Beyond regulation

Privacy demands while adapting to COVID-19 and supporting a culture of continuous improvement

MNP.ca

Table of Contents

Internal audit plays a core risk management role

Internal audit reinforces the need for effective controls and helps align everyone from the executive suite to the mail room around identifying, understanding, and mitigating privacy risks.

This function is particularly valuable through disruptive periods when risk management appears at odds with responding quickly and effectively to change. Internal audit clears a path through the privacy and security minefield — whether the challenge is rolling out a new business model, undergoing a digital transformation, or responding to a global pandemic.

Asks the right questions of executives and key leaders

Internal audit also helps individuals across the organization understand the consequences of their decisions and actions and take steps to mitigate them. In terms of data privacy and security, that means ensuring all data collection, analysis and management processes serve their intended purpose without introducing new challenges or liabilities.

The following questions can help provide clarity around appropriate privacy practices, behaviours, and considerations:

1. What are our regulatory and legal requirements?
2. Do we understand where PII is located across the organization?
3. Do we have privacy policies and procedures in place?
4. How do we protect PII across the information lifecycle?
5. Do we have a process in place to respond to privacy and cyber security incidents?
6. Are we monitoring our privacy program?
7. Do we have a process to review secondary uses of data?
8. Are we identifying privacy risks?
9. Are we performing privacy impact assessments on new initiatives?
10. Do we understand the impact of COVID-19 on our privacy program?

Understands how privacy and security fit within other organizational risks

Internal auditors rarely consider anything in isolation. One of their most valuable functions is helping leaders understand how the specific risks relate to one another in context. For example, the data and privacy risks of rapidly onboarding a new application versus the risk of permanently losing customers whose shopping habits the global pandemic has shifted.

Internal Audit provides a 360-degree view of the entire risk landscape, which can help key decision makers find the most effective path forward: The path that both protects the organization from the most likely and / or damaging consequences of any specific threat — and allows it to seize the greatest opportunities available.

Makes sure priorities and controls are functioning as expected

Even the most thorough risk assessments, frameworks, and controls cannot guarantee universal compliance — nor can they account for every risk the organization will face. That's why formal audits remain one of Internal audit's most important functions. As a snapshot of the current state, audits reveal how current practices either insulate or expose the organization.

Among the many data privacy and security concerns a formal audit can help address include:

- Are employees regularly sharing sensitive information over unencrypted platforms (e.g. email)?
- Is the organization using PII for purposes besides those disclosed?
- Does the organization securely delete PII once it has served its purposes?
- Has the organization evolved its data handling and storage processes to comply with new or upcoming regulations?
- Have employees and leaders received adequate training on the secure and responsible handing of PII?

Formal audits can also help simulate the impacts of a data breach or leak. Knowing the organization's deficiencies and strengths at a given moment can reveal (a) where a privacy violation is most likely to occur, (b) the likely extent and severity of the data compromise, (c) how difficult it would be to fix the problem, and (d) the likely financial, regulatory, and reputational damages.

These kinds of insights are sobering and highly effective at getting everyone on the same page for rigorous privacy and information risk management.

When to seek Internal audit advisory

Review overall enterprise data privacy and security risks

Annual audit planning, program maturity efforts, alignment with new regulations, etc.

Digital transformation

Business process automation, data analytics, client engagement, etc.

New technology implementation

Cloud migrations, ERP, CRM, switching vendors, etc.

New business or customer engagement models

e-Commerce, value-added services, subscription-based sales or services, etc.

Privacy auditing in the age of COVID-19

Securing remote work and collaboration

Internal audit can advise in evaluating the organization's current remote work practices, and capabilities to determine where it's currently exposed to privacy risks.

This audit would focus on new and existing technology platforms to identify whether any security vulnerabilities are being exposed. Also, whether employees are taking the appropriate data handing measures and protecting their devices against cyber attacks.

Supporting a secure return to work

Internal audit can also help evaluate and calculate the risks involved with adopting new COVID-19 testing and contact tracing applications.

Responsibilities would also include vetting specific vendors to make sure they are following adequate security protocols. Also, coordinating with executives, human resources, and performance managers to ensure the right data collection and management policies and procedures are in place for this kind of data collection and sharing.

How to get started

Developing an Internal audit privacy strategy can seem daunting, especially if you don't have an Internal audit department or haven't included privacy within your annual audit planning. Remember this is a continuous and iterative process. Take small steps initially to get a lay of the land and understand the most urgent risks. Then use those learnings to continually mature the program.

Understand your context

Begin by understanding the role(s) private and personal information play within and throughout the organization and the specific regulations these are subject to.

What jurisdictions does the organization operate within and what regulatory laws apply? For example, all Canadian organizations must comply with the Personal Information Protection and Electronic Documents Act (PIPEDA). Organizations that engage with European clients must follow General Data Protection Regulations (GDPR), etc.

What PII does the organization collect, use, process, and share? This includes employee data, customer data, information collected through the organization's website, surveys, emails and other correspondence, etc.

How is PII collected and shared across the organization? Examples include CRM, ERP, human resources management (HRM), and data analytics applications. Also, email, spreadsheets, paper files, shared file servers, accounting software, etc.

What policies, procedures, and data privacy frameworks are currently in force? When were they last updated? Are they readily available? Have employees received adequate training? Are they being followed?

Define your next steps

Once you have a baseline, start planning for how to bring the organization into compliance. Reach out to relevant leaders and subject matter experts to address the most obvious risks and deficiencies. Encourage them to connect with one another to create better alignment across the organization.

You'll also need to start incorporating privacy audits into annual audit plans. Depending on the program maturity, level of risk, and number of regulatory frameworks involved, you may choose to conduct additional monthly or quarterly audits until the organization consistently achieves compliance.

Embed internal audit into other business initiatives

Take a proactive approach to addressing data privacy and security risks as they emerge by getting involved with upcoming initiatives across the organization. Reach out to executives and department heads to find out what their teams are currently working on and whether these could potentially introduce new risks.

Position internal audit as a supportive and helpful resource that can reduce costs, save time, and increase their chances of success. Ideally, leaders and change agents will begin approaching Internal Audit prior to beginning any new initiatives.

Some high-risk initiatives you'll want to pay close attention to include:

- Cloud migrations (especially those involving personal or private information)
- Digital transformation and new technology adoption
- New data management policies and processes
- New business models (e.g. e-commerce)

Focus on education

Everyone in the organization needs the knowledge and skills to handle information securely. Work with Human Resource and Information Technology departments to roll out continuous training and awareness initiatives. At the very least this means ensuring everyone understands the data security policies and procedures, is informed of any changes, and knows how they apply specifically to their work and the applications they use.

Consider incorporating regular data security and privacy training into every employee's performance management evaluations. There are numerous organizations provide customized online modules on relevant data privacy laws, best practices, and pitfalls. The vast majority of leaks and breaches occur at the individual level, so this can be one of the most effective ways for organizations to reduce privacy risks.

Executing an effective privacy audit

Privacy needs to be an integral part of the annual audit plan. Just as data informs strategic and engagement decisions across the organization, department leaders and planners need data to improve the collection and management of PII.

Define the scope and context

Every country and jurisdiction you operate in has specific privacy legislation you must comply with. Your audit needs to account for and measure against these expectations.

Create a list of all the places you conduct business; your employees and customers have citizenship; and where you collect, process, use, and share PII. Next, identify the relevant privacy legislation (e.g. PIPEDA, GDPR, etc.) which apply and when. Then catalogue the PII you collect, process, use, and share — as well as how and in what context the various legislations apply.

These insights will inform how you build and execute your audit plan. But they are also extremely useful for making recommendations around organizational privacy policies and procedures — and how the organization can most effectively and efficiently manage privacy compliance moving forward.

Build a risk model for your organization

Next, select an appropriate risk model that best applies to your scope and context. You can choose from several different frameworks to help focus your audit and understand how certain factors increase or decrease your risk. These can also be tailored to your industry, regulatory obligations, and digital maturity.

The most common options include:

Canadian Standards Association (CSA) 10 Fair Information Principles Set out under PIPEDA, these tenets apply to all organizations that operate in Canada or collect personal information on Canadian citizens.	**National Institute of Standards and Technology (NIST) Privacy Framework** A voluntary set of risk management principles to help establish a common language and goals for cross-organization teams mitigate privacy risks.
GDPR Privacy rules and considerations organizations must follow when operating in the European Union or collecting personal information European Union citizens.	**System and Organization Controls (SOC) Trust Services Criteria for Privacy** Multi-phased, technology-focused framework that analyzes the nature, functionality, breadth, processes, and security of data management systems.

CSA / PIPEDA 10 Fair Information Principles

Accountability

Designate an individual who is responsible for information management, compliance, and security across the organization.

Purpose

Define all primary and secondary uses for information before it is collected.

Consent

Collect, use, and disclose only the information that users have agreed to in advance.

Limiting collection

Collect only information that is necessary for the intended purposes — and do so fairly and lawfully.

Limiting use, disclosure and retention

Use information only for its intended purposes — and securely dispose of the information once it has served those purposes.

Accuracy

Ensure information is sufficiently accurate, complete, and up to date to serve its intended purposes.

Safeguards

Ensure security controls are in place to protect information. Their stringency must be proportionate to the sensitivity of the information.

Openness

Be transparent about information management policies and practices. Make this information public and easily accessible.

Individual Access

Respond promptly and transparently to individuals who request disclosure on what information has been collected, how it's being used, and how it is being stored.

Challenging compliance

Enable individuals to challenge the organization's compliance with the information management framework.

Develop a work plan

Given your chosen risk framework, identify the systems / applications, departments, individuals, and third-party partners you need to include in your privacy audit. Also, the regulatory bodies and legislation the organization needs to comply with. Outline the steps required to fully evaluate the organization's privacy and security posture, including:

- Who you will need to speak with
- How you will evaluate employee habits and behaviours
- What system logs and historical data you will need to review
- What upcoming initiatives or projects you will need to evaluate
- Key areas of non-compliance to be aware of

Compare your work plan with the guidelines and best practices outlined in your chosen risk framework to make sure it still aligns with your needs and objectives.

Execute the audit

Reach out to relevant stakeholders to conduct interviews, collect relevant documentation, test controls, and observe how individuals and systems are managing sensitive information. Analyze the organization's privacy and security controls to understand:

- Whether these align with your chosen risk framework
- Whether they are performing as expected
- Whether users are harnessing these controls as prescribed and intended.

Report and implement key learnings

Extensively document all findings and their immediate and potential consequences. Be sure to emphasize those which reveal significant risks and shortfalls across the organization. Use the parameters within your selected risk framework to demonstrate your observations in context.

Frame results, insights, and recommendations in an action-oriented, forward looking format which will allow decisionmakers to make quick and effective changes moving forward. This report will also form the baseline for future privacy audits.

Resourcing for effective privacy audits

As you execute your audit, you may realize the organization lacks the skills and expertise to identify and advise on privacy risks. The following model can help determine what skills are required to meet your needs and objectives, as well as when it may be advisable to partner with a third-party.

Analyze current capabilities

Review your audit team's existing security and data privacy expertise. Does it possess the qualifications and skills required to evaluate and advise on data privacy risks? If yes, you can begin forming a data privacy and security working group to oversee the process internally.

If not, you'll need to decide whether an external or hybrid sourcing model is most appropriate. The fewer qualified individuals you have, or the less qualified these individuals are, the more likely you are to look outside the organization.

Bring skills and training up to date

Support your privacy audit program continued specialization by equipping your team with the knowledge and skills they need to be effective. Professional development opportunities for key subject matter experts help to legitimize your efforts and back sound leadership with relevant certifications. More importantly, it keeps your organization up to date on the latest regulations, technologies and best practices.

Recruit qualified program partners

Identify service providers with a proven track record to fill any gaps. Look for organizations with experience in your industry or sector that understand your risks and needs. Specifically, you want a program partner that can contribute skills and expertise your organization is lacking — especially if you're considering a hybrid sourcing model.

Depending on your capacity, complexity, and goals, you may consider recruiting multiple partners to help address specific needs. For example, one partner may specialize in regulatory compliance, while another is expert in technical controls. In these cases, communication and alignment are essential.

Implement the resourcing model

Monitor your audit team's capacity and capabilities as you put the necessary training and manpower in place. Share your findings with team members, relevant leaders, and third-party vendors — and encourage input on what resources may be lacking or underutilized. Use these insights to continuously upgrade your resourcing model.

The path forward

Data collection and analytic capacities have evolved dramatically over the past 15 years and will continue to accelerate for years to come. However, now may be a good time to tap the brakes and re-focus priorities around data risk and whether current practices and procedures are meeting increasingly stringent privacy and security requirements.

Governments are increasingly concerned about the information organizations collect about citizens and the steps they are taking to preserve public trust. Consumers, too, are more conscientious than ever about their privacy rights and have increased expectations on how organizations collect, use and protect their data.

No matter the maturity of your current data privacy program, now is the time to look at it with a fresh set of eyes. The following steps will ensure you stay on the right side of the law, and may even help you find new opportunities to safely add more fuel to your data engine.

Understand the impact

Begin with an environmental scan to understand the specific privacy risks that affect your business and industry. Prioritize these risks against a range of factors, including the:

- Types of breaches and attacks you're most likely to face
- Systems and information that are most likely to be at risk of a breach
- Potential costs and damages of specific data falling into the wrong hands
- Costs and resources involved with protecting specific systems and information

You also need to evaluate how COVID-19 has shifted privacy and security risks. What new business models, processes, and technologies has your oganization introduced? They may have created new requirements for the collection and storage of sensitive information — and new vulnerabilities as well.

It's not feasible, or even advisable to fortify the entire organization. Extra layers of security add extra costs. And information needs to flow to be useful. Focus on the areas of highest vulnerability and highest consequence and assess whether controls are prioritized and functioning in line with your risk assessment.

Provide training

All team members must understand their roles in information security. Determine whether the organization is supporting a culture of knowledge and empowerment through ongoing training programs — and whether these are sufficiently coaching employees on general best practices, as well as your organization's specific data management policies and procedures.

Where possible, ensure specific modules suit each team member's access to PII and assess the various data management tools they use. Ensure the training is kept relevant to increase engagement and help address the specific risks various roles and departments face across the organization

Overcommunicate

Management should strive to make data privacy and security a regular topic of discussion across the organization. An internal audit therefore needs to ensure there is a process for integrating this in to agendas to broadcast frequent tips, updates, and. reminders about cyber security and secure information management — and encourage questions.

Advocate for a culture where team members feel confident in calling out risky actions and blowing the whistle on unethical or non-compliant practices. Drive home the importance of secure technology practices at work and at home. Especially given that the two environments are now one and the same for many people.

Collaborate

Build strong relationships with leaders across the organization and secure buy-in on the importance of data privacy and security. Each department will have specific objectives, priorities, and key performance indicators. Position the internal audit team as a partner who can support the responsible implementation of new technologies and business models.

Agility and adaptability are important, especially as organizations are responding to COVID-19. But quick decisions also need to be calculated and risk based. That can only happen when there's an open channel between the decision maker and the risk expert.

Audit

Close the loop on this process by continuously measuring the effectiveness of security controls. Perform formal audits using the data privacy frameworks discussed previously, and ask:

- Is the organization focusing on the right risk priorities?
- Where is the organization most vulnerable to data leaks or breaches?
- Are information management practices and priorities consistent across the organization?
- Is the organization in compliance with all policies, procedures, and regulatory requirements?
- Do employees understand their roles and are they handling PII appropriately?
- Has the organization adopted any new business models or technologies — and have these introduced new risks we need to account for?

There is still a place for exhaustive annual or semi-annual audits. But given the pace of technological and cultural change — especially those brought on by the COVID-19 pandemic — it's pertinent to ask these questions more frequently.

Regularly evaluate what is changing across the organization, both technologically and structurally, and audit the extent these are compromising your preparedness to protect customer data. In this way, internal audit teams can bridge the gap between the ever-competing needs for agility and assurance.

About MNP

Our internal audit professionals will work with you to develop an appropriate system of internal controls to address your key business risks. We create tailored, cost-effective internal audit solutions to help you achieve effective corporate governance and provide senior management with timely and reliable business intelligence.

MNP is a leading national accounting, tax and business consulting firm in Canada. We proudly serve and respond to the needs of our clients in the public, private and not-for-profit sectors. Through partner-led engagements, we provide a collaborative, cost-effective approach to doing business and personalized strategies to help organizations succeed across the country and around the world.

To learn more, contact:

Adriana Gliga-Belavic, CISSP, CIPM, PCIP
National Privacy Leader
416 419 4228
adriana.gliga-belavic@mnp.ca

PRAXITY™ Empowering Business Globally

KINCENTRIC› Best Employer CANADA 2019