out rules for the collection, use, and disclosure of personal information in the course of commercial activities. Compliance with PIPEDA is crucial for protecting sensitive data and maintaining business resilience in the face of data breaches and privacy incidents.
- **Digital Privacy Act (Bill S-4):** This legislation amends PIPEDA and introduces additional requirements for data breach notification, further enhancing data protection and incident response obligations for organizations.

Business resilience (including third parties)

- **Canadian Anti-Spam Legislation (CASL):** CASL regulates commercial electronic messages, including email marketing and the installation of computer programs. Compliance with CASL is essential for maintaining customer trust and avoiding penalties for non-compliance.
- **Personal Information Protection Acts (PIPA):** Various provinces in Canada, such as British Columbia and Alberta, have their own PIPA legislation that governs the collection, use, and disclosure of personal information within those provinces.
- **Canadian Securities Administrators (CSA) Guidelines:** The CSA provides guidelines and regulations related to cybersecurity and business continuity planning for financial institutions and publicly traded companies in Canada.
- **Bank of Canada's Cyber Security Self-Assessment Guidance:** The Bank of Canada provides guidance on cyber resilience for financial institutions to enhance their cybersecurity posture and ensure operational resilience in the face of cyber threats.
- **Canadian Centre for Cyber Security (CCCS) Guidance:** The CCCS offers guidance and resources to help organizations improve their cyber resilience, including best practices for incident response, threat intelligence sharing, and cybersecurity awareness.
- **Office of the Superintendent of Financial Institutions (OSFI) Guidelines:** OSFI issues guidelines and requirements for financial institutions to ensure the resilience of the Canadian financial system, including expectations for business continuity planning and cybersecurity.
- **Canadian Radio-television and Telecommunications Commission (CRTC) Regulations:** The CRTC regulates the telecommunications and broadcasting sectors in Canada, including rules related to data protection, network security, and service continuity.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework:** While not a Canadian law or regulation, many organizations in Canada use the NIST Cybersecurity Framework as a best practice for developing and implementing cyber security and resilience measures.

Supply chain, capital projects and operational fragility

- **Supplier management audit:** Evaluate the effectiveness of supplier selection, performance monitoring, contract management, and risk mitigation strategies in the supply chain.
- **Inventory management audit:** Assess inventory control processes, accuracy of inventory records, inventory turnover rates, and compliance with inventory management policies.
- **Procurement process audit:** Review procurement procedures, vendor selection criteria, contract negotiations, purchase order processing, and compliance with procurement policies.
- **Supply chain risk management audit:** Evaluate risk identification, assessment, and mitigation strategies related to supply chain disruptions, supplier dependencies, and geopolitical risks.
- **Project management audit:** Assess project planning, budgeting, scheduling, risk management, stakeholder communication, and adherence to project management methodologies in capital projects.
- **Operational performance audit:** Review key performance indicators (KPIs), operational metrics, process efficiency, cost controls, and opportunities for operational improvements.
- **Compliance audit:** Ensure compliance with relevant laws, regulations, industry standards, and internal policies governing supply chain, capital projects, and operations.
- **Data analytics audit:** Utilize data analytics tools to analyze operational data, identify trends, anomalies, and opportunities for process optimization within supply chain, capital projects, and operations.
- **Internal controls audit:** Evaluate the design and operating effectiveness of internal controls related to financial reporting, asset protection, and compliance within supply chain, capital projects, and operations.
- **Business continuity planning audit:** Assess the adequacy of business continuity and disaster recovery plans to mitigate risks associated with supply chain disruptions, operational failures, and other emergencies.

Relevant laws and regulations

- **Canada Labour Code:** Regulates labor standards, occupational health and safety, and employment conditions for federally regulated industries, which can impact operations and supply chain management.
- **Competition Act:** Addresses competition law, including anti-competitive practices, mergers, and deceptive marketing practices that can impact supply chain relationships and capital projects.
- **Customs Act:** Governs the import and export of goods into and out of Canada, including customs duties, tariffs, and trade compliance requirements that affect supply chain operations.
- **Canadian Environmental Protection Act:** Regulates environmental protection, pollution prevention, and hazardous waste management, which can impact capital projects and operations in Canada.
- **Transportation of Dangerous Goods Act:** Regulates the transportation of hazardous materials by road, rail, air, and water, impacting supply chain logistics and operations.
- **Privacy laws (e.g., Personal Information Protection and Electronic Documents Act - PIPEDA):** Regulates the collection, use, and disclosure of personal information in commercial activities, including supply chain management and operations.
- **Canadian Anti-Spam Legislation (CASL):** Regulates commercial electronic messages, including email marketing and SMS communications, which can impact marketing operations within the supply chain.

Supply chain, capital projects and operational fragility

- **Food and Drugs Act:** Regulates the safety and labeling of food, drugs, cosmetics, and medical devices in Canada, impacting supply chain management in industries such as food and healthcare.
- **Canadian Consumer Product Safety Act:** Regulates the safety of consumer products, including product testing, labelling, and recall requirements that can impact supply chain operations.
- **Investment Canada Act:** Regulates foreign investments in Canadian businesses, including capital projects and operations, to ensure they provide a net benefit to Canada.

Climate crisis fallout

- **Carbon footprint analysis:** Audit the organization's greenhouse gas emissions inventory and reporting processes to ensure accuracy and compliance with regulatory requirements.
- **Risk management processes:** Assess the organization's risk management framework to identify how climate change risks are identified, assessed, and mitigated within the overall risk management process.
- **Policy and strategy alignment:** Audit the alignment of the organization's climate change policies and strategies with its overall business objectives and long-term sustainability goals.
- **Climate-related financial disclosures:** Review the organization's disclosure practices related to climate risks and opportunities to ensure transparency and compliance with reporting standards such as TCFD.
- **Supply chain resilience:** Evaluate the organization's supply chain management processes to identify climate-related risks within the supply chain and assess the resilience of key suppliers.
- **Physical risk assessment:** Audit the organization's assessment of physical risks associated with climate change, such as extreme weather events, sea-level rise, and temperature changes.
- **Transition risk assessment:** Assess how the organization evaluates and addresses transition risks related to regulatory changes, market shifts, and technological developments impacting its operations.
- **Scenario analysis:** Review the organization's use of scenario analysis to model the potential impacts of different climate change scenarios on its operations, financial performance, and reputation.
- **Energy efficiency and renewable energy:** Evaluate the organization's efforts to improve energy efficiency, reduce carbon emissions, and transition to renewable energy sources as part of its climate change mitigation strategy.
- **Employee training and awareness:** Assess the organization's training programs and employee awareness initiatives related to climate change risks, ensuring that staff are informed and engaged in sustainability efforts.

Relevant laws and regulations

- **Canadian Environmental Protection Act, 1999 (CEPA):** CEPA is the primary federal legislation in Canada for regulating toxic substances and protecting the environment, including addressing climate change impacts.
- **Pan-Canadian Framework on Clean Growth and Climate Change:** A collaborative effort between the federal government and provinces/territories to set emissions reduction targets and implement climate mitigation measures.
- **Greenhouse Gas Pollution Pricing Act (GGPPA):** This federal law establishes a national carbon pricing system to reduce greenhouse gas emissions by pricing carbon pollution.
- **Species at Risk Act (SARA):** SARA is aimed at protecting wildlife species at risk, including those affected by climate change and habitat loss.
- **Canadian Energy Regulator Act (CERA):** Regulates the energy industry, including pipelines, and addresses environmental considerations such as climate impacts and emissions.
- **Federal Sustainable Development Act:** Sets out requirements for federal departments to implement sustainable development practices, including addressing climate change risks.
- **Impact Assessment Act (IAA):** Requires federal environmental assessments for major projects to consider climate change impacts and mitigation measures.

Climate crisis fallout

- **National Energy Board Act:** Regulates the energy industry, including pipelines, and may include requirements related to climate change mitigation and adaptation.
- **Climate Change Accountability Act (proposed):** Proposed legislation to set binding emissions reduction targets for Canada in line with international climate goals.
- **Provincial and territorial regulations:** Each province and territory in Canada may have its own environmental laws and regulations related to climate change, emissions reductions, and environmental protection

Fraud and corruption

- **Vendor and supplier due diligence:** Reviewing the processes and controls in place for onboarding and managing vendors and suppliers to ensure compliance with anti-corruption policies and to prevent conflicts of interest.
- **Expense reimbursement:** Examining expense reimbursement processes to ensure that expenses are legitimate, adequately supported, and compliant with company policies to prevent fraudulent claims.
- **Procurement processes:** Assessing procurement processes to identify any potential red flags for corruption, such as bid-rigging, conflicts of interest, or kickbacks.
- **Employee payroll and benefits:** Reviewing payroll and benefits processes to ensure that employee compensation is accurate and in compliance with company policies to prevent payroll fraud.
- **Cash handling and financial controls:** Evaluating cash handling procedures and financial controls to prevent misappropriation of funds and unauthorized transactions.
- **Conflict of interest:** Assessing the organization's policies and procedures for disclosing and managing conflicts of interest among employees and key stakeholders to prevent unethical behavior.
- **Contract compliance:** Reviewing contracts and agreements to ensure compliance with regulatory requirements, internal policies, and ethical standards to prevent fraud and corruption risks associated with contract mismanagement.
- **Data security and privacy:** Examining data security measures to protect sensitive information from unauthorized access and ensure compliance with data privacy regulations to prevent data breaches and associated fraud risks.
- **Internal controls and segregation of duties:** Evaluating the effectiveness of internal controls and segregation of duties within key processes to prevent and detect fraudulent activities.
- **Whistleblower program effectiveness:** Assessing the effectiveness of the organization's whistleblower program, including the reporting mechanisms, anonymity protections, and follow-up procedures to encourage the reporting of fraud and corruption incidents.

Relevant laws and regulations

- **Criminal Code of Canada:** The Criminal Code contains provisions that address various types of fraud and corruption offenses, such as fraud, bribery, and corruption.
- **Corruption of Foreign Public Officials Act (CFPOA):** This legislation makes it a criminal offense for Canadians and Canadian companies to bribe foreign public officials.
- **Competition Act:** The Competition Act contains provisions related to deceptive marketing practices, price-fixing, bid-rigging, and other anti-competitive behaviors that can be associated with fraud and corruption.
- **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA):** This legislation aims to prevent money laundering and terrorist financing activities, which are often associated with fraud and corruption.
- **Public Servants Disclosure Protection Act (Whistleblower Protection):** This Act provides protection to federal government employees who disclose wrongdoing in the workplace, including fraud and corruption.
- **Securities Act:** Regulates the securities industry in Canada and includes provisions related to fraud, insider trading, and other securities-related offenses.

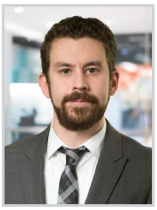
Fraud and corruption

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** Governs the collection, use, and disclosure of personal information in the private sector and includes provisions related to data security and privacy, which are relevant to fraud prevention.
- **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC):** Regulates and monitors financial transactions to prevent money laundering and terrorist financing activities.
- **Canada Business Corporations Act (CBCA):** Contains provisions related to corporate governance, financial disclosure, and transparency, which are important in preventing fraud and corruption within corporations.
- **Anti-Corruption laws:** In addition to the CFPOA, Canadian companies operating internationally should also be aware of anti-corruption laws in other countries, such as the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act, which may apply to their activities abroad.

Contributors

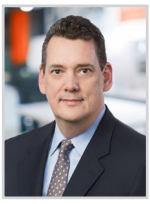
Richard Arthurs
National Internal Audit Leader

Olena Batuev
Business Intelligence Developer



Drew Buhr
Partner, Digital

Craig Burkart
National Leader, Insurance Advisory



Gord Chalk
Consulting Leader, Energy and Utilities

Caitlin Crowley
Partner, Digital

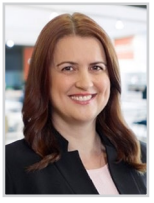
James Dyack
Partner, Valuations and Litigation Support

Johnny Earl
Managing Director, Corporate Finance

Mariesa Fett
National Leader, Enterprise Risk Services

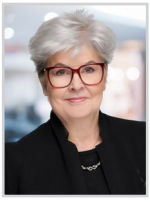
Soumya Ghosh
Director, Digital Transformation and Advisory

Denise Gigova
Partner, Digital



Adriana Gliga
Partner, Privacy and Data Governance

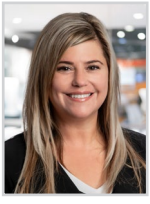
Wendy Gnenz
Partner, Digital Strategy and Planning



Mary Larson
Leader, Organizational Renewal

Chris Law
Partner, Cyber Security

Jason Lee
Partner, Machine Learning and AI



Lisa Majeau-Gordon
National Leader, Forensics and Litigation Support

Gustavo Meschler
Business Advisor, Enterprise Risk Services

Contributors

Len Nanjad
Partner, Organization Change Management

Eugene Ng
Partner, Cyber Security

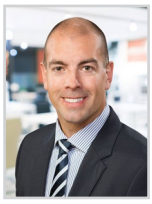
Cameron Ollenberger
Partner, Enterprise Risk Services

Edward Olson
ESG Leader

Hash Qureshi
Partner, Enterprise Risk Services

Phil Racco
Partner, Enterprise Risk Services

Mark Reynolds
Managing Director, Corporate Finance



Mike Reynolds
Managing Director, Corporate Finance

Ian Shaule
Director, Advanced Analytics

Lee Thiessen
Vice President, Real Estate and Construction

Cliff Trollope
National Leader, Business Resilience Services

Colin Wenngatz
Partner, Data and 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®
A member of the Praxity Global Alliance