Secrétariat à la réforme
des institutions
démocratiques
et à l'accès
à l'information

Québec

GUIDE DE RÉFÉRENCES

PROCESSUS D'ÉVALUATION DES RISQUES D'ATTEINTE À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS LIÉS AUX PROJETS D'ACQUISITION, DE DÉVELOPPEMENT ET DE REFONTE D'UN SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES

Direction de l'accès à l'information
et de la protection des renseignements personnels
Secrétariat à la réforme des institutions démocratiques
et à l'accès à l'information

Novembre 2010

Remerciements

Le présent guide de références a été produit par la Direction de l'accès à l'information et de la protection des renseignements personnels du Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information, ci-après appelé SRIDAI.

Le processus d'évaluation des risques d'atteinte à la protection des renseignements personnels liés aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services, qui y est décrit, a été soumis à un essai dans deux organismes publics, soit la Société de l'assurance automobile du Québec et Services Québec.

Le SRIDAI remercie ces organismes et leurs représentants d'avoir accepté de collaborer à la validation du canevas d'analyse de risques.

TABLE DES MATIÈRES

Introduction

Le présent document s'adresse tout particulièrement aux organismes publics visés par le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, ci-après appelé Règlement.

En vertu du Règlement, un organisme public a l'obligation d'informer le comité sur l'accès à l'information et la protection des renseignements personnels[1], ci-après appelé comité, relevant du sous-ministre ou du dirigeant concerné de son intention de réaliser un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, communique, conserve ou détruit de tels renseignements.

Le comité veille à ce que certains de ces projets soient encadrés par des mesures particulières de protection. Pour ce faire, il suggère à l'organisme public de procéder à l'évaluation des risques d'atteinte à la protection de renseignements personnels, et cela, dès l'étude préliminaire d'un projet de ce type.

Cet instrument de travail a été rédigé en vue d'aider les organismes publics à respecter les obligations prévues par le second alinéa de l'article 7 du Règlement[2]. Il permet également aux membres du groupe de travail chargés de l'évaluation des risques d'atteinte à la protection des renseignements personnels d'accomplir plus aisément leur mandat.

> Pour toute question relative au présent guide de références, veuillez joindre la Direction de l'accès à l'information et de la protection des renseignements personnels par téléphone 418 528-8024 ou par courriel (sridai@mce.gouv.qc.ca).

[1] Ce comité se compose du responsable de l'accès aux documents, du responsable de la protection des renseignements personnels et, le cas échéant, du responsable de la sécurité de l'information ainsi que du responsable de la gestion documentaire, et ce, conformément à l'article 2 du Règlement (voir l'annexe 1).
[2] Voir l'annexe 1.

Mise en garde

Un organisme public qui procède à l'évaluation des risques d'atteinte à la protection des renseignements personnels liés à un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services doit examiner, s'il en a l'entière responsabilité, tous les aspects des phases du cycle de vie de ces renseignements. Il est ainsi en mesure d'élaborer des scénarios de risques plausibles et de prévoir les mesures de protection s'y rattachant.

Par ailleurs, les partenaires privés ou publics qui participent à un projet de ce type sont tenus d'évaluer les risques d'atteinte à la protection des renseignements personnels que comporte la portion du projet dont ils sont responsables.

De la sorte, tous les partenaires ont la certitude non seulement que la plupart des scénarios de risques ont été prévus, mais que chacun a pris les mesures appropriées afin d'assurer la protection des renseignements personnels sous sa responsabilité durant la réalisation du projet et lors de l'utilisation, de l'entretien et de l'évolution du système d'information ou de prestation électronique de services.

Bien que l'article 7 du Règlement spécifie le moment où il y a lieu d'évaluer les risques d'atteinte à la protection des renseignements personnels, rien n'empêche un organisme public d'effectuer une évaluation en d'autres temps, s'il le juge à propos.

Mise en oeuvre du processus d'évaluation des risques d'atteinte à la protection des renseignements personnels liés aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services

Dès qu'il le juge opportun, le comité recommande qu'une évaluation des risques liés à un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services soit effectuée. Il en informe le chargé de projet afin qu'il établisse un calendrier de travail[3].

Le processus d'évaluation des risques d'atteinte à la protection des renseignements comporte huit étapes :

- Étape 1 – Description générale des procédés administratifs et technologiques liés aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services
- Étape 2 – Élaboration des scénarios de risques d'atteinte à la protection des renseignements personnels
- Étape 3 – Validation des scénarios de risques d'atteinte à la protection des renseignements personnels
- Étape 4 – Évaluation de la probabilité de réalisation des scénarios de risques d'atteinte à la protection des renseignements personnels
- Étape 5 – Identification des scénarios de risques d'atteinte à la protection des renseignements personnels nécessitant l'application de mesures de protection
- Étape 6 – Détermination des mesures de protection et élaboration d'un plan d'action concernant leur application
- Étape 7 – Présentation du rapport d'évaluation des risques d'atteinte à la protection des renseignements personnels et approbation du plan d'action concernant l'application des mesures de protection appropriées
- Étape 8 – Application des mesures de protection conformément au plan d'action approuvé en la matière

Chaque étape du processus d'évaluation fait l'objet d'une section du présent document.

Le chargé de projet peut faire appel à des experts pour élaborer et mettre en œuvre le processus d'évaluation des risques d'atteinte à la protection des renseignements personnels.

[3] Voir l'annexe 2.

Étape 1 – Description générale des procédés administratifs et technologiques liés aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services

À la première étape, le chargé de projet ou les experts qu'il désigne ont pour tâche de décrire les procédés administratifs et technologiques liés à chacune des phases du cycle de vie des renseignements personnels (collecte, accès au système, utilisation, communication, conservation, sécurité et destruction, accès et rectification par la personne concernée) à consigner dans le système d'information ou de prestation électronique de services.

Pour y arriver, ils doivent tenir compte de tous les éléments associés à ces phases et des obligations que la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ci-après appelée Loi sur l'accès, confère aux organismes publics à cet égard.

- Collecte (art. 64 et 65)
  - Auprès de qui les renseignements seront-ils colligés?
  - Lesquels colligera-t-on? Seront-ils tous nécessaires?
  - Comment et où seront-ils colligés?
  - Auront-ils déjà été colligés par une personne ou un organisme? Si oui, la Commission d'accès à l'information en sera-t-elle informée?

- Accès au système (art. 62)
  - Qui pourra accéder au système?
  - Comment y accédera-t-on (voies ou modes d'accès)?
  - Quel sera le mode d'identification et d'authentification requis?
  - Quelles mesures de protection appliquera-t-on?

- Utilisation (art. 65 et 65.1)
  - À quelles fins serviront les renseignements personnels colligés?
  - Aura-t-on obtenu au préalable le consentement de la personne concernée?

- Communication (art. 59)
  - Quels renseignements personnels communiquera-t-on?
  - Comment et pourquoi seront-ils communiqués?

- Conservation, sécurité et destruction (art. 63.1, 72 et 73)
  - Quels renseignements personnels conservera-t-on?
  - Seront-ils à jour, exacts et complets?
  - Comment seront-ils classés?
  - Une journalisation (en lecture, en modification ou autre) sera-t-elle faite?
  - Que contiendra le journal?
  - Comment et quand un renseignement personnel sera-t-il détruit?

- Accès et rectification par la personne concernée (art. 83 et suivants)
  - La personne concernée pourra-t-elle accéder à son dossier ou rectifier un renseignement personnel?

Étape 2 – Élaboration des scénarios de risques d'atteinte à la protection des renseignements personnels

À la deuxième étape, donc une fois décrits les procédés administratifs et technologiques liés au projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services, le chargé de projet ou les experts qu'il désigne élaborent différents scénarios de risques d'atteinte à la protection des renseignements personnels.

Exemple d'un scénario de risques

Risque lié à l'objectif concernant la confidentialité des renseignements personnels

SCÉNARIO

CAUSE	RISQUE	IMPACT
Accès non autorisé à un renseignement personnel	Mauvais usage du renseignement ainsi obtenu	Atteinte à la réputation de la personne concernée

Il est recommandé de se servir du tableau de synthèse qui suit pour élaborer des scénarios de risques au regard de chacune des phases du cycle de vie des renseignements personnels.

Tableau de synthèse – Scénarios de risques d'atteinte à la protection des renseignements personnels				
← **Numéro du scénario**				
↓	**Causes**	**Risques**	**Articles de la Loi sur l'accès**	**Impacts sur les personnes, les MO ou les partenaires**
Collecte				
1				
Accès au système				
…				
Utilisation				
…				
Communication				
…				
Conservation, sécurité et destruction				
…				
Accès et rectification par la personne concernée				
…				

Il est proposé de numéroter chaque scénario de risques afin de le repérer plus aisément dans la grille de repérage présentée à la cinquième étape.

À titre d'exemple, voici un tableau de synthèse dûment complété.

Tableau de synthèse – Scénarios de risques d'atteinte à la protection des renseignements personnels (exemple)				
← **Numéro du scénario**				
↓	**Causes**	**Risques**	**Articles de la Loi sur l'accès**	**Impacts sur les personnes, les MO ou les partenaires**
Collecte				
1	Inscription : renseignements personnels colligés en trop, donc non requis	Non-nécessité	64	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
2	Journalisation et historique : renseignements personnels colligés en trop, donc non requis	Non-nécessité	64	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
3	Information non fournie à la personne concernée	Absence de consentement ou invalidité de celui-ci	65	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
Accès au système				
4	Accès d'une personne à des renseignements personnels ne la concernant pas	Usurpation d'identité	62 et 63.1	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
5	Accès du personnel de soutien à des renseignements personnels sans avoir obtenu le consentement de la personne en cause, alors qu'ils ne sont pas nécessaires à l'exercice de ses fonctions	Bris de confidentialité	62	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
6	Accès du personnel technique à privilège élevé à des renseignements personnels en dehors de l'exercice de ses fonctions	Bris de confidentialité	62	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
7	Accès du personnel de soutien ou technique à plus de renseignements personnels que ceux qui sont nécessaires à l'exercice de ses fonctions	Bris de confidentialité	62	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
Utilisation				
8	Utilisation par l'organisme public de renseignements personnels sans avoir obtenu le consentement de la personne en cause, et ce, à des fins autres que celles pour lesquelles ils ont été recueillis	Non-respect de la Loi sur l'accès	65.1	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
Communication				
9	Communication de renseignements personnels par l'organisme public à une tierce personne sans avoir obtenu le consentement de la personne en cause	Divulgation de renseignements personnels	59 et 63.1	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
Conservation, sécurité et destruction				
10	Non-destruction de renseignements personnels une fois utilisés aux fins requises	Conservation illicite	73	Préjudice porté à l'image de l'organisme public ou à celle du gouvernement
11	Accès d'une tierce personne à des renseignements personnels ne la concernant pas, et cela, en raison d'une erreur d'identification	Bris de confidentialité	63.1	Préjudice porté à la personne, à l'image de l'organisme public ou à celle du gouvernement
Accès et rectification par la personne concernée				
	Aucun scénario envisagé			

Étape 3 – Validation des scénarios de risques d'atteinte à la protection des renseignements personnels

À la troisième étape, le chargé de projet s'assure que des membres du personnel de l'organisme public feront partie du groupe de travail chargé de valider les scénarios de risques. Ces personnes ou leur représentant sont notamment le responsable de l'accès aux documents, le responsable de la protection des renseignements personnels, le responsable de la sécurité des renseignements personnels et le responsable de la gestion documentaire.

Quelques jours avant la tenue du premier atelier, le chargé de projet transmet à chacun des membres du groupe de travail une note de service l'informant qu'il a été désigné pour participer à l'évaluation des risques d'atteinte à la protection des renseignements personnels liés au projet visé et qu'en conséquence il doit prendre connaissance des documents suivants : la description des procédés administratifs et technologiques et le tableau de synthèse des scénarios de risques.

Le chargé de projet agit lui-même comme animateur de l'atelier ou désigne un membre du groupe pour jouer ce rôle.

Les questions à l'ordre du jour se résument ainsi :

- Explication du processus d'évaluation des risques en huit étapes
- Détermination de la portée du projet faisant l'objet du processus d'évaluation des risques et obtention d'un consensus
- Description générale des procédés administratifs et technologiques liés aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services
- Présentation de chacun des scénarios de risques envisagés
- Validation de chacun des scénarios de risques envisagés
- Vérification de l'existence possible d'autres scénarios de risques et, le cas échéant, validation de ces derniers

Afin d'en arriver à un consensus, chaque participant peut faire des commentaires, demander des précisions ou proposer des modifications ou des reformulations. Ainsi, tous ont la même compréhension des scénarios de risques envisagés et la possibilité de s'impliquer dans la réalisation du projet.

Étape 4 – Évaluation de la probabilité de réalisation des scénarios de risques d'atteinte à la protection des renseignements personnels

Une fois le tableau de synthèse des scénarios de risques validé, l'animateur demande d'abord aux membres du groupe de travail d'évaluer, immédiatement ou ultérieurement, la probabilité que ces scénarios se réalisent. Pour leur faciliter la tâche, il leur fournit la définition des termes[4] en usage.

> *Probabilité de réalisation d'un scénario de risques*
> Degré de prévisibilité qu'un scénario de risques se réalise, compte tenu de tous les facteurs pertinents
>
> *Impact*
> Effet d'un scénario si le risque anticipé survient, compte tenu de la valeur attribuée aux opérations d'affaires en cause et de tous les autres facteurs pertinents

Ensuite, l'animateur passe en revue les valeurs attribuées à un scénario de risques selon la probabilité qu'il se réalise.

Valeurs attribuées à un scénario de risques d'atteinte à la protection des renseignements personnels selon sa probabilité de réalisation	
Très improbable (TI)	Le scénario a peu de chances de se réaliser, mais il existe une infime probabilité que ce soit le cas.
Improbable (I)	Le scénario ne se réalisera pas si l'organisme public se fie aux expériences passées. N'étant néanmoins pas invraisemblable, sa réalisation demeure possible.
Probable (P)	Le scénario pourrait se réaliser à plus ou moins court terme. Entretenir l'espoir qu'il en aille autrement n'est pas insensé, mais dénote un certain optimisme. Par conséquent, s'il se réalisait, l'organisme public serait déçu, mais non surpris.
Très probable (TP)	Le scénario se réalisera à court terme. L'organisme public n'est donc pas surpris quand c'est le cas.

[4] Les définitions des valeurs sont extraites ou inspirées du *Guide d'utilisation de la méthode MÉHARI* et de l'outil RISICARE.

Valeurs attribuées aux impacts associés à l'atteinte à la protection des renseignements personnels	
Bas (B) – Impacts non significatifs	Impacts plutôt négligeables, limités à un secteur administratif. Ne portent préjudice ni à la clientèle, ni aux partenaires, ni à l'image de l'organisme public ou à celle du gouvernement.
Moyen (M) – Impacts limités	Impacts notables, limités à un secteur administratif. Peuvent causer des désagréments tolérables à la clientèle ou aux partenaires ou nuire à l'image de l'organisme public de façon marquée, mais pour une courte durée.
Élevé (É) – Impacts graves	Impacts notables sur l'organisme public, la clientèle ou les partenaires. Ne menacent toutefois pas la survie ou l'intégrité de celui-ci dans son ensemble ni la santé et la sécurité physique des personnes. Peuvent causer des dommages à la clientèle et aux partenaires ou nuire considérablement à l'image de l'organisme public.
Très élevé (TÉ) – impacts extrêmement graves	Impacts très graves menaçant la survie ou l'intégrité de l'organisme public dans son ensemble ou touchant la clientèle et les partenaires. Peuvent non seulement paralyser le fonctionnement et les opérations critiques de l'organisme public de manière presque irrémédiable mais aussi nuire considérablement à l'économie du Québec, entraver sérieusement la sécurité publique ou compromettre la santé ou la sécurité physique des personnes, voire mener à une crise financière sans précédent.

L'évaluation de la probabilité de réalisation d'un scénario de risques doit être faite, d'une part, sans tenir compte d'aucune mesure de protection et, d'autre part, en les prenant toutes en considération.

Il importe de noter que cette évaluation doit s'effectuer en deux temps en vue :

- de déterminer si des mesures de protection sont requises;
- de voir si les mesures de protection réduisent le risque résiduel;
- d'apprécier davantage les mesures de protection existantes ou à venir;
- de savoir si toutes les mesures de protection envisagées sont suffisantes.

Voici des exemples des champs d'application des mesures de protection :

- Gestion accrue de l'authentification
- Journalisation et analyse
- Enquête sur le personnel
- Rehaussement des niveaux de sécurité
- Renforcement des procédés administratifs
- Réglementation plus rigoureuse en matière d'organisation du travail

Lorsque toutes les informations nécessaires pour faire l'évaluation des scénarios de risques sont disponibles, les membres du groupe de travail peuvent revoir avec l'animateur les scénarios retenus à la troisième étape, juger de la probabilité qu'ils se réalisent et prendre en considération la valeur attribuée aux impacts, compte tenu ou non des mesures de protection. Après consensus, les valeurs obtenues sont inscrites dans le tableau de données suivant :

Tableau de données relatives aux scénarios de risques d'atteinte à la protection des renseignements personnels selon leur probabilité de réalisation

← Numéro du scénario						
	Causes	**Évaluation (sans mesures de protection)**		**Mesures de protection existantes (e) ou à venir (v)**	**Évaluation (avec mesures de protection)**	
		Impacts	**Probabilité de réalisation**		**Impacts**	**Probabilité de réalisation**
Collecte						
1						
Accès au système						
…						
Utilisation						
…						
Communication						
…						
Conservation, sécurité et destruction						
…						
Accès et rectification par la personne concernée						
…						

Un tableau de données complété est fourni ci-après à titre d'exemple. Dans ce tableau, toutes les mesures de protection sont déjà existantes.

Tableau de données relatives aux scénarios de risques d'atteinte à la protection des renseignements personnels selon leur probabilité de réalisation						
← **Numéro du scénario**						
	Causes	**Évaluation (sans mesures de protection)**		**Mesures de protection existantes (e) ou à venir (v)**	**Évaluation (avec mesures de protection)**	
		Impacts	**Probabilité de réalisation**		**Impacts**	**Probabilité de réalisation**
Collecte						
1	Inscription : renseignements personnels colligés en trop, donc non requis	É	TP	Champs de saisie disponibles (e) Transferts automatisés (e)	M	TI
2	Journalisation et historique : renseignements personnels colligés en trop, donc non requis	É	TP	Champs de saisie disponibles (e) Transferts automatisés (e)	M	TI
3	Information non fournie à la personne concernée	É	P	Informations à intégrer aux conditions d'utilisation (e)	M	TI
Accès au système						
4	Accès d'une personne à des renseignements personnels ne la concernant pas	TÉ	TP	Mesures prises par X pour gérer l'authentification (e) Conditions d'utilisation (e)	M	P
5	Accès du personnel de soutien à des renseignements personnels sans avoir obtenu le consentement de la personne en cause, alors qu'ils ne sont pas nécessaires à l'exercice de ses fonctions	B	TP	Mesures prises par X pour vérifier l'identité de l'appelant (e)	B	P
6	Accès du personnel technique à privilège élevé à des renseignements personnels en dehors de l'exercice de ses fonctions	M	P	Journalisation et analyse (e) Enquête sur le personnel (e)	M	TI
7	Accès du personnel de soutien ou technique à plus de renseignements personnels que ceux qui sont nécessaires à l'exercice de ses fonctions	TÉ	TP	Journalisation et analyse (e)	TÉ	P
Utilisation						
8	Utilisation par l'organisme public de renseignements personnels sans avoir obtenu le consentement de la personne en cause, et ce, à des fins autres que celles pour lesquelles ils ont été recueillis	TÉ	TP	Processus administratifs (e) Organisation du travail (e)	TÉ	P
Communication						
9	Communication de renseignements personnels par l'organisme public à une tierce personne sans avoir obtenu le consentement de la personne en cause	É	P	Processus administratifs (e) Organisation du travail (e)	É	TI

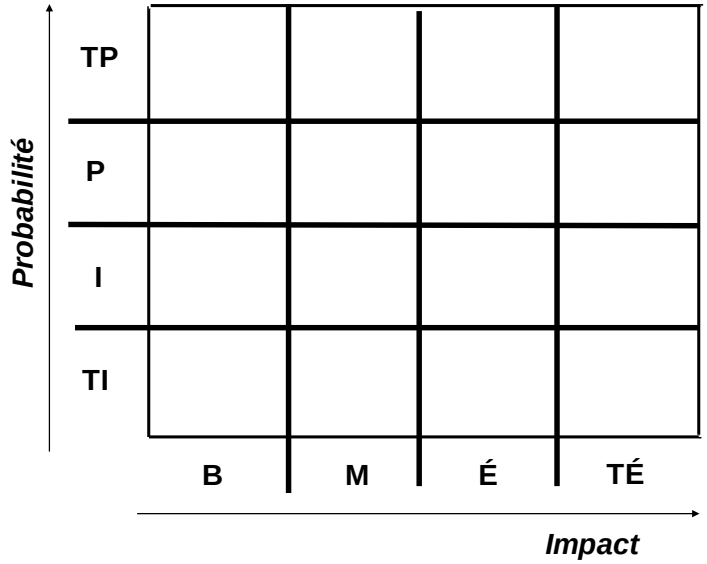
Conservation, sécurité et destruction						
10	Non-destruction de renseignements personnels une fois utilisés aux fins requises	B	I	Calendrier de conservation (e) Mesures de destruction (e)	B	TI
11	Accès d'une tierce personne à des renseignements personnels ne la concernant pas, et cela, en raison d'une erreur d'identification	É	P	Amélioration du processus (e) Rehaussement des niveaux de sécurité (e)	É	I
Accès et rectification par la personne concernée						
	Aucun scénario envisagé					

Cette étape se termine dès que le tableau de données relatives aux scénarios de risques d'atteinte à la protection des renseignements personnels selon leur probabilité de réalisation est complété.

Étape 5 – Identification des risques d'atteinte à la protection des renseignements personnels nécessitant l'application de mesures de protection

La cinquième étape consiste à transposer les risques d'atteinte à la protection des renseignements personnels dans la grille de repérage dont le modèle est présenté ci-après.

Grille de repérage des risques anticipés d'atteinte à la protection des renseignements personnels



La classification qui suit permet de constater si les risques anticipés d'atteinte à la protection des renseignements personnels sont au-delà ou en deçà du seuil de tolérance[5] de l'organisme public, c'est-à-dire de sa capacité représente le niveau de confort d'une organisation à y faire face le cas échéant.

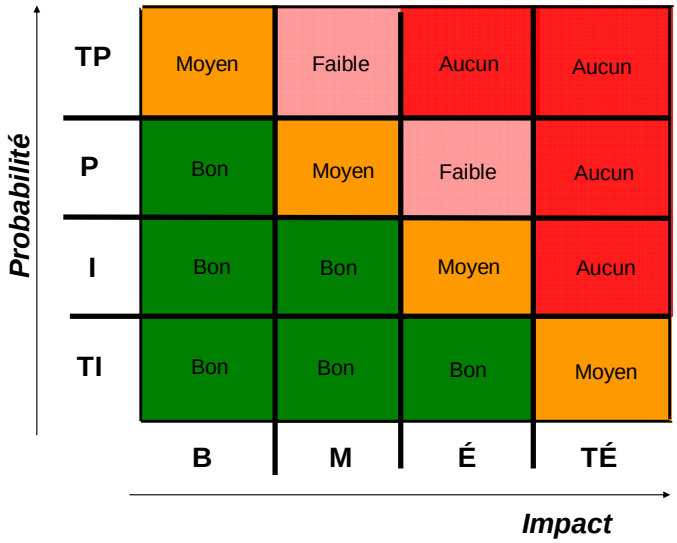
Classification des seuils de tolérance aux risques d'atteinte à la protection des renseignements personnels

Bon	Risques généralement acceptés sans appliquer aucune mesure de protection supplémentaire
Moyen	Risques à surveiller, donc en envisageant l'application de mesures de protection supplémentaires, mais à faible coût
Faible	Risques nécessitant une intervention dans les meilleurs délais et pouvant entraîner des investissements considérables
Aucun	Risques inacceptables nécessitant l'application immédiate des mesures de protection

[5] Voir la note précédente.

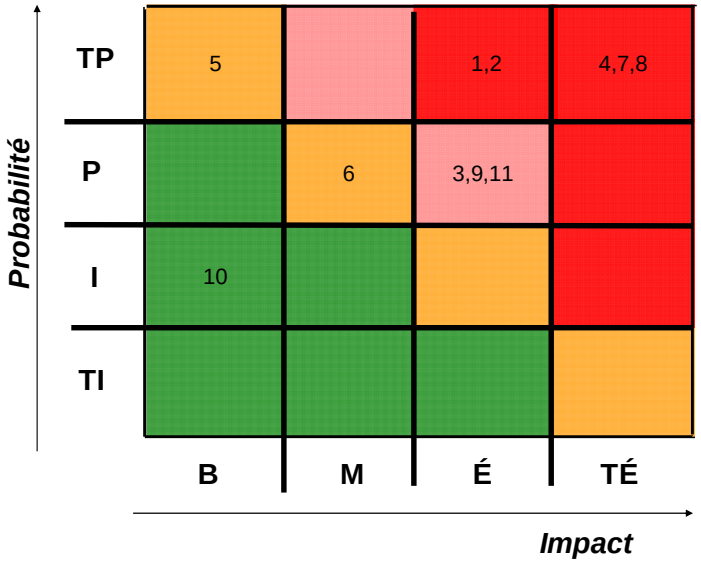
Voici, la grille avec les seuils de tolérance généralement établis.

Grille de repérage des risques anticipés d'atteinte à la protection des renseignements personnels selon les seuils de tolérance établis



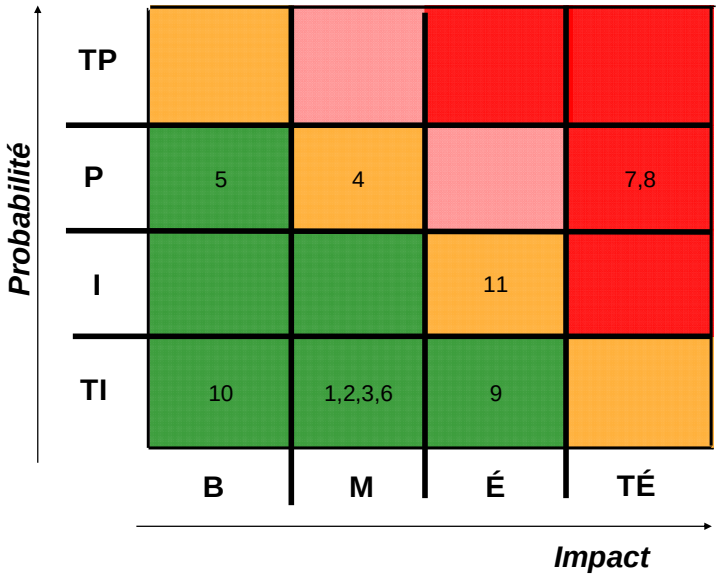
Dans un premier temps, l'animateur ou la personne qu'il désigne transpose les risques anticipés dans la grille de repérage en ne tenant compte d'aucune mesure de protection. Les numéros inscrits dans l'exemple fourni ci-dessous renvoient aux scénarios décrits dans le tableau de données dressé précédemment.

Grille de repérage des risques d'atteinte à la protection des renseignements personnels selon les seuils de tolérance établis *(sans mesures de protection)*



Dans un deuxième temps, l'animateur ou la personne qu'il désigne transpose les risques anticipés dans la grille de repérage en tenant compte des mesures de protection existantes ou à venir. Les numéros inscrits dans l'exemple fourni ci-dessous renvoient aux scénarios de risques retenus dans le tableau de données dressé précédemment.

Grille de repérage des risques anticipés d'atteinte à la protection des renseignements personnels selon les seuils de tolérance établis (avec mesures de protection)



La comparaison des deux grilles aide l'organisme public :

- à mieux analyser les mesures de protection existantes ou à venir;
- à savoir si une mesure de protection envisagée est trop ferme ou, au contraire, si elle doit être renforcée;
- à faire la gestion des risques en modifiant les mesures de protection à la hausse ou à la baisse;
- à déterminer s'il peut faire face aux risques anticipés ou s'il doit plutôt prévoir des mesures de protection supplémentaires à cette fin.

Ainsi, l'exemple fourni précédemment permet de conclure que toutes les mesures ont une certaine efficacité, puisque tous les scénarios de risques sans exception se trouvent en meilleure situation.

Toutefois, il importe de noter que d'autres mesures de protection devraient être proposées en ce qui concerne les scénarios 4, 7, 8 et 11 puisqu'ils sont au-delà du seuil de tolérance.

Par ailleurs, si certains de ces scénarios avaient des mesures de protection « à venir », ceux-ci devraient également être pris en compte dans le plan d'action.

Étape 6 – Détermination des mesures de protection et élaboration d'un plan d'action concernant leur application

À la sixième étape, le chargé de projet détermine, seul ou en collaboration avec les membres du groupe de travail, les mesures de protection associées aux scénarios de risques anticipés et élabore un plan d'action en vue de les mettre en application, le cas échéant. S'il effectue ce travail lui-même, il doit présenter à ces personnes le plan d'action qu'il a élaboré.

Étape 7 – Présentation du rapport d'évaluation des risques et approbation du plan d'action concernant les mesures de protection appropriées

À la septième étape, le chargé de projet prépare, à l'intention du comité, les documents dans lesquels sont décrits la démarche retenue aux fins d'évaluation des scénarios de risques d'atteinte à la protection des renseignements personnels, les résultats de cet exercice ainsi que le plan d'action proposé.

Dans sa présentation, le chargé de projet doit préciser, entre autres :

- les raisons justifiant la démarche d'évaluation de risques d'atteinte à la protection des renseignements personnels;
- la liste et les fonctions des participants;
- les mesures de protection à appliquer;
- les impacts sur l'organisme public s'il ne tient pas compte des mesures de protection ou bien s'il ne les applique pas;
- les risques résiduels que l'organisme public peut assumer ou auxquels il peut faire face;
- les mesures de protection recommandées dans le plan d'action.

Le chargé de projet entend ainsi obtenir l'approbation du comité en ce qui a trait au plan d'action élaboré aux fins requises.

Étape 8 – Application des mesures de protection conformément au plan d'action approuvé en la matière

Une fois le plan d'action approuvé, le sous-ministre ou le dirigeant s'assure qu'il sera appliqué au besoin, conformément à l'article 63.1 de la Loi sur l'accès :

> 63.1. Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Si l'évaluation des scénarios de risques n'exige pas l'application de mesures de protection supplémentaires, le sous-ministre ou le dirigeant doit quand même prévoir la tenue d'une séance de sensibilisation, comme le prescrit l'article 2 du Règlement, pour l'ensemble du personnel qui veillera au bon fonctionnement du nouveau système d'information ou de prestation électronique de services.

Enfin, l'organisme public doit réévaluer les scénarios de risques après l'application des mesures de protection ou lorsque des modifications sont apportées au projet en vue d'apprécier leur efficacité selon le seuil de tolérance établi.

ANNEXE 1

Extraits de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et du Règlement sur la diffusion de l'information et de la protection des renseignements personnels

L'article 3 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels prescrit ce qui suit :

> *3. Sont des organismes publics : le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires et les établissements de santé ou de services sociaux.*
>
> *Sont assimilés à des organismes publics, aux fins de la présente loi : le lieutenant-gouverneur, l'Assemblée nationale, un organisme dont celle-ci nomme les membres et une personne qu'elle désigne pour exercer une fonction en relevant, avec le personnel qu'elle dirige.*
>
> *Les organismes publics ne comprennent pas les tribunaux au sens de la Loi sur les tribunaux judiciaires (chapitre T-16).*

Les articles 2 et 7 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels prescrivent ce qui suit :

> *2. Le sous-ministre ou le dirigeant d'un organisme public doit :*
>
> *1° s'assurer de la mise en œuvre des responsabilités et des obligations attribuées par le présent règlement à l'organisme public qu'il dirige;*
>
> *2° mettre sur pied un comité sur l'accès à l'information et la protection des renseignements personnels qui relève de lui; ce comité se compose du responsable de l'accès aux documents et de la protection des renseignements personnels et, le cas échéant, du responsable de la sécurité de l'information et du responsable de la gestion documentaire; il est chargé de soutenir le sous-ministre ou le dirigeant de l'organisme public dans l'exercice de ses responsabilités et obligations et, à cette fin, il peut s'adjoindre toute autre personne dont l'expertise est requise pour exercer sa fonction;*
>
> *3° veiller à la sensibilisation et à la formation des membres du personnel et des membres du personnel de direction ou d'encadrement de l'organisme public sur les obligations et les pratiques en matière d'accès à l'information et de protection des renseignements personnels;*
>
> *4° (vig. 10-11-29) insérer dans le rapport annuel de gestion ou d'activités un bilan qui atteste la diffusion des documents visés à la section III et qui rend compte:*
>
> *a) de la nature et du nombre de demandes d'accès reçues, du délai pris pour les traiter, des dispositions de la Loi justifiant que certaines d'entre elles ont été refusées, du nombre de demandes d'accès acceptées, partiellement acceptées ou refusées, du nombre de*

demandes d'accès ayant fait l'objet de mesures d'accommodement raisonnables et du nombre de demandes ayant fait l'objet d'une demande de révision à la Commission d'accès à l'information;

b) des activités relatives à l'accès à l'information et à la protection des renseignements personnels réalisées au sein de l'organisme public.

7. Un organisme public doit informer le comité visé à l'article 2 des projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels.

Le comité suggère, parmi ces projets, ceux qui doivent être encadrés par des mesures particulières de protection des renseignements personnels.

Ces mesures comprennent :

1° la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels pour chaque projet;

2° l'évaluation, dès l'étude préliminaire du projet, des risques d'atteinte à la protection des renseignements personnels;

3° des mesures propres à assurer la protection des renseignements personnels pendant toute la période de réalisation du projet et son maintien lors de l'utilisation, de l'entretien, de la modification et de l'évolution du système d'information ou de prestation électronique des services visés;

4° la description des exigences de protection des renseignements personnels dans le cahier de charges ou le contrat relatif au projet, à moins que l'exécutant du contrat soit un autre organisme public;

5° la description des responsabilités des participants au projet en matière de protection des renseignements personnels;

6° la tenue d'activités de formation sur la protection des renseignements personnels à l'intention des participants au projet.

ANNEXE 2

Exemple de la mise en œuvre du mécanisme d'évaluation des risques d'atteinte à la protection des renseignements personnels liés aux projets d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services

ACTIVITÉS	TEMPS ESTIMÉ EN J/P	PERSONNES RESPONSABLES				DATE DE DÉBUT	DATE DE FIN
		Chargé de projet	(groupe de travail)	Comité	Sous-ministre ou dirigeant		
Désigner les membres participants du groupe de travail		S		As			
Décrire les procédés administratifs et technologiques		R/F	R/P				
Élaborer les scénarios de risques d'atteinte à la protection des renseignements personnels		R/F	R				
Valider les scénarios de risques d'atteinte à la protection des renseignements personnels par la tenue d'un atelier;		An	R				
Évaluer la probabilité de réalisation des scénarios de risques d'atteinte à la protection des renseignements personnels		An	R				
Identifier les scénarios de risques nécessitant l'application de mesures de protection		R					
Déterminer les mesures de protection et élaborer le plan d'action concernant leur application		R/P	R/P				
Présenter le rapport d'évaluation des risques d'atteinte à la protection des renseignements personnels et obtenir l'approbation du plan d'action concernant les mesures de protection appropriées		R		Ap			
Mettre en application le plan d'action approuvé en la matière		R		F	S		

Légende
An = Anime
Ap = Approuve
As = Assigne avec autorisation des responsables des unités administratives concernées
F = Fait le suivi
P = Participe
R = Réalise
S = S'assure