PROJET DE LOI 64
Protection des renseignements personnels au Québec

Présenté par Vincent Bureau

Délégué à la protection des données personnelles
Directeur des Services de protection des données & Vie privée

Présentation du 15 Octobre 2020


HITACHI
Inspire the Next
C’EST
NOTRE
AVENIR
PRIVACY+SECURITÉ = CONFIANCE
= AFFAIRES
= ADMINISTRATION PUBLIQUE

Centre intégré universitaire de santé et de services sociaux du Nord-de-l'Île-de-Montréal

Québec

Desjardins

Gouvernement du Québec

- Développer une identité numérique
- Encadrer les agences de crédit (projet de loi 53)
- Protéger les renseignements personnels dans le privé et le public (projet de loi 64).

LA PARABOLE DU BBQ

HITACHI
Inspire the Next

“C’est drôle,
vous magasinez un barbecue et sur votre Facebook ou votre Instagram
on vous offre des barbecues à répétition!”

Sonia Lebel, ministre de la Justice, 12 juin 2020.

La parabole est une figure de rhétorique consistant en une courte histoire qui utilise les événements quotidiens pour illustrer un enseignement, une morale ou une doctrine. Wikipedia.

Data protection & Privacy

https://www.youtube.com/watch?v=T5mwleZBYoA

ISACA Section de Québec

HITACHI Inspire the Next

Agenda

Introduction

1 Comprendre le projet de loi 64
2 Comparer le projet L64 avec le RGPD
3 Utiliser les ressources ISACA
4 Lancer votre programme de mise en conformité
5 Vos questions

PROTECTION DES RENSEIGNEMENTS PERSONNELS: LES PRINCIPES À APPLIQUER

HITACHI
Inspire the Next

1. Traitées de manière **licite, loyale et transparente** au regard de la personne concernée
2. Collectées pour des **finalités limitées**
3. Adéquates, pertinentes et limitées à ce qui est **nécessaire** au regard des finalités
4. **Exactes** et, si nécessaire, tenues à jour ;
5. **Conservées** pendant une durée n'excédant pas celle nécessaire au regard des finalités
6. Traitées de façon à garantir une **sécurité** appropriée des données
7. Le responsable du traitement est responsable du respect de ces principes ("**responsabilité**") et doit être en mesure d'en **apporter la preuve**

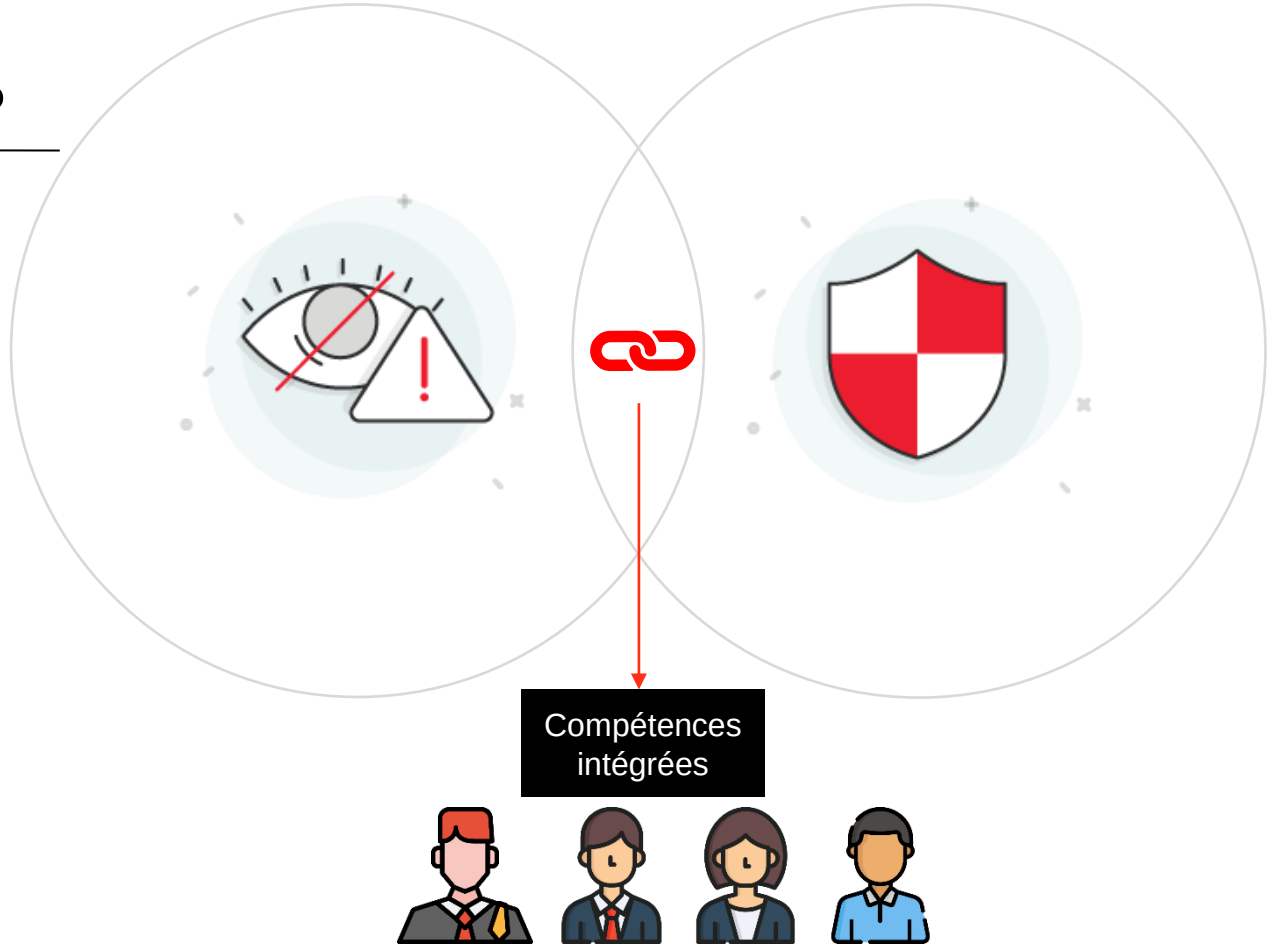
PRIVACY+SECURITY

HITACHI
Inspire the Next

Protection des RP

Protection des données à caractère personnel dans le contexte des droits de la personne

- Surveillance
- Catégorisation
- Discrimination



Sécurité de l'information

Protection de tous les actifs informationnels (y compris les RP), des informations confidentielles et des systèmes hébergeant les actifs informationnels

- Confidentialité
- Intégrité
- Disponibilité

Vincent Bureau

Délégué à la protection des données personnelles
Directeur des Services de protection des données & Vie privée

Diplômé *Maîtrises Droit Public, Télécom., Gestion de projet, Marketing,*
Certifié *CDPSE, CIPP/E, ISO/IEC27701, PMP, MoP, PRINCE2, Mg. Benefits.*

Expertise:

- +20 ans Télécom. & TI,
- +15 ans Gouvernance, Risque, Conformité,
- Lois & traités: Données Personnelles, Sécurité, Commerce Électronique, Canada, U.E, U.S.A, Afrique, Asie,
- Privacy by Design & by Default,
- Privacy Enhancing Technologies,
- Gestion de programme de conformité,
- Formateur (École de Technologies Supérieure - ÉTS),
- Conférencier (ISACA, PMI, Printemps Numérique MTLconnecte, Salon de la Data).

Email: vincent.bureau@hitachi-systems-security.com
Twitter: @vincentbureau
Linkedin: @bureauvincent

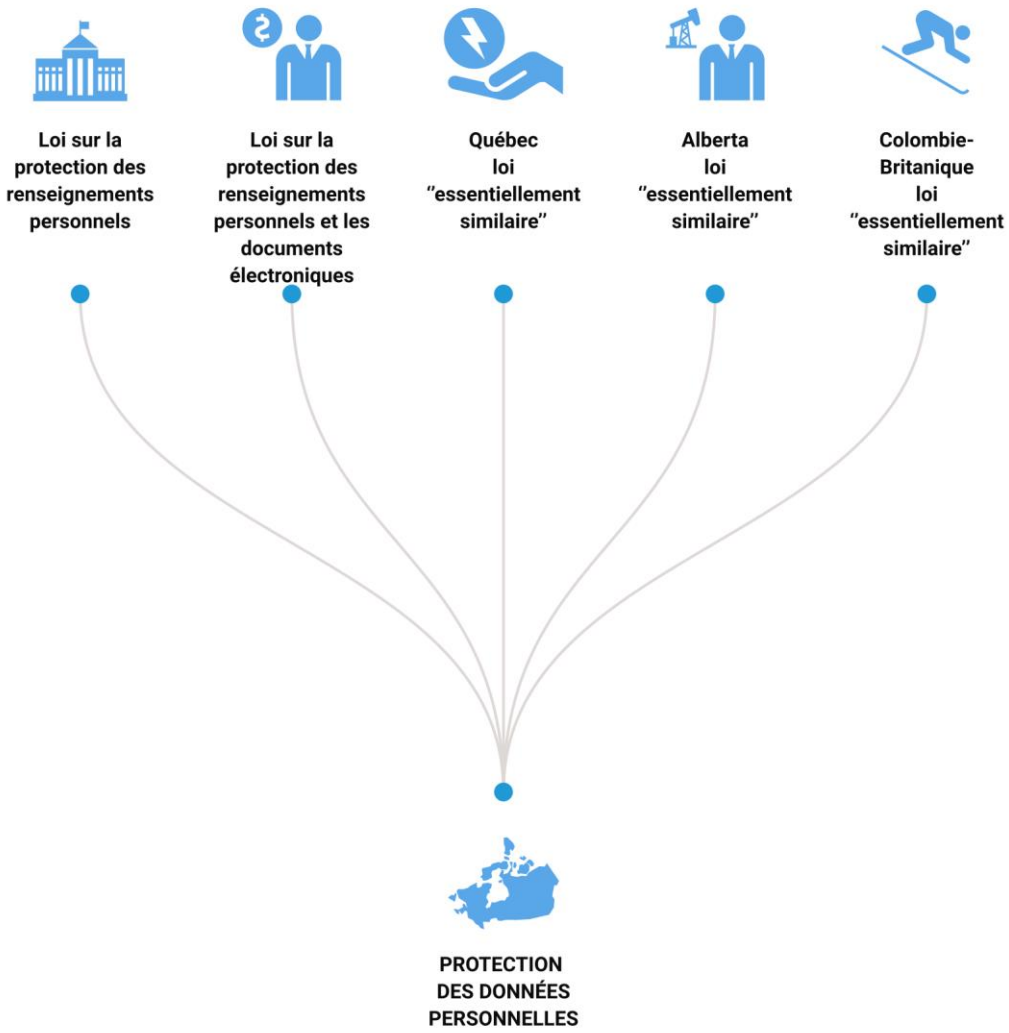
ISACA Section de Québec

HITACHI Inspire the Next

Agenda

Introduction
1 Comprendre le projet de loi 64
2 Comparer le projet L64 avec le RGPD
3 Utiliser les ressources ISACA
4 Lancer votre projet de mise en conformité
5 Vos questions

Les régimes de protection au Canada



Le projet de Loi 64

HITACHI
Inspire the Next

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.

- Secteur privé
- Secteur public
- Partis politiques

LE PROJET DE LOI 64

HITACHI
Inspire the Next

Loi sur la protection des renseignements personnels dans le secteur privé

La protection des RP au Québec

- **Code civil du Québec**
  - Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire
- **Charte des droits et libertés de la personne**
  - Toute personne a droit au respect de sa vie privée
- **Loi sur la protection des renseignements personnels**
  - Le représentant de la personne morale qui a autorisé l'infraction est passible de la peine qui y est prévue

Commission d’Accès à l’Information . CAI

La **Commission** peut:

- De sa propre initiative ou sur la plainte d’une personne intéressée faire enquête sur toute matière relative à la protection des renseignements personnels

- Ordonner à une personne exploitant une entreprise de donner communication ou de rectifier un renseignement personnel ou de s’abstenir de le faire

Les objectifs du projet de Loi 64

Référence:
Loi sur la protection des renseignements personnels dans le secteur privé

1. Donner le contrôle aux citoyens,
2. Responsabiliser les entreprises,
3. Protéger par conception & par défaut,
4. Aligner aux principes du RGPD et bonnes pratiques européennes,
5. Garder les entreprises compétitives,
6. Augmenter les sanctions.

PL64: points principaux

PRINCIPES

- Confidentialité
- Recueil du consentement de la personne

droits

risques

PL64: points principaux

RESPONSABILITÉ RENFORCÉE

- Responsable de la Protection des Renseignements Personnels
- Protection de la vie privée par conception & par défaut
- Politiques et pratiques
- Évaluations des facteurs relatifs à la vie privée

droits

- Impartition & Transfert
- Incident de confidentialité
- Nouveaux droits pour les personnes
- Consentement exprès

risques

PL64: points principaux

ALLÉGEMENTS

- Exclusion de la définition de « renseignements personnels » des contacts d’affaires
- Exception de consentement pour la recherche
- Exception de consentement pour les transactions commerciales

droits

risques

PL64: points principaux

SANCTIONS

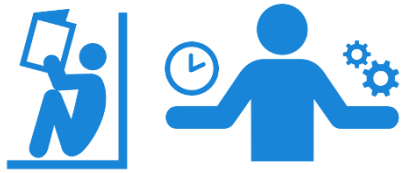
- Commission d’accès à l’information, pouvoir augmenté
- Sanctions jusqu'à 10 millions de dollars ou 2 % du chiffre d'affaires mondial
- Sanctions pénales pouvant aller jusqu'à 25 millions de dollars ou 4 % du chiffre d'affaires mondial.
- Poursuite en dommages-intérêts

droits

risques

PL64: Responsable de la Protection des Renseignements Personnels

- Un nouveau rôle de RPRP
- Par défaut le responsable PRP de chaque entreprise est le Président
- Responsabilité de la mise en œuvre et respecte la loi
- Délégation possible

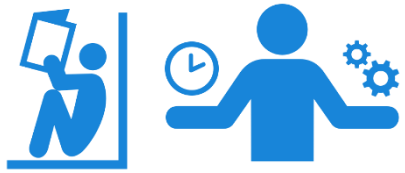


PL64: Protection de la vie privée par conception & par défaut

- Obligation de s’assurer que les paramètres des produits ou services technologiques offrent le plus haut niveau de confidentialité par défaut, sans aucune intervention de la personne concernée

PL64: Évaluations des facteurs relatifs à la vie privée

- Évaluation des facteurs relatifs à la vie privée (EFVP) pour les projets de système d'information ou de prestation électronique de services avec des traitement de renseignements personnels



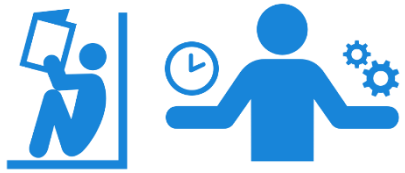
PL64: Impartition

Entente écrite entre l’entreprise et le fournisseur de services:

- Mesures prises par le fournisseur de services pour assurer la confidentialité des renseignements personnels
- Pas d’utilisation autre des RP
- Pas de conservation des RP après expiration du contrat
- Obligation d’informer d’une violation ou tentative de violation de la confidentialité RP et permettre les vérifications

PL64: Transfert

- Évaluation des facteurs relatifs à la vie privée (EFVP) avant de communiquer des renseignements personnels à l'extérieur du Québec pour déterminer si les renseignements bénéficieront d'un niveau de protection équivalent à celui accordé en vertu de la Loi



PL64: Prochaines étapes

Processus législatif

1. Projet de loi 64, 12 juin 2020
2. Commission pour consultation, automne 2020
3. Modifications LPRPSP un an après la date de sanction du projet de loi
4. Droits de portabilité des données, trois ans après la date de sanction
5. Entrée en vigueur 2021 / 2023

RP, Marque, Développement d'affaires, Relations clients

https://www.youtube.com/watch?v=ErMZe_e79Nw

LE PROJET DE LOI 64

HITACHI
Inspire the Next

Loi sur la protection des renseignements personnels dans le secteur public

Les objectifs du projet de Loi 64

Référence:
Loi sur l'accès aux documents des organismes publics
et sur la protection des renseignements personnels

1. Permettre les nouveaux services numériques
2. Renforcer la protection des renseignements personnels
3. Améliorer le traitement des demandes d'accès

PL64: points principaux

- Responsabilité,
- Analyse du risque et information,
- Gestionnaire de renseignements personnels,
- Incidents de confidentialité,
- Consentement,
- Données de recherches,
- Exportation des renseignements personnels,
- Demandes d'accès à l'information abusives,
- Procédure de la Commission d'accès à l'information.

droits

risques

ISACA Section de Québec

HITACHI Inspire the Next

Agenda

Introduction

1 Comprendre le projet de loi 64

2 Comparer le projet L64 avec le RGPD

3 Utiliser les ressources ISACA

4 Lancer votre programme de mise en conformité

5 Vos questions

ALIGNEMENT RGPD

HITACHI
Inspire the Next

Le projet de loi 64 suit les principes du RGPD et les bonnes pratiques Européennes.

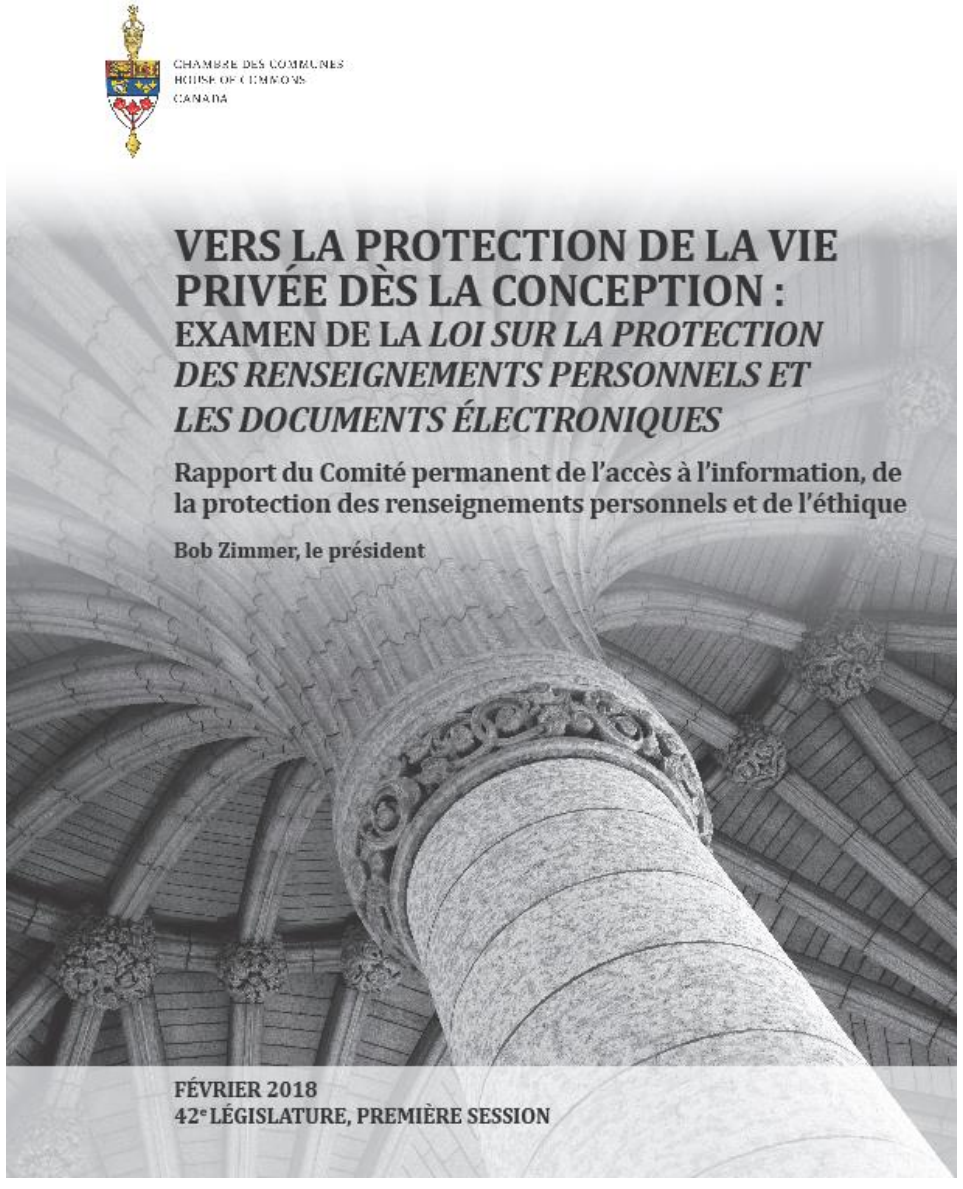
Sonia Lebel, ministre de la Justice, 12 juin 2020.

L'alignement sur le RGPD permettra des coopérations avec l'Europe sur la cybersécurité.

Éric Caire, Ministre délégué à la transformation numérique, iHack, 20 juin 2020

RAPPORT LPRPDE: VERS LA PROTECTION PAR CONCEPTION

HITACHI
Inspire the Next



RGPD: UNE REFERENCE POUR LA COLOMBIE BRITANIQUE

‘’While PIPA predates the GDPR and does not provide the same level of privacy protection, provisions such as mandatory breach notification will likely be incorporated into PIPA in the near future. Until that time, organizations can largely ensure compliance with PIPA by ensuring compliance with the GDPR, with some exceptions’’

OIPC, March 2018

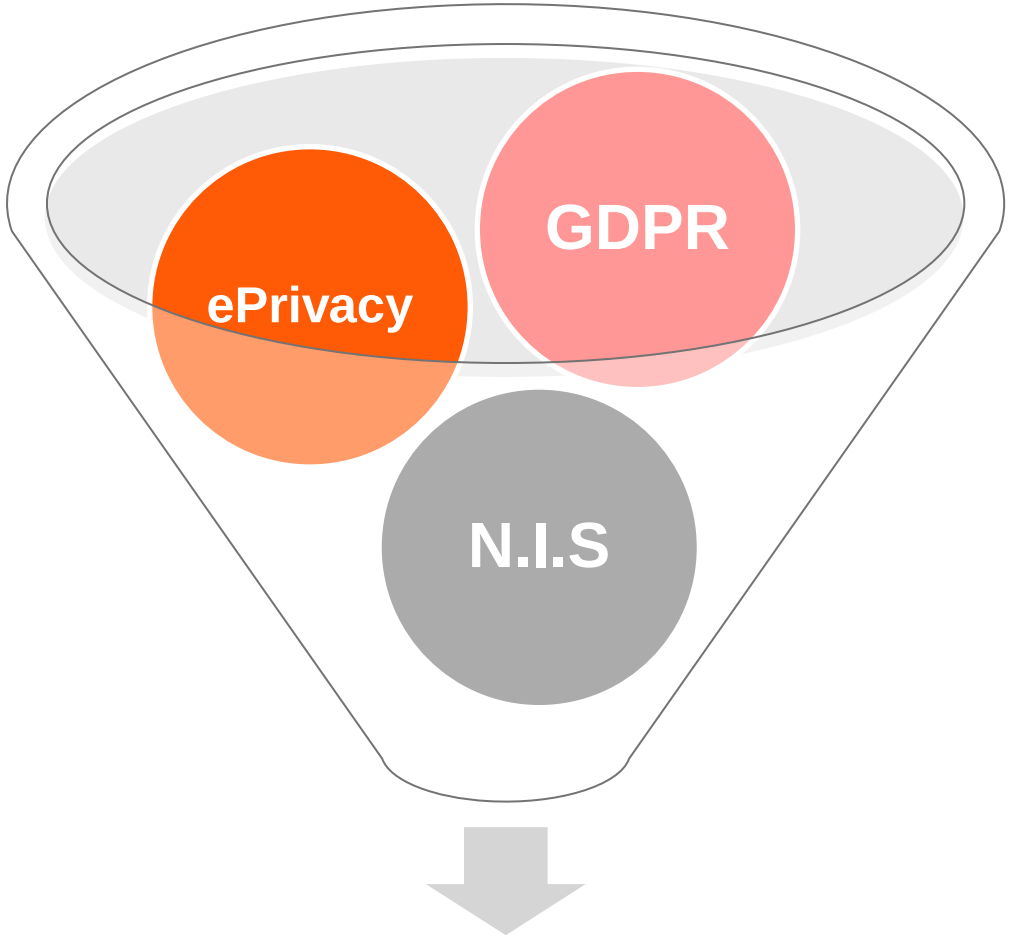
RGPD

Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

droits

risques

Le cadre de réference européen



COMPLIANCE

Les changements du RGPD

HITACHI
Inspire the Next

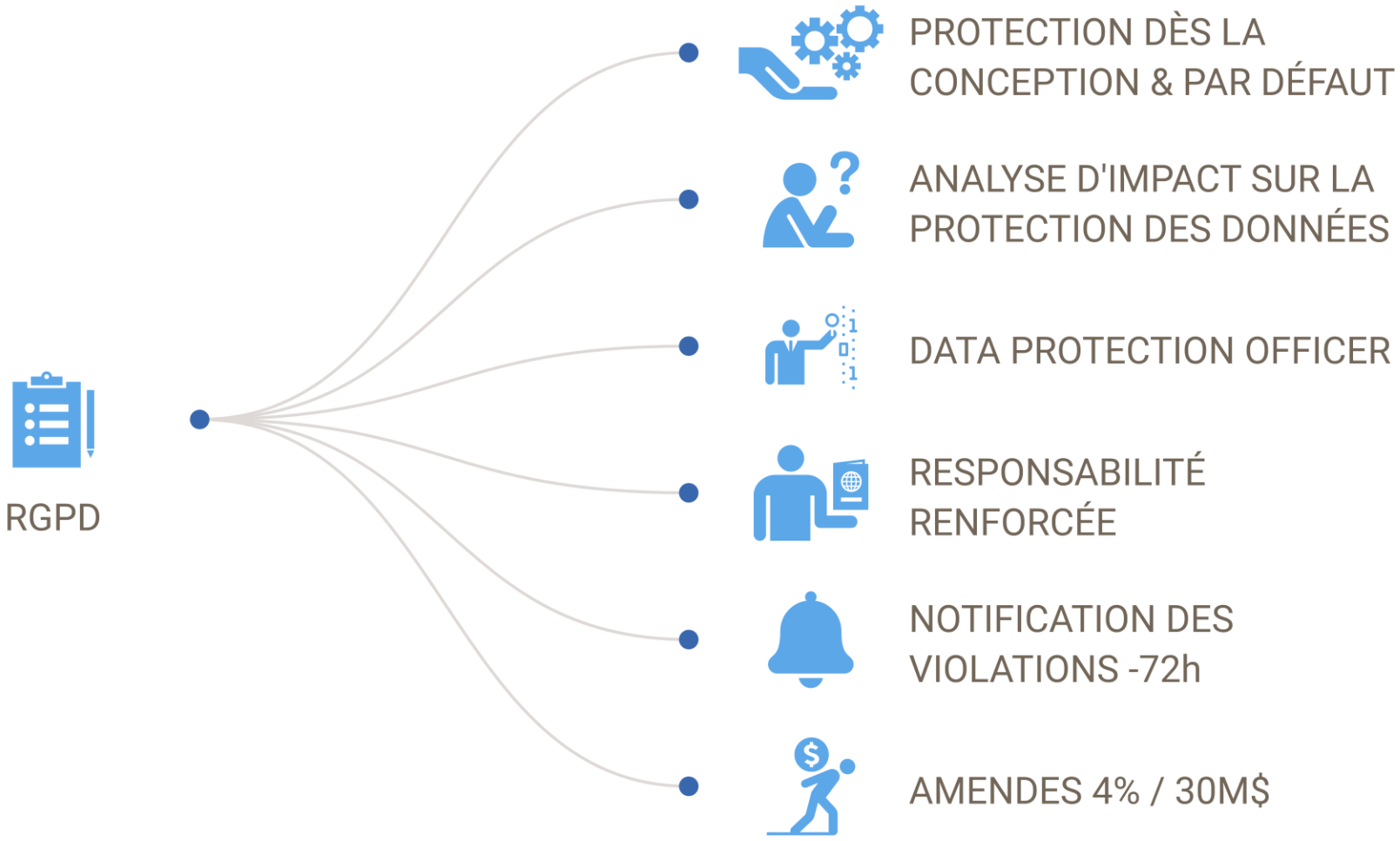


TABLEAU COMPARATIF PROJET DE LOI 64 VS RGPD

HITACHI
Inspire the Next

HITACHI
Inspire the Next

PrudenceAI

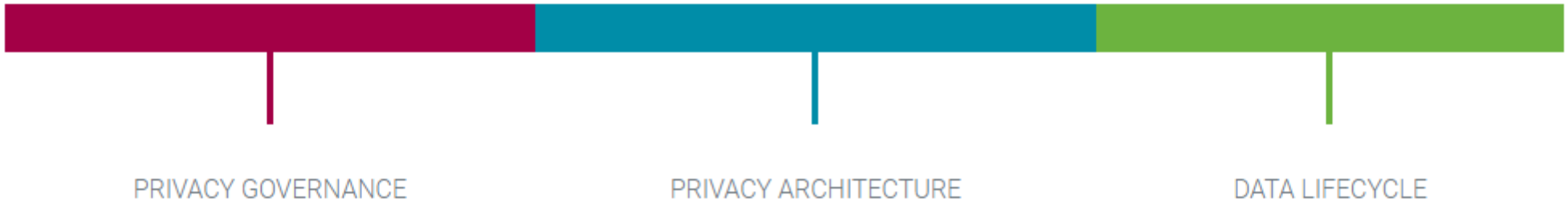
		Québec Projet de loi (PL) n° 64 *Loi sur la protection des renseignements personnels dans le secteur privé (Chapitre P-39.1)*	Union Européenne Règlement Général sur la Protection des Données (RGPD)
1. Champ d'application	1.1. Temporel	L'étude du projet de loi commencera à l'automne.	Pleinement applicable depuis le 25 mai 2018
	1.2. Territorial	Sur le territoire du Québec: • Applicable au secteur privé : Toute entreprise qui recueille, détient, utilise ou communique des renseignements personnels • Applicable au secteur public • Applicable aux partis politiques	Applicable au secteur privé et public. Critère d'établissement : RT et ST établis dans l'UE ou l'EEE. Critère de ciblage : RT et ST établis hors de l'UE/EEE mais dont les activités de traitement sont liées: * à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou * au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
	1.3. Matériel	- Champ d'application inchangé pour les entreprises. Spécificités: - Les renseignements personnels visés comprennent ceux recueillis par l'entreprise, même si leur conservation est assurée par un tiers - La LPRPSP ne viendra pas s'appliquer " aux renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise, tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail."	Applicable aux traitements de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données personnelles appelées à figurer dans un fichier Non applicables - Aux traitements réalisés dans le cadre d'une activité strictement personnelle ou domestique - Aux informations anonymisées

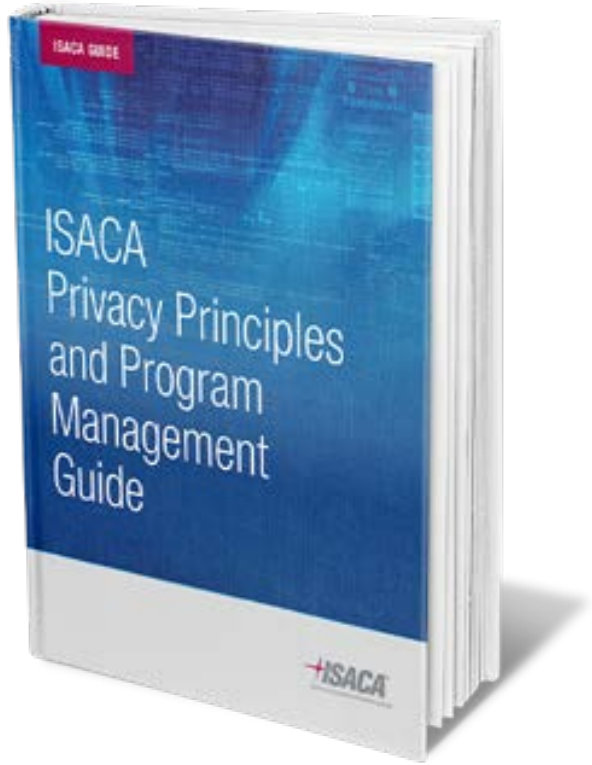
ISACA Section de Québec

HITACHI Inspire the Next

Agenda

Introduction
1 Comprendre le projet de loi 64
2 Comparer le projet L64 avec le RGPD
3 Utiliser les ressources ISACA
4 Lancer votre projet de mise en conformité
5 Vos questions





ISACA Section de Québec

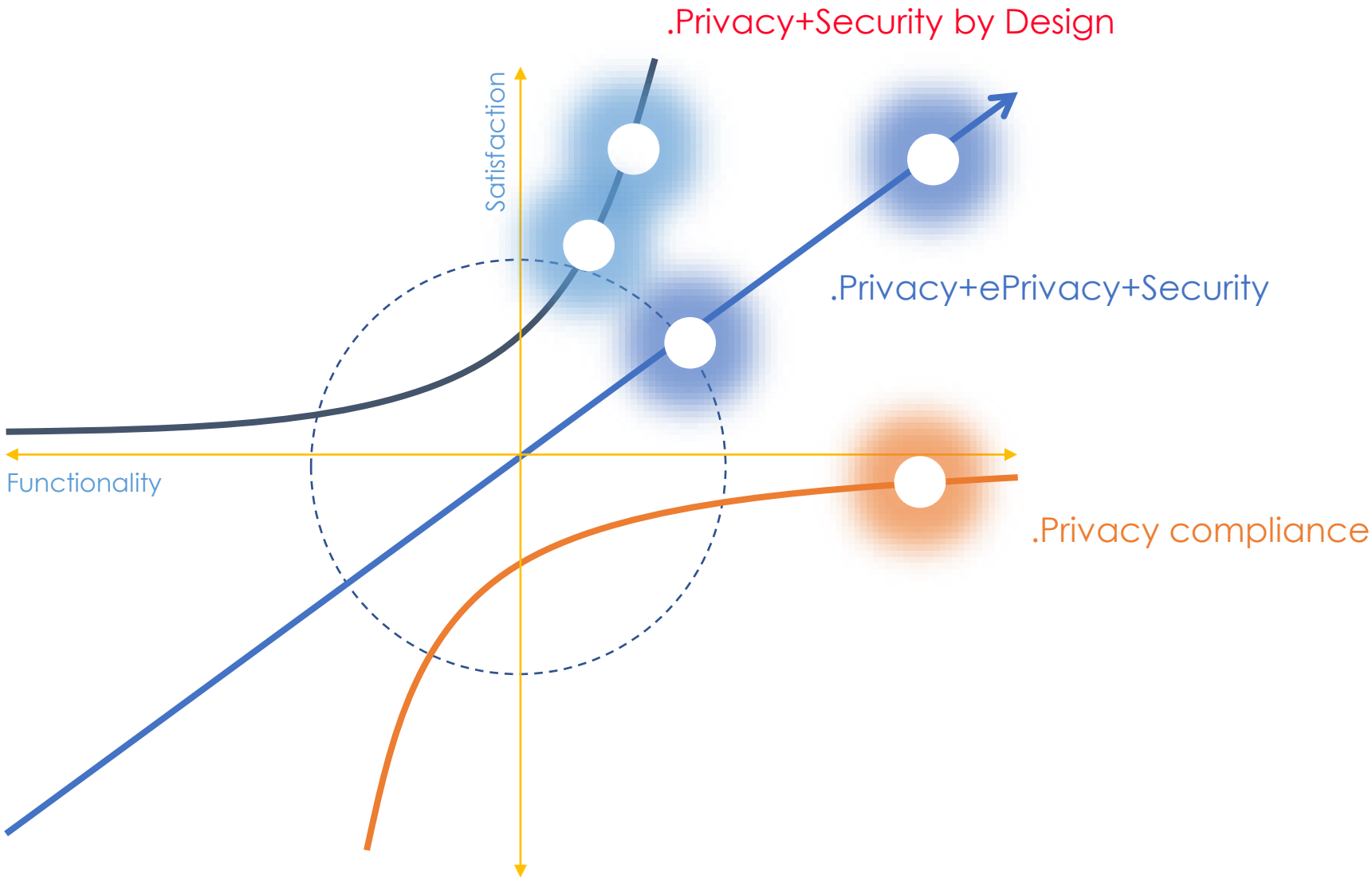
HITACHI Inspire the Next

Agenda

Introduction
1 Comprendre le projet de loi 64
2 Comparer le projet L64 avec le RGPD
3 Utiliser les ressources ISACA
4 Lancer votre programme de mise en conformité
5 Vos questions

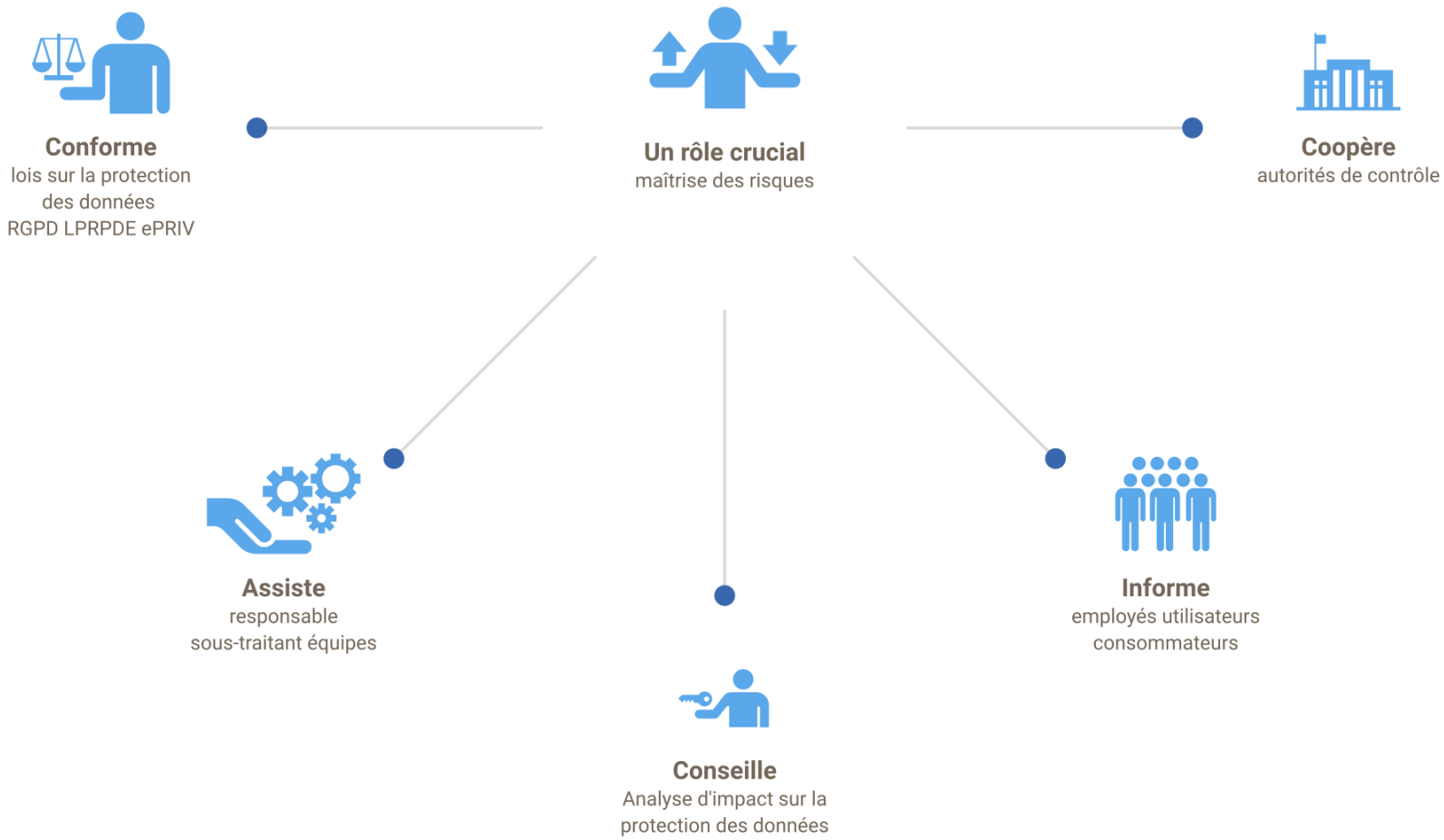
PRIVACY+SECURITY BY DESIGN

HITACHI
Inspire the Next

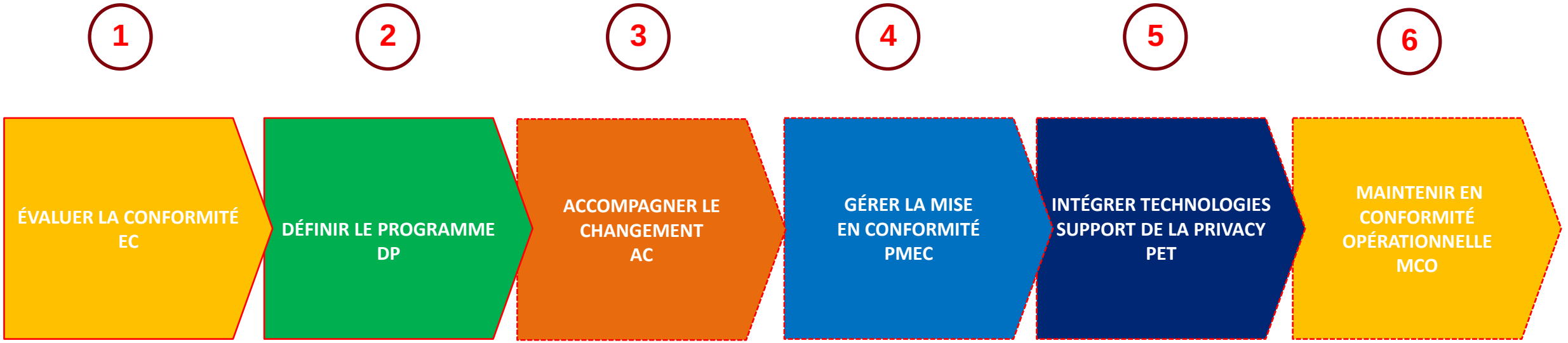


DATA PROTECTION OFFICER

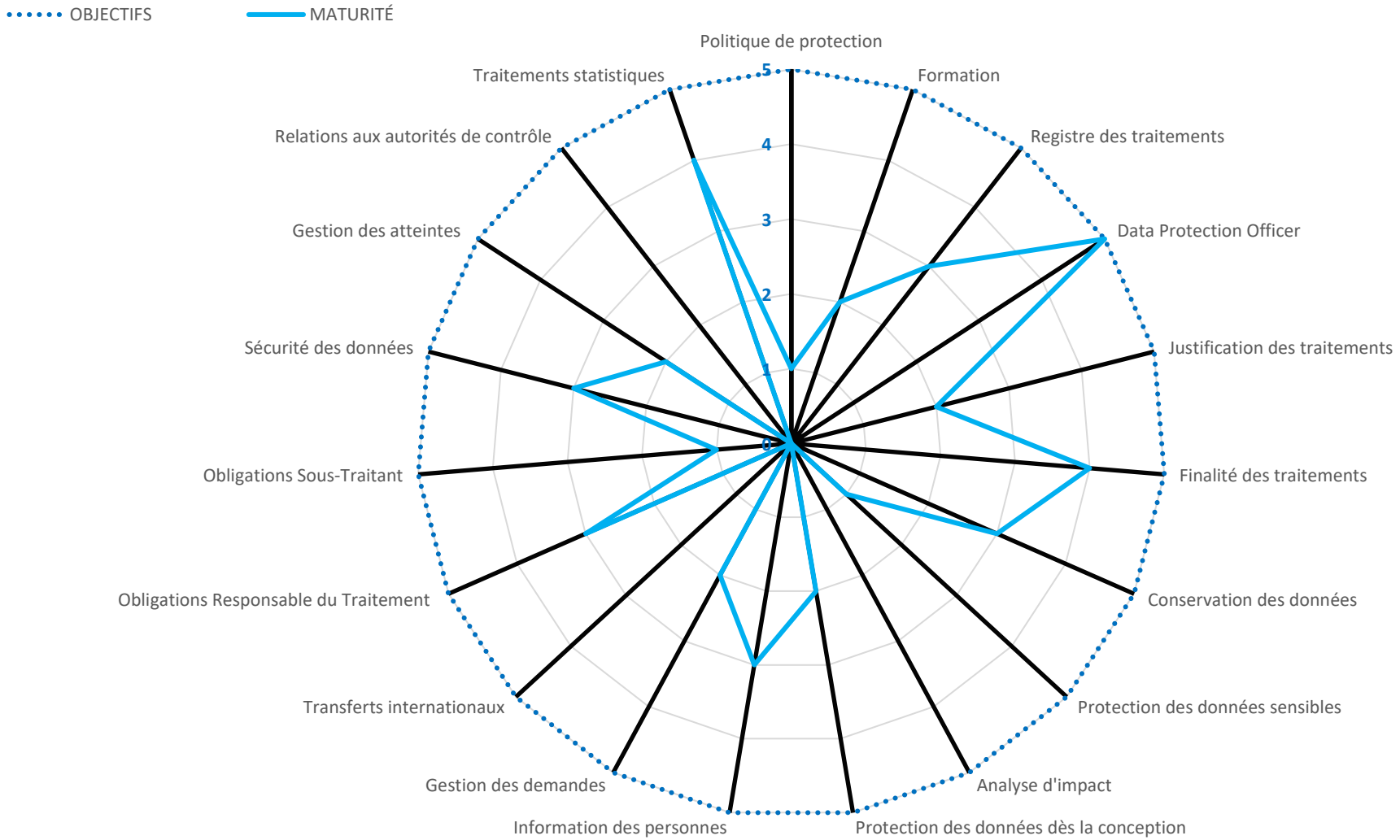
rend compte directement au niveau le plus élevé



ORGANISER LA CONFORMITÉ



Évaluer votre maturité organisationnelle



Évaluer la maturité de votre organisation

WEBINAIRE PL64

5 évaluations de maturité offertes

Évaluations de maturité à la protection des renseignements personnels d'une durée de 3 heures offertes aux organisations Québécoises ayant des membres ISACA.

Accompagner le changement

CRÉER
UN SENTIMENT D'URGENCE

FORMER
une coalition

DÉVELOPPER
une vision

COMMUNIQUER
la vision

INCITER
à l'action

DÉMONTRER
des résultats rapides

BÂTIR
sur les résultats pour accélérer

ANCRER
dans la cultutre d'entreprise

Types & Catégories
d'information personnelle

Strategic Privacy by Design IAPP
DPOsolutions inc.

Protection par Conception & par Défault

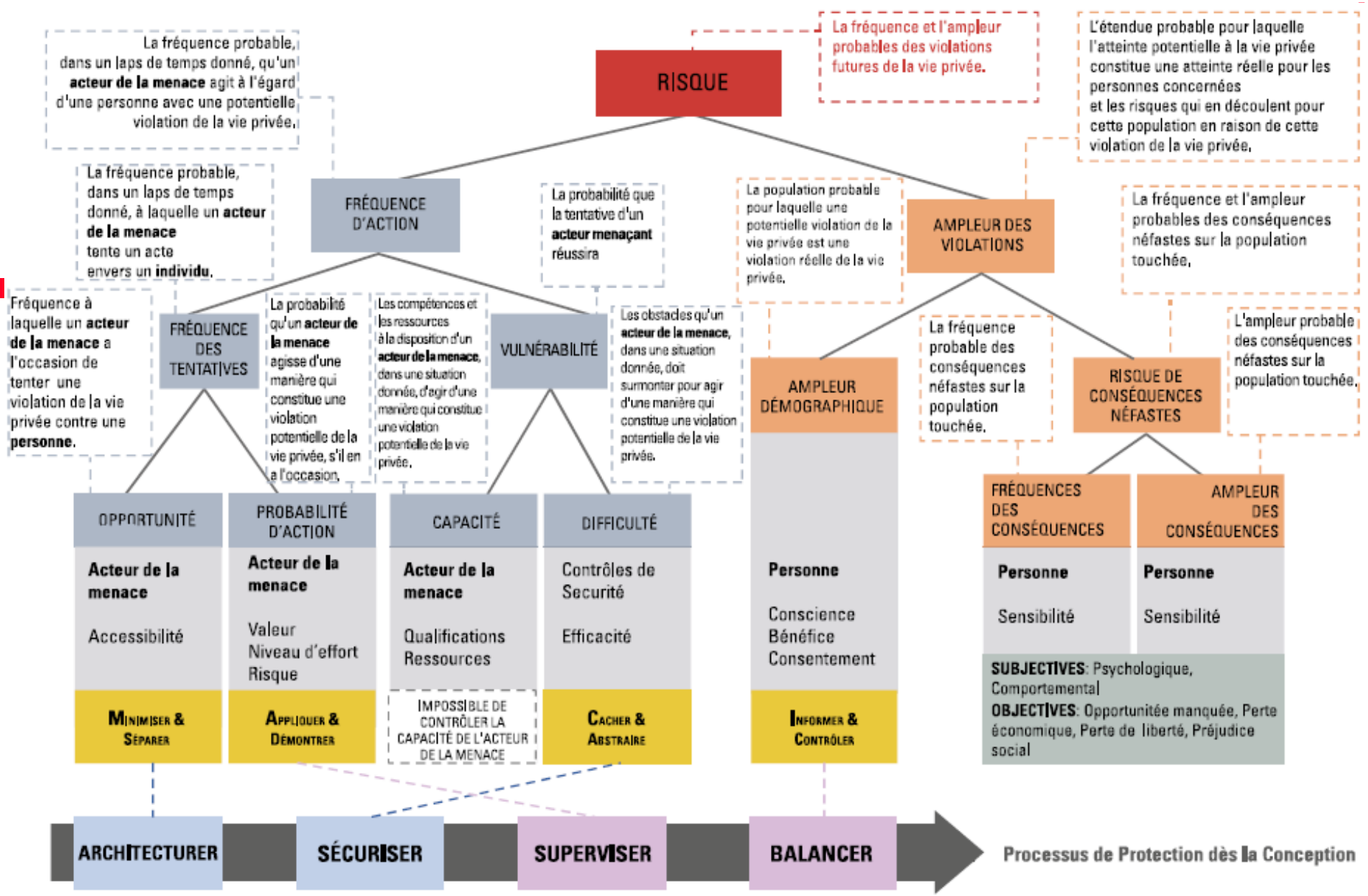
+

Évaluation des Facteurs Relatifs à la Vie Privée

RISQUE POUR LA VIE PRIVÉE

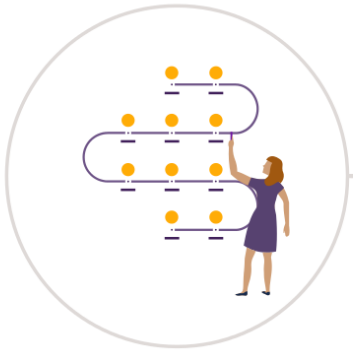
HITACHI

Analyse factorielle du risque lié à l'information



Strategic Privacy by Design IAPP
DPOsolutions inc.

Protection dès la conception & par défaut 7 principes fondamentaux

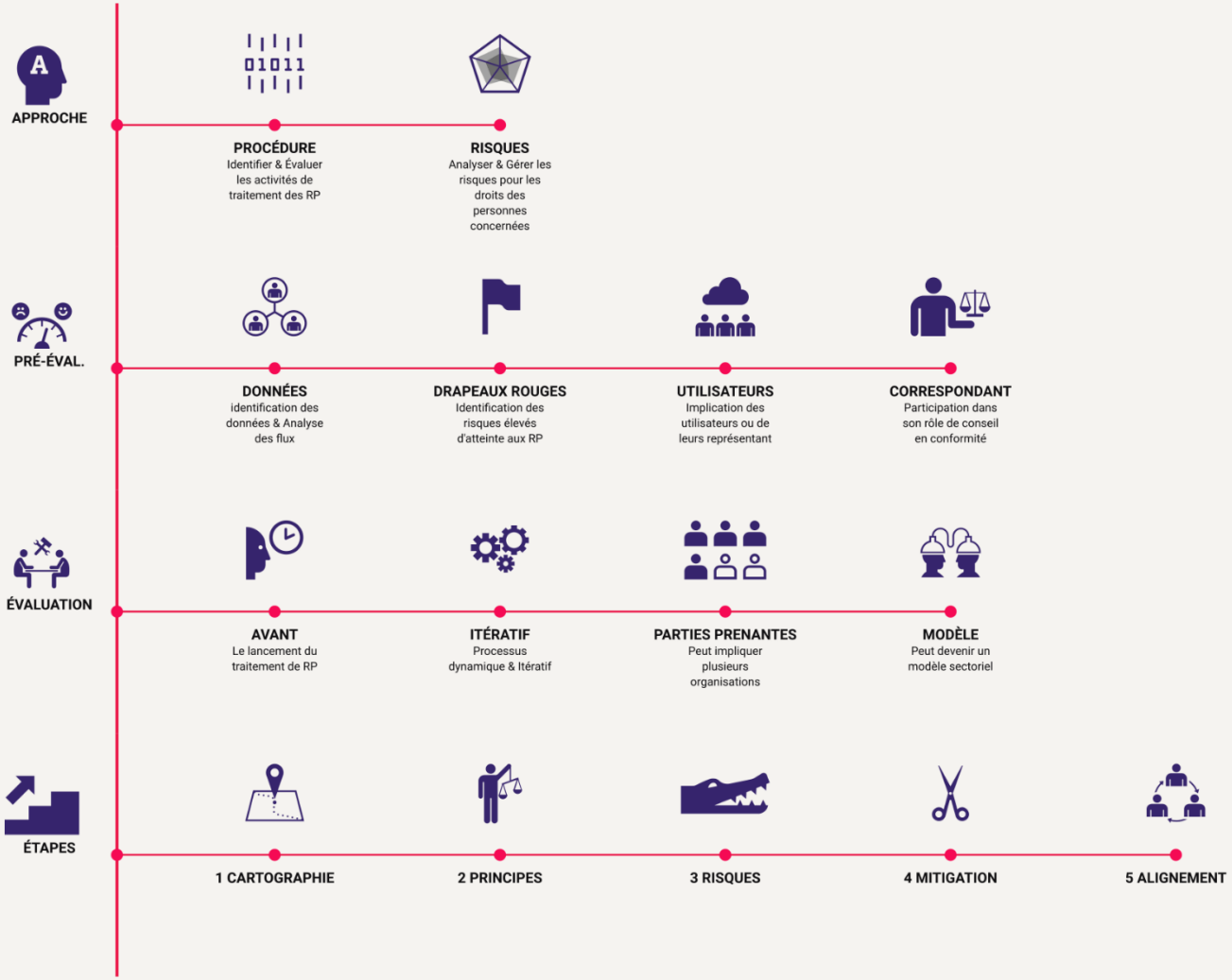


- PROACTIF & PRÉVENTIF
- PAR DÉFAUT
- INTÉGRÉ À LA CONCEPTION
- À SOMME POSITIVE
- SÉCURISÉ DE BOUT EN BOUT
- VISIBILITÉ & TRANSPARENCE
- CENTRÉ UTILISATEUR

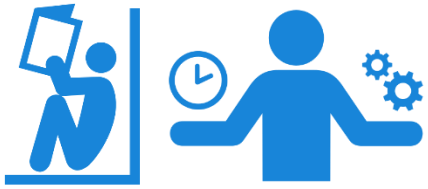
ÉVALUATION DES FACTEURS REALTIFS À LA VIE PRIVÉE

Approche . Méthode , Étapes

Vincent Bureau 2020

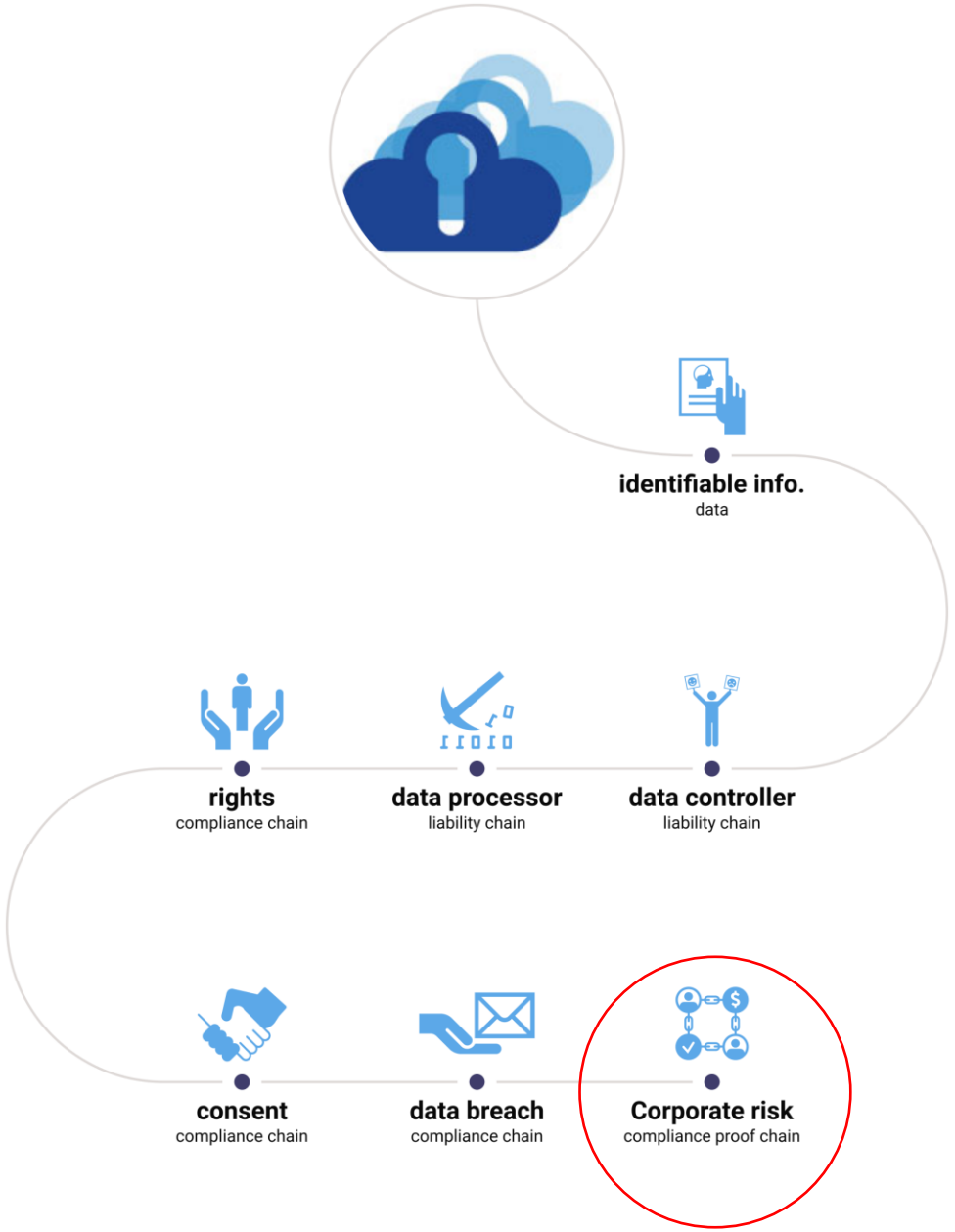


HITACHI
Inspire the Next



Compliance Proof Chain

data protection & liability



PL64: Incident

REGISTRE & DÉCLARATION OBLIGATOIRES

protection des renseignements personnels

- en cas d'atteinte aux mesures de sécurité :
- évaluer les risques, sensibilité & probabilité
- identifier un risque réel de préjudice grave
- déclarer au Commissaire à la vie privée
- aviser les personnes concernées
- aviser des organisations pour atténuer
- tenir un registre de toutes atteintes
- garder les informations 2 ans

Établir votre dossier de conformité

LA DOCUMENTATION DES **TRAITEMENTS** DE DONNÉES

- Le registre des traitements ou des catégories d'activités de traitements.
- EFVP.
- L'encadrement des transferts de données.

L'**INFORMATION** DES PERSONNES

- Les notices d'information.
- Les modèles de recueil du consentement des personnes concernées.
- Les procédures mises en place pour l'exercice des droits.

LES **CONTRATS** QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- Les contrats avec les sous-traitants
- Les procédures internes en cas de violations de données
- Les preuves que les personnes concernées ont donné leur consentement.

ISACA Section de Québec

HITACHI Inspire the Next

Agenda

Introduction
1 Comprendre le projet de loi 64
2 Comparer le projet L64 avec le RGPD
3 Utiliser les ressources ISACA
4 Lancer un programme de mise en conformité
5 Vos questions

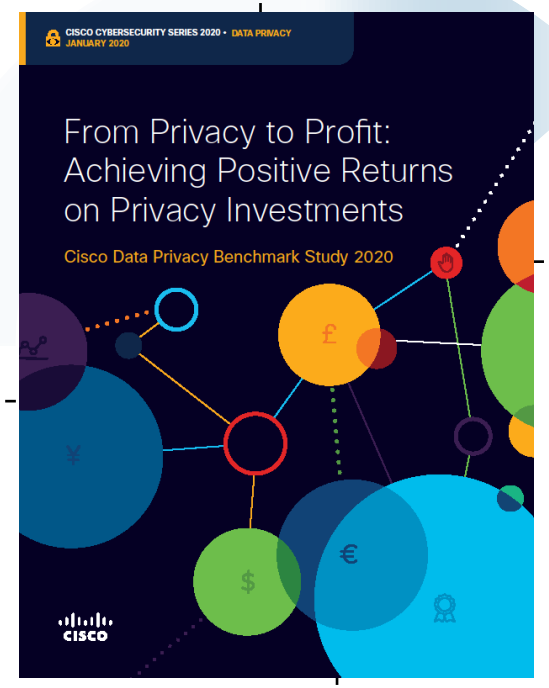
HITACHI
Inspire the Next

Retour sur notre conférence

De la conformité aux bénéfices

Acquisition de nouveaux clients

Mitigation $ Incidents cyber sécurité



Confiance dans la marque

Gestion des riques réglementaires et réputationnels

Cisco Cybersecurity series 2020 Data privacy

PROJET DE LOI 64
Protection des renseignements personnels au Québec

vincent.bureau@hitachi-systems-security.com

ISACA Section de Québec