Risk management and compliance monitoring

Today's webinar you'll learn about how risk management and compliance monitoring can help your organization to protect the personal information it collects from clients, customers, employees, or other individuals.

First, what is risk management?

Well, when you think about risk, it's really the **potential** for something negative to happen. Risk *management, then,* is when you identify and evaluate risks AND work to monitor, minimize, avoid, or otherwise mitigate those risks.

Let's take a look at some the risks involving personal information, or PI.

Organizations face a number of common privacy risks when it comes to protecting PI. Here are some of the most common:

- Inadequate electronic or physical security safeguards
- Human error
- PI being shared too broadly within an organization
- Snooping or misuse of PI by staff
- Theft, hacking or other intrusions
- Damage to reputation resulting from a potential breach
- Additional financial costs associated with managing breaches after they occur.

PIPA requires organizations to make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks. Risk management can help you to identify specific risks to the security of the PI your organization collects, and to determine appropriate solutions.

A risk management approach to protecting PI allows organizations to implement a scalable and proportionate approach to compliance.

The threshold for compliance with PIPA is one of reasonableness. What would a reasonable person would consider appropriate in the circumstances?

Well, what is "reasonable" for protecting PI can depend on any number of factors.

For example, the security safeguards your organization needs to implement will depend on the context for collection and processing of PI, the types and amount of PI involved, the sensitivity

of the PI, and so on. For instance, your safeguards will be different if you are collecting email addresses only versus credit card numbers, family history, or health information.

Just know that if your organization decides to collect and use ANY PI, you will incur a degree of risk.

By working to understand and manage the risks, organizations can minimize the risk and ensure compliance with your legal obligations.

Risk assessment tools will help you identify and evaluate risks involving PI, mitigate risks, and ensure compliance with PIPA.

Let's take a look at some common risk assessment tools….

First up is a **Privacy Impact Assessment**, or PIA.

So… what is a PIA?

A PIA is an assessment of a current or proposed initiative. PIAs help organizations like yours determine whether their projects will meet legal requirements and obligations under PIPA for collecting, using, disclosing, or otherwise processing PI.

Why do a PIA?

PIAs are one of the most effective risk assessment tools. They can help ensure compliance throughout the lifecycle of your program or information sharing initiative. They provide transparency.

They can also save you time, money, and your reputation.

Who should write the PIA?
The person who knows the initiative well is often the best person to describe it in your PIA. This person does not need to be a privacy expert or the CEO of your organization.

PIAs are scaleable to the size of your organization, but be sure to include the following elements:

- Identify **who** is responsible for your organization's information sharing initiative or program;
- Include the objective or **what** you are trying to achieve with the initiative; and

- Identify the **types** of PI that are to be collected, used or disclosed through the initiative.
    - Any collection, use or disclosure of PI must be what a ***reasonable person*** would consider appropriate in the circumstances.
- Indicate **how** your organization will collect, use or disclose the PI, obtain **consent** for these activities, and which section of PIPA provides you with the **authority** to conduct these activities;
- Be sure to include an inventory or framework of potential risks, including the likelihood and potential harm associated with the risks, and appropriate mitigation measures.
    - For example, how likely is it that the PI you have collected could be accessed by those without authority? What will you do to prevent unauthorized access from occurring? What would you do if a breach occurs?
- Detail the security safeguards and compliance monitoring that you'll have in place to ensure PI is handled properly within the program or initiative.
- Remember: Your organization should review and update PIAs as initiatives change or evolve.

What about other methods for risk assessment? Here's where activities like compliance monitoring and privacy or security audits come in….

Regularly monitor your security safeguards to ensure that they are operating effectively. In addition, monitor compliance with policies and training to ensure staff understand and follow expectations for protecting PI.

Compliance monitoring and internal or external audit activities are scalable to the size of your business and the need for any particular initiative. These activities allow you to find and address privacy concerns before they become large and costly issues**.**

For larger organizations with an audit or compliance department, audits of privacy and security for PI should be regularly scheduled into organizational audit or review plans. Your Privacy Officer should be included in the planning and involved in mitigating any risks to PI identified through an audit or compliance review.

For smaller organizations, or for less formal reviews, organizations should develop checklists to assist in monitoring compliance. Review these lists on a regular basis to ensure they reflect the appropriate security safeguards for types, amount and sensitivity of the PI collected by the organization.

In addition to PIAs, audits and compliance monitoring activities, there are other methods you should take to ensure that your organization is managing risks and taking reasonable steps to protect PI. These methods include:

- ensuring contracts are in place that detail privacy and security obligations for service providers;
- providing regular training for staff on privacy obligations, and reviewing and modifying training periodically to ensure it remains current;
- monitoring and updating your PI inventory to ensure it reflects current holdings, collections, uses, and disclosures;
- making sure that PI is retained for one year after using that information to make a decision that directly affects the individual the information is about - and taking steps to destroy personal information that is no longer needed for the purpose of collection or for other legal or business purposes.
- reviewing and revising privacy and access to information policies, as needed; and
- ensuring breach and incident management response protocols are in place and reviewed regularly.

As with any other aspect of your business, you should be prepared to deal with things when they go wrong. Breaches do occur, and processes should be in place for responding to them. This includes determining whether the risk of harm to individuals makes it appropriate or necessary to notify individuals and the OIPC.

A well-established risk management program will help you learn from these incidents and use them to identify gaps or weaknesses in existing privacy controls.

Risk management and compliance monitoring offer approaches to systematically identify and assess privacy risks and obligations at the outset of a project and over time. By conducting risk assessments and monitoring compliance on a regular basis, your organization will be better able to establish measures that avoid or mitigate the risks. And you'll be better able to achieve compliance with PIPA by protecting the PI you collect, use, or disclose.