Pratique recommandée en sécurité de l'information

PR-057 Version 2.1

Guide de catégorisation de l'information

ENSEMBLE on fait avancer le Québec

Québec

Guide de catégorisation de l’information

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – juillet 2016
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71120-9 (en ligne)

Table des matières

Table des figures

Sigles et Acronymes

Acronymes

DIC : disponibilité, intégrité, confidentialité

ROSI : responsable organisationnel de la sécurité de l'information

Sigles

RADPRP : responsable de l'accès aux documents et de la protection des renseignements personnels

Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel pour leur participation et le travail accompli.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Roza Lami, chargée de projet
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Daniel Landry
Sûreté du Québec

Jacques Blouin
Régie de l'assurance-maladie du Québec

Catherine Thibault
Ministère du Conseil exécutif

Javier Betancour
Contrôleur des finances

Dany Michaud
Commission de protection du territoire agricole du Québec

Denyse Roussel
Ministère du Conseil exécutif

Claude Côté
Commission des transports du Québec

Marthe-Anaïs Kambou
Ministère de la Santé et des Services sociaux

Daniel Guimont
Commission des lésions professionnelles

Pierre Bonhomme
Ministère de l'Éducation, du Loisir et du Sport

Mario Trudel
Société de l'assurance automobile du Québec

Notes à l'intention du lecteur

Note 1 :	Cette version 2.1 du guide ne présente que des modifications mineures par rapport à la version diffusée en 2014, lesquelles ne portent aucunement sur le processus de catégorisation.
Note 2 :	Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document.
Note 2 :	Le terme « organisme public » ou « organisme » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].
Note 3 :	Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.
Note 4 :	Certains termes ou acronymes sont définis à leur première apparition dans le texte. Ces définitions sont également présentées à l'annexe A – Acronymes, sigles et définitions.

1. Introduction

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie[1]. Cependant, les éléments d'information qu'une organisation détient n'ont pas tous la même valeur et ne nécessitent pas tous le même niveau de protection.

La catégorisation des actifs informationnels[2] en sécurité de l'information est un processus permettant à l'organisme d'évaluer le degré de sensibilité de son information, dans le but d'en déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité (DIC). Un organisme pourra ainsi tenir compte du degré de sensibilité déterminé pour mettre en place les mesures lui permettant de se conformer à ses obligations légales, d'éviter des pertes financières, d'atteindre ses objectifs en ce qui a trait à son niveau de services et de rehausser la confiance des citoyens et des entreprises à l'égard des services publics.

Le présent guide vise à fournir aux organismes publics une démarche de catégorisation leur permettant d'évaluer le niveau de criticité de leurs actifs informationnels en matière de DIC. Cette démarche est appuyée par :

- ✓ un outil, sous forme de chiffrier Excel, regroupant l'ensemble des formulaires proposés;
- ✓ un exemple d'application de la démarche de catégorisation pour un cas fictif, décrit à l'Annexe XII et dont l'intégralité des résultats est présentée dans un chiffrier Excel.

1.1 Mise en contexte

Le présent guide a été élaboré en remplacement d'une version antérieure intitulée « Guide relatif à la catégorisation des documents technologiques en matière de sécurité - Juillet 2003 », qui se limitait à la catégorisation de l'information numérique. Le présent guide tient compte des principaux éléments de contexte suivants :

- ✓ la portée de la Directive sur la sécurité de l'information gouvernementale, actuellement en vigueur[3], laquelle s'applique à l'information, quels que soient son support (numérique ou non numérique) ou son mode d'expression;
- ✓ le champ d'application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement[4], lequel

1. Cycle de vie de l'information : l'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme public. [Source : Directive sur la sécurité de l'information gouvernementale, 2014]
2. Actif informationnel : tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1). À titre de rappel, cette loi définit le document comme étant :
   « Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.
   [...] est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »
3. Directive adoptée le 15 janvier 2014.
4. Loi adoptée le 13 juin 2011.

inclut les ministères et les organismes, budgétaires et autres que budgétaires, ainsi que les organisations du réseau de l'éducation et du réseau de la santé et des services sociaux;

- ✓ l'évolution des normes et des méthodes de gestion de risques en sécurité de l'information, nécessitant de nouvelles approches de catégorisation des actifs informationnels.

1.2 Portée

Le présent guide s'applique à l'information qu'un organisme détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers. Cette information peut être consignée sur tout type de support, qu'il soit papier, électronique ou autre.

Il ne couvre pas le choix des mesures de sécurité à mettre en œuvre, étape relevant du processus de gestion des risques.

1.3 Public cible

Le présent guide s'adresse principalement aux :

- ✓ responsables organisationnels de la sécurité de l'information;
- ✓ détenteurs de l'information ou leurs mandataires désignés;
- ✓ conseillers en gestion de la sécurité de l'information;
- ✓ autres intervenants dans des domaines connexes (responsable de l'accès aux documents et de la protection des renseignements personnels, vérificateur interne, responsable de gestion documentaire, responsable de la sécurité physique, etc.).

1.4 Cadre légal et normatif

La catégorisation des actifs informationnels s'inscrit dans un cadre légal et normatif comprenant des lois, des directives, des pratiques gouvernementales, des normes internationales et des standards de l'industrie. Les principaux éléments constitutifs de ce cadre sont présentés à l'Annexe II.

1.5 Principaux changements

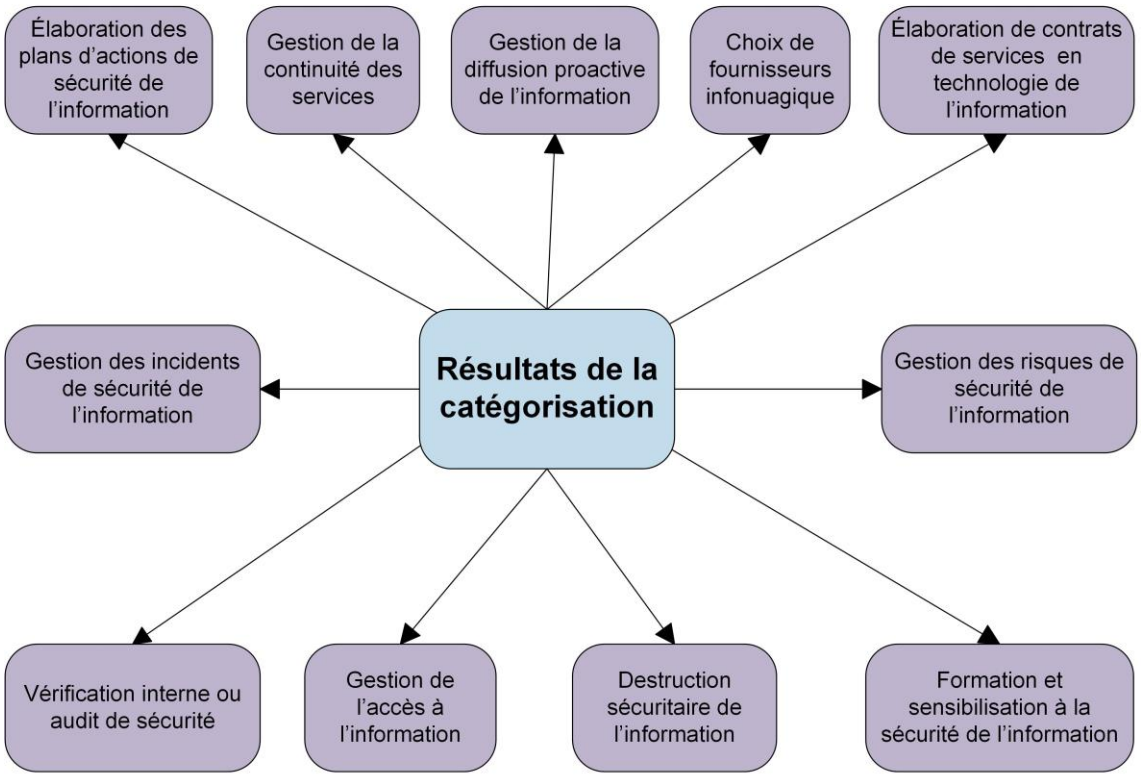
Les principaux changements par rapport à la version du guide de catégorisation diffusée en 2003 se traduisent par :

- ✓ l'utilisation du concept d'actif informationnel, assimilé à un document, quel que soit son support. La version antérieure se limitait à la catégorisation de l'information numérique;

- ✓ la prise en compte du concept de risque de sécurité de l'information à portée gouvernementale[5];
- ✓ la restriction du contenu du guide à la démarche de catégorisation, sans s'étendre au choix des mesures de sécurité à mettre en œuvre;
- ✓ la prise en considération de paramètres d'influence sur la catégorisation tels que le temps, l'agrégation de l'information et le périmètre de validité de la catégorisation (voir section 3.4).

2. Exemples de cas d'utilisation des résultats de la catégorisation

Figure 1 : Exemples de cas d'utilisation des résultats du processus de catégorisation



5. Risque de sécurité de l'information à portée gouvernementale : risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services d'autres organismes publics.
[Source : Directive sur la sécurité de l'information gouvernementale, 2014]

Comme l'illustre la figure 1, présentée ci-dessus, les résultats de l'exercice de catégorisation constituent un intrant fondamental à plusieurs processus concourant à la gestion de la sécurité de l'information. À titre d'exemple, on peut citer :

- ✓ la gestion des risques de sécurité de l'information, laquelle établit des priorités de traitement des risques sur la base du degré de sensibilité des actifs informationnels;
- ✓ le choix du fournisseur infonuagique en vue d'assurer la protection des actifs informationnels selon leur sensibilité;
- ✓ l'élaboration du plan d'action de sécurité de l'information, lequel accorde une plus grande priorité aux actifs informationnels importants pour l'organisme;
- ✓ la gestion de la diffusion proactive de l'information eu égard au Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, y compris la diffusion de renseignements personnels à caractère public et de données dont on a enlevé le caractère nominatif, en format ouvert, en vue de leur réutilisation;
- ✓ la vérification de l'adéquation des mesures de sécurité par rapport aux niveaux de criticité des actifs informationnels;
- ✓ la gestion des incidents de sécurité de l'information, en tenant compte du degré de sensibilité des actifs informationnels;
- ✓ la mise en œuvre de stratégies de continuité des services, axées sur les actifs informationnels à valeur élevée;
- ✓ la rédaction de clauses contractuelles en vue d'assurer la protection des actifs informationnels à forte sensibilité, confiés à un tiers;
- ✓ le choix du procédé de destruction sécuritaire de l'information, en tenant compte de la valeur de cette information;
- ✓ la mise en place de mécanismes de contrôle d'accès à l'information selon son niveau de sensibilité;
- ✓ la sensibilisation des employés et des partenaires aux mesures de protection associées à la valeur de l'information utilisée.

3. Concepts utilisés

Cette section décrit les principaux concepts utilisés dans la démarche de catégorisation, objet du présent guide.

3.1 Critères de sécurité

La valeur de l'information est évaluée sur le plan de la disponibilité, de l'intégrité et de la confidentialité (DIC) requises pour l'atteinte des objectifs d'affaires d'une organisation. À titre de rappel, ces critères se définissent comme suit :

- ✓ la disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

- ✓ l'intégrité : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation.
- ✓ la confidentialité : Propriété d'une information de n'être accessible ou divulguée qu'aux personnes ou entités désignées et autorisées.

3.2 Niveaux d'impact

Le niveau d'impact traduit l'importance des conséquences qu'un bris de sécurité d'un actif informationnel peut avoir sur l'organisme et sa clientèle ou sur d'autres organismes. Ces conséquences peuvent se traduire par l'incapacité de l'organisme à :

- ✓ remplir sa mission;
- ✓ se conformer aux lois, aux règlements et aux obligations contractuelles;
- ✓ préserver son image de marque et celle du gouvernement;
- ✓ maintenir ou rehausser la confiance de la clientèle et des partenaires à l'égard des services offerts;
- ✓ préserver la vie, la santé ou le bien-être des personnes;
- ✓ respecter les droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée;
- ✓ ne pas affecter le fonctionnement d'organismes tiers, tributaires de ses services.

La figure 2, présentée ci-après, décrit, à titre indicatif seulement, des niveaux d'impact que les organismes publics peuvent adapter à leur contexte.

Figure 2 : Grille de niveaux d'impact

Niveau d'impact		Description
1	Bas (négligeable)	✓ affecte un secteur d'activité de l'organisme.
2	Moyen (modéré)	✓ affecte plusieurs secteurs d'activité de l'organisme.
3	Élevé (grave)	✓ affecte de manière significative la qualité de services indispensables à la population. ✓ affecte l'image de marque de l'organisme. ✓ affecte les activités propres à un ou plusieurs autres organismes. ✓ affecte le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée, sans porter atteinte à la santé, à la vie ou au bien-être de ces personnes.

4	Très élevé (très grave)	✓ un ou plusieurs services indispensables à la population ne peuvent être rendus. ✓ met en danger la santé, la vie ou le bien-être des personnes. ✓ affecte le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée et, de ce fait, met en danger la santé, la vie ou le bien-être de ces personnes. ✓ affecte l'image de marque du gouvernement, avec ou sans médiatisation.

Une explication détaillée de ces niveaux d'impact est présentée à l'Annexe III.

De plus, les niveaux d'impact exprimés sur le plan de la disponibilité, de l'intégrité et de la confidentialité sont décrits à la figure 3, présentée ci-après.

Figure 3 : Niveaux d'impact exprimés sur le plan de la DIC

Niveaux d'impact / Critères de sécurité	Niveau 1 (Bas)	Niveau 2 (Moyen)	Niveau 3 (Élevé)	Niveau 4 (Très élevé)
Disponibilité	La perturbation des accès ou de l'utilisation de l'actif informationnel a un impact négligeable pour l'organisme.	La perturbation des accès ou de l'utilisation de l'actif informationnel a un impact modéré pour l'organisme.	La perturbation des accès ou de l'utilisation de l'actif informationnel a un impact grave pour l'organisme.	La perturbation des accès ou de l'utilisation de l'actif informationnel a un impact très grave pour l'organisme.
Intégrité	La modification non autorisée ou la destruction de l'actif informationnel a un impact négligeable pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a un impact modéré pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a un impact grave pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a un impact très grave pour l'organisme.
Confidentialité	L'accès non autorisé ou la divulgation de l'actif informationnel a un impact négligeable pour l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a un impact modéré pour l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a un impact grave pour l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a un impact très grave pour l'organisme.

À titre d'exemple, l'Annexe IV présente :

- ✓ une grille de niveaux d'impact sur le plan de la DIC selon le contexte propre à un organisme fictif;
- ✓ l'utilisation de cette grille pour l'attribution des niveaux d'impact à des actifs informationnels.

3.3 Niveau de granularité

Le niveau de granularité est le degré de détail recherché lors de l'identification des objets à catégoriser, ci-après dénommés « objets de catégorisation ». Ainsi, un objet de catégorisation peut être assimilé à un processus, un regroupement d'actifs informationnels ou un actif informationnel. Le choix du niveau de granularité est tributaire du contexte de l'organisation et du degré de précision souhaité pour répondre à ses besoins en matière de sécurité de l'information. À titre d'exemple, un organisme souhaitant procéder à une analyse de risques de sécurité de l'information choisirait, pour son exercice de catégorisation, le niveau de granularité « regroupement d'actifs informationnels » au lieu de « processus ». En revanche, pour élaborer des contrats de services en technologie de l'information, une catégorisation au niveau « processus » serait suffisante.

3.4 Facteurs d'influence sur les niveaux d'impact

a) Le temps

La catégorisation de certains actifs informationnels est sensible au facteur « temps ». Un actif informationnel peut avoir un niveau de confidentialité élevé pour une période donnée et être public par la suite. Dans ce cas, il est recommandé de revoir la catégorisation de cet actif selon les étapes de son cycle de vie. Dans le cas où cette révision n'est pas certaine, voire impossible, il est recommandé d'attribuer à l'actif le niveau d'impact le plus élevé de son cycle de vie.

À titre d'exemple :

- ✓ Le niveau d'impact sur le plan de la confidentialité, associé au budget du gouvernement, avant l'annonce officielle, pourrait prendre les valeurs 3 ou 4. Une fois le budget publié, cette valeur passe à 1.
- ✓ L'article 36 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ci-après appelée Loi sur l'accès, stipule : « Un organisme public peut refuser de communiquer toute version préliminaire ou tout projet de texte législatif ou réglementaire jusqu'à l'expiration de dix ans de sa date ». Quant à l'article 38 de cette même loi, son libellé est le suivant : « Un organisme public peut refuser de communiquer un avis ou une recommandation que lui a fait un organisme qui en relève ou qu'il a fait à un autre organisme public, jusqu'à ce que la décision finale sur la matière faisant l'objet de l'avis ou de la recommandation ait été rendue publique par l'autorité compétente ».

b) L'agrégation de l'information

Lorsqu'un objet de catégorisation contient des éléments de niveaux d'impact différents, c'est généralement le niveau le plus élevé qui l'emporte. Ainsi, un processus impliquant plusieurs actifs informationnels de niveaux d'impact différents peut être considéré comme une agrégation de ces actifs et hériter du niveau d'impact le plus élevé.

De même, un objet de catégorisation peut hériter d'un niveau d'impact supérieur à ceux attribués individuellement aux actifs informationnels qui le composent.

À titre d'exemple :

- ✓ La description physique d'un témoin important et son lieu de résidence, pris isolément, peuvent être catégorisés comme étant de niveau « élevé » sur le plan de la confidentialité. Par contre, l'objet réunissant ces deux éléments pourrait nécessiter un niveau d'impact « très élevé ».
- ✓ Des renseignements anonymisés peuvent, lorsqu'ils sont regroupés, permettre d'identifier des personnes à nouveau. La possibilité que cet impact survienne est ainsi multipliée dans un contexte de diffusion proactive de données en format ouvert, dont le principal objectif est la réutilisation dans de nouveaux contextes.

Pour comprendre l'effet de l'agrégation sur la détermination des niveaux d'impact, il suffit d'apprécier :

- ✓ la différence entre la perte d'un dossier et celle d'un classeur contenant plusieurs dossiers;
- ✓ la différence entre la divulgation de l'enregistrement d'une conversation et celle de l'ensemble des enregistrements associés à une enquête;
- ✓ l'attrait que peut représenter une banque de données de l'ensemble des personnes atteintes d'une maladie grave, par opposition au dossier de santé d'une seule personne;
- ✓ l'impact que pourrait avoir une erreur dans le dossier d'un citoyen par rapport à l'impact que pourrait avoir une erreur influençant les calculs sur l'ensemble des dossiers.

c) Le périmètre de validité de la catégorisation

Les niveaux d'impact attribués aux objets de catégorisation d'un processus sont basés sur l'analyse du contexte d'affaires définissant le périmètre de ce processus. Ils sont donc valides au sein de ce périmètre. Pour s'assurer de la cohérence de ces niveaux d'impact à l'échelle de l'organisme, il y a lieu de procéder à leur validation, en tenant compte des interrelations du processus en question avec les autres processus.

3.5 Registre de catégorisation

Le registre de catégorisation permet une description détaillée des objets de catégorisation. On y retrouve leurs principaux attributs tels que le libellé, l'unité administrative responsable, le processus utilisateur, le détenteur, la localisation[6], le niveau d'impact sur le plan de la DIC, la date de catégorisation, les références aux justificatifs d'attribution de niveaux d'impact, etc.

La gestion de ce registre est généralement confiée à une personne de l'organisme, soit le détenteur du registre de catégorisation. Celui-ci est notamment chargé :

- ✓ d'y consigner les résultats de la catégorisation;
- ✓ de tenir à jour le registre et de s'assurer de la cohérence de son contenu;
- ✓ de veiller à la sécurité et à la validité du registre;
- ✓ d'attribuer les autorisations d'accès au registre;
- ✓ de s'assurer périodiquement, auprès des détenteurs de l'information, que les niveaux d'impact attribués aux actifs sous leur responsabilité sont toujours valides.

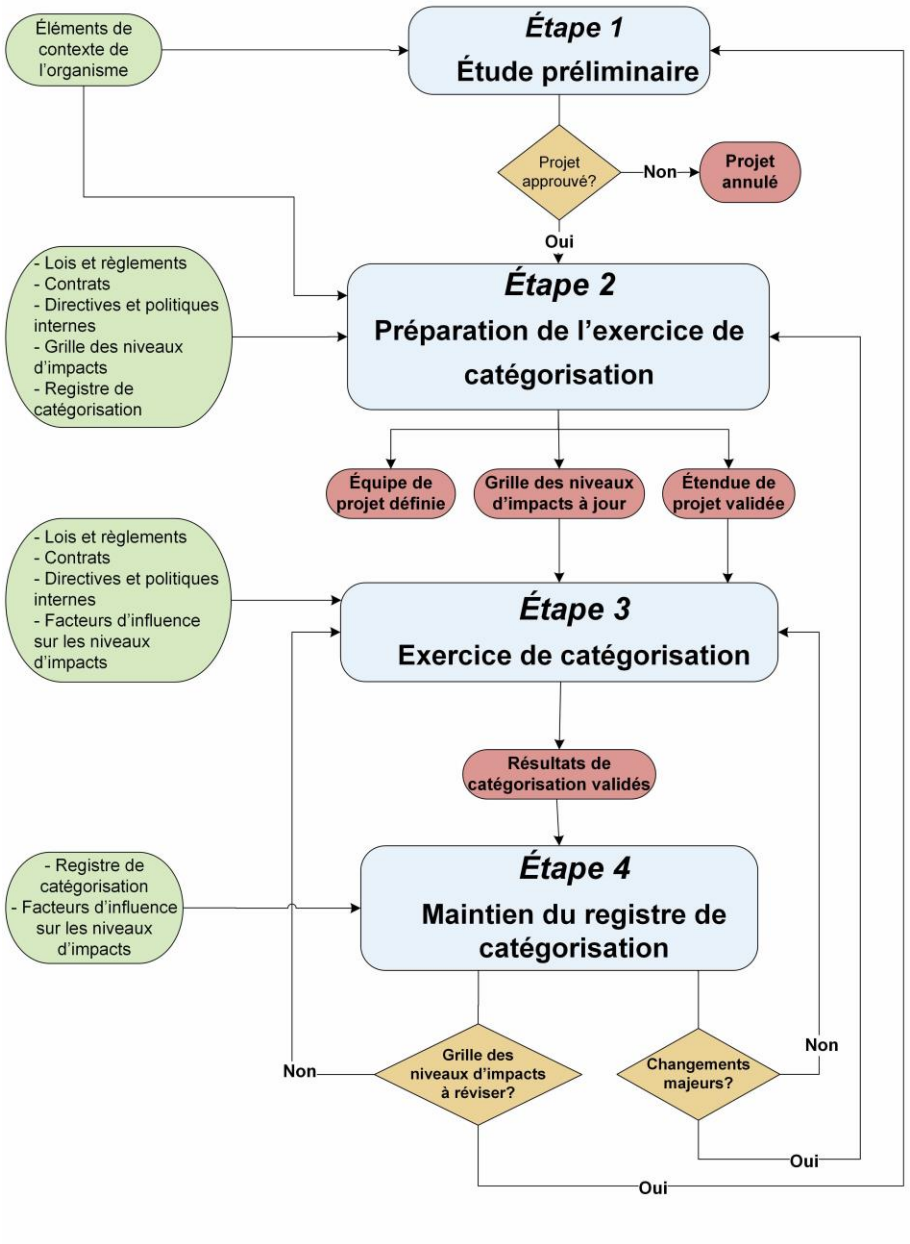
6. La localisation d'un objet de catégorisation peut être un classeur, un serveur ou autre.

4. Processus de catégorisation

L'objectif principal de la catégorisation n'est pas de faire un inventaire de l'ensemble des actifs informationnels de l'organisme, mais plutôt d'identifier ceux qui sont importants sur le plan de la disponibilité, de l'intégrité et de la confidentialité. Cependant, devant la variété d'actifs informationnels que détient un organisme, l'expression des besoins s'avère difficile : « Que faut-il protéger et à quel niveau? ».

La présente section apporte des éléments de réponse à cette question; il s'agit de suivre une démarche comportant plusieurs étapes.

Figure 4 : Étapes du processus de catégorisation



Étape 1 : Étude préliminaire

L'étude préliminaire permet à la haute direction d'apprécier la pertinence de l'exercice de catégorisation. Elle est généralement requise pour un exercice de catégorisation d'envergure, nécessitant l'aval de la haute direction et la confirmation de sa volonté de dégager les ressources nécessaires à la réalisation du projet.

Les principaux éléments de l'étude préliminaire sont les suivants :

- ✓ une mise en contexte du projet (assises légales et réglementaires, contraintes contractuelles, évolution croissante des menaces et vulnérabilités, etc.);
- ✓ les objectifs généraux de l'exercice de catégorisation (p. ex. déterminer les actifs informationnels critiques en vue d'une analyse de risques en sécurité de l'information, établir les processus nécessitant un plan de continuité des services);
- ✓ les avantages de l'exercice de catégorisation et ses retombées sur la sécurité de l'information et les enjeux d'affaires;
- ✓ l'étendue globale de l'exercice exprimée sous l'angle des unités administratives ou des processus visés. Cette étendue n'est pas définitive et sert à donner un ordre de grandeur au projet;
- ✓ les biens livrables attendus (grille des niveaux d'impact, calendrier des ateliers de travail, résultats de la catégorisation, registre de catégorisation, etc.);
- ✓ le calendrier de réalisation des biens livrables et les efforts devant être consentis (date et durée de réalisation, efforts requis);
- ✓ les validations et les approbations nécessaires;
- ✓ les coûts estimés.

L'étude préliminaire est généralement confiée à une personne-ressource investie de responsabilités en matière de sécurité de l'information (p. ex. le ROSI[7]). Elle est présentée au comité chargé de la sécurité de l'information[8], aux fins d'obtenir l'approbation de la haute direction.

Une fois l'étude approuvée, la haute direction officialise le lancement de l'exercice de catégorisation, en communiquant aux unités administratives visées la date de démarrage et le nom du chargé de projet.

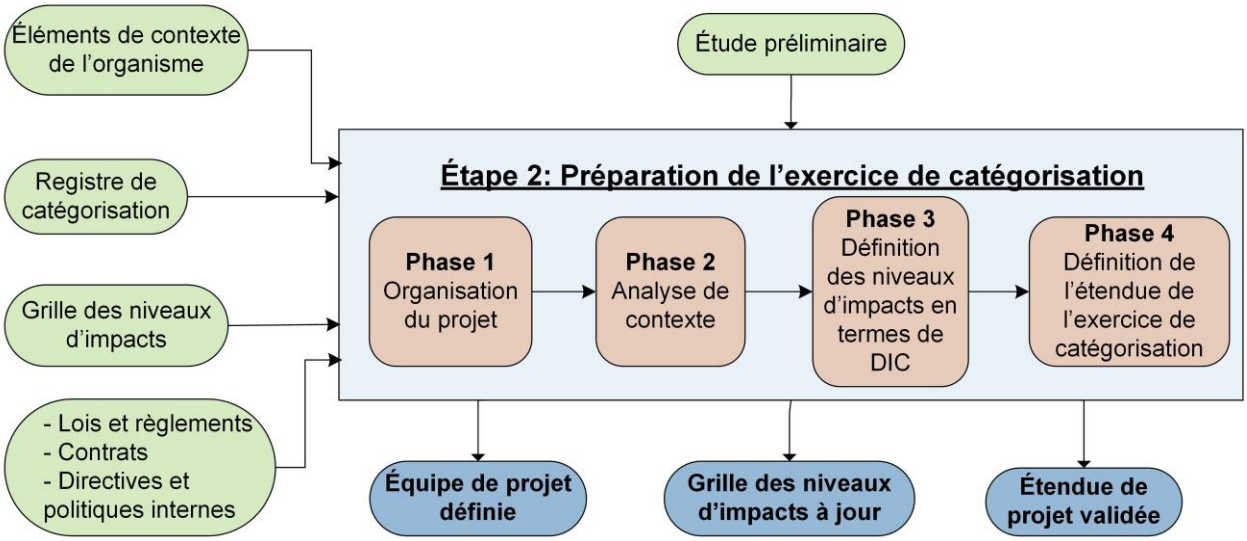
Un exemple d'étude préliminaire est présenté à l'Annexe XII.

Étape 2 : Préparation de l'exercice de catégorisation

Cette étape permet de s'assurer de la disponibilité des éléments nécessaires au bon déroulement de l'exercice de catégorisation. Il s'agit, notamment, de la constitution de l'équipe de projet, de l'analyse du contexte, de la définition de la grille des niveaux d'impact et de la définition de l'étendue de l'exercice de catégorisation.

7. ROSI : responsable organisationnel de la sécurité de l'information.
8. Le comité chargé de la sécurité de l'information : Il joue un rôle conseil, auprès du dirigeant d'organisme, relativement à toute question se rapportant à la sécurité de l'information, y compris la catégorisation des actifs de l'organisation (pour obtenir de plus amples renseignements, consulter le Cadre de gestion gouvernementale de la sécurité de l'information).

Figure 5 : Étape 2 du processus de catégorisation



Comme l'illustre la figure 5, présentée ci-dessus, cette étape se décline en quatre phases.

Phase 1- Organisation du projet de catégorisation

La phase 1 est requise dans les cas où :

- ✓ l'exercice de catégorisation vise un nombre important de processus;
- ✓ la grille des niveaux d'impact en matière de sécurité de l'information doit être définie ou révisée. En effet, cette tâche exige une analyse des enjeux d'affaires, nécessitant la contribution de divers acteurs.

Cette phase permet de définir la structure fonctionnelle du projet, les rôles et les responsabilités des divers intervenants ainsi que le calendrier des ateliers de travail. Une proposition d'organisation de projet, que chaque organisme public pourra adapter à son contexte, est présentée à l'Annexe IV.

Phase 2 - Analyse de contexte

Au cours de la phase 2, l'équipe de projet procède à la collecte et prend connaissance de toute documentation pertinente lui permettant de préciser l'étendue de la catégorisation, de définir les niveaux d'impact sur le plan de la DIC, propres à l'organisme et de prendre conscience des contraintes règlementaires et administratives régissant les domaines d'affaires de l'organisation. L'analyse de contexte porte principalement sur :

- ✓ la mission, la vision, les orientations et les objectifs stratégiques ainsi que les besoins d'affaires de l'organisme;
- ✓ les obligations légales et contractuelles ainsi que les politiques, les directives et les autres règles permettant de déterminer les besoins et les objectifs de l'organisme en matière de DIC;

- ✓ la structure fonctionnelle de l'organisme (organigramme);
- ✓ la clientèle ciblée et la déclaration de services aux citoyens;
- ✓ les représentations graphiques ou les descriptions narratives des processus d'affaires;
- ✓ les analyses des enjeux d'affaires de l'organisme;
- ✓ les analyses de risques réalisées;
- ✓ le registre d'autorité[9] de la sécurité de l'information;
- ✓ le registre de catégorisation;
- ✓ tout autre document pertinent tel que le cadre de référence de l'information gouvernementale défini dans l'architecture d'entreprise gouvernementale et qui présente la structure fonctionnelle de l'activité gouvernementale (domaines d'affaires, secteurs d'activité, sous-secteurs d'activité, etc.)

Phase 3 - Définition des niveaux d'impact sur le plan de la DIC

La définition des niveaux d'impact sur le plan de la DIC se fait généralement dans le cadre d'un atelier de travail réunissant l'équipe de projet, les détenteurs et les autres intervenants de domaines connexes. Pour ce faire, les participants prennent appui sur :

- ✓ l'analyse de contexte décrite précédemment (point 4.2.2);
- ✓ les grilles de niveaux d'impact présentées aux figures 2 et 3 du point 3.2.

Le résultat de la phase 3 est une grille de niveaux d'impact, sur le plan de la DIC, à jour et conforme au contexte de l'organisme.

Phase 4 - Définition de l'étendue de l'exercice de catégorisation

L'équipe de projet définit l'étendue de l'exercice de catégorisation, en prenant appui sur :

- ✓ l'analyse de contexte précédemment décrite (point 4.2.2);
- ✓ la portée de l'exercice de catégorisation, définie globalement dans le cadre de l'étude préliminaire.

La définition de l'étendue se traduit par l'établissement des processus d'affaires nécessaires à l'accomplissement de la mission de l'organisation. La fiche descriptive présentée ci-après peut être utilisée à cet effet.

9. Registre d'autorité : Répertoire, recueil ou fichier, dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information. Dans ce registre sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information.

Figure 6 : Fiche de description de l'étendue du projet de catégorisation

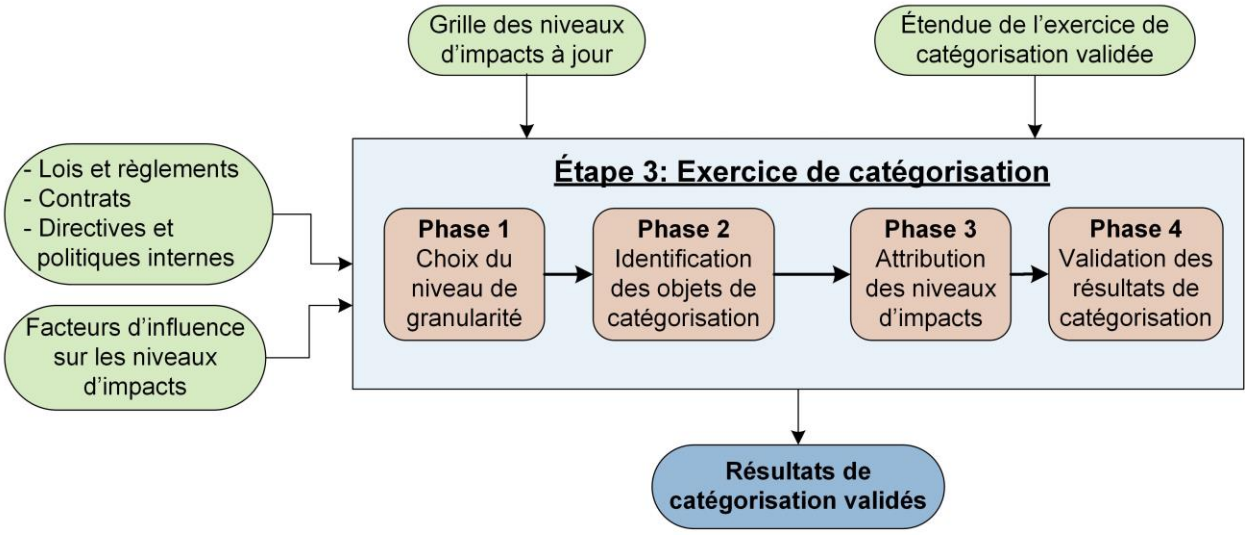
Processus	Unité administrative	Nom du détenteur	Impacts possibles d'un bris de sécurité de l'information	Dernière date de catégorisation[10]	À catégoriser? (Oui/Non)

Un atelier de travail, mettant à contribution les détenteurs, permet de valider le choix des processus précédemment déterminés par l'équipe de projet. Lors de cet atelier, les participants s'assurent de prendre en considération à tout le moins les processus exposés à un bris de sécurité de l'information aux conséquences graves (niveau d'impact = 3) ou très graves (niveau d'impact = 4).

Un exemple d'identification de l'étendue de projet est présenté à l'Annexe XII.

Étape 3 : Exercice de catégorisation

Figure 7 : Étape 3 du processus de catégorisation



10. Dernière date de catégorisation : Information disponible dans le registre de catégorisation. Elle s'applique à un processus déjà catégorisé.

Comme l'illustre la figure 7, présentée ci-dessus, l'étape 3, tout comme l'étape 2, se décline en quatre phases :

- ✓ le choix du niveau de granularité;
- ✓ l'identification des objets de catégorisation, selon le niveau de granularité choisi;
- ✓ l'attribution des niveaux d'impact aux objets de catégorisation identifiés;
- ✓ la validation des résultats de catégorisation par les intervenants concernés.

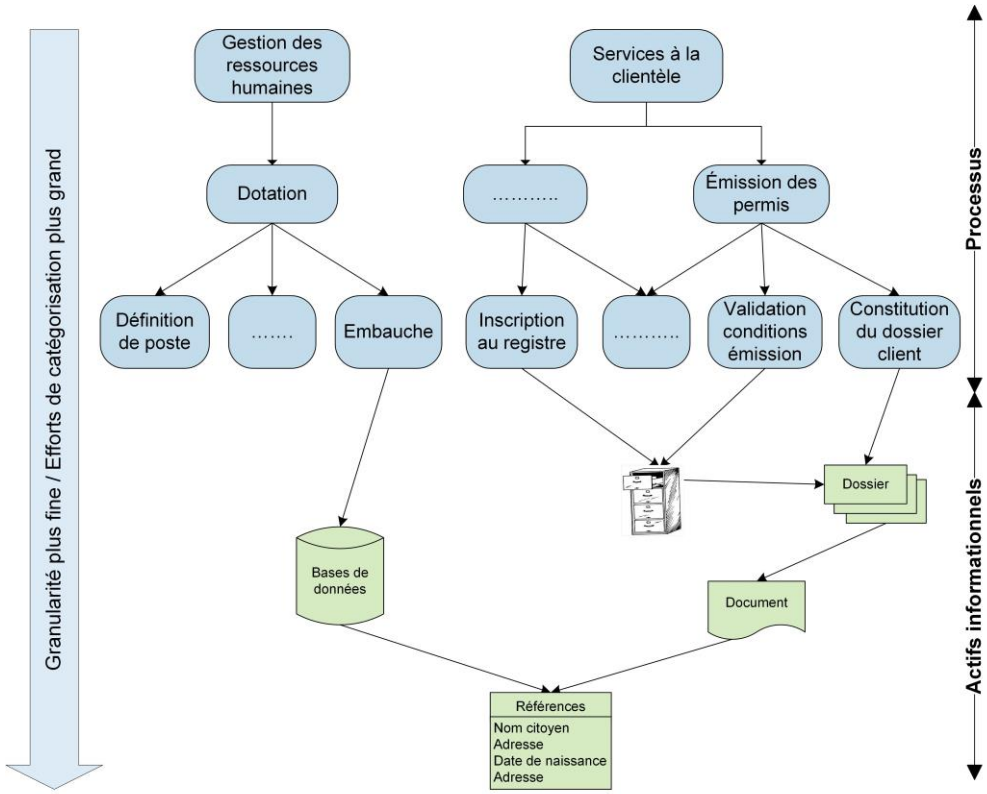
Phase 1 - Choix du niveau de granularité

Le choix du niveau de granularité se fait en atelier de travail réunissant les détenteurs. Il se base sur l'analyse de contexte (consulter le point 4.2.2) et sur les exigences de l'organisme en matière de DIC. Le cadre de référence de l'information gouvernementale, défini dans l'architecture d'entreprise gouvernementale, peut être utilisé par les détenteurs pour avoir un aperçu global de la décomposition du domaine d'affaires de l'organisme en secteurs et sous-secteurs d'activité.

Cet atelier permet d'examiner la pertinence d'évaluer les impacts d'un bris de DIC au niveau « processus » ou « regroupement d'actifs informationnels ».

Ainsi, différents niveaux de granularité peuvent être retenus, selon le degré de criticité des processus considérés lors d'un même projet de catégorisation.

Figure 8 : Exemple d'objets de catégorisation

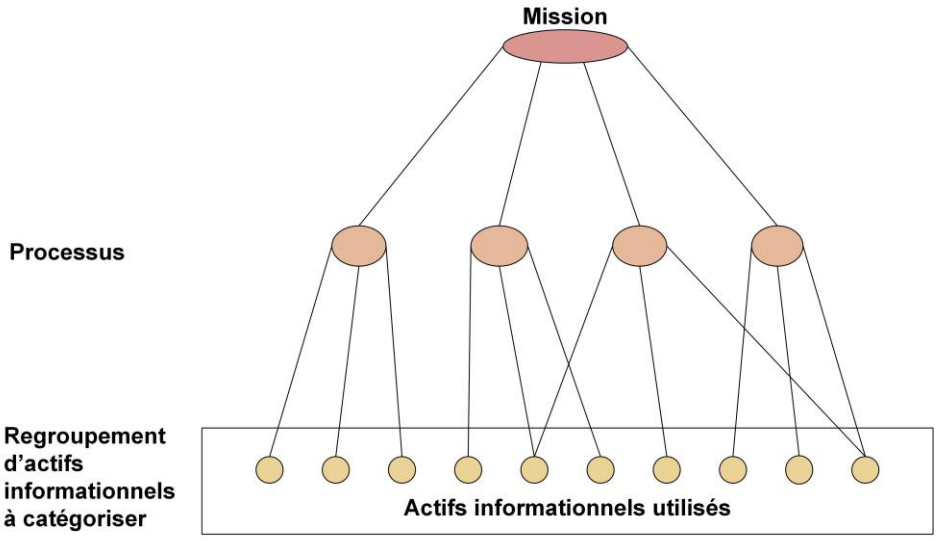


Il est à noter que le choix du niveau de granularité a une incidence directe sur le nombre d'objets à catégoriser et, par conséquent, sur les efforts qui doivent être consentis pour réaliser l'exercice de catégorisation. En effet, plus la granularité est fine, plus longue sera la liste des objets à catégoriser et plus importants seront les efforts à consentir. La figure 8, présentée ci-dessus, illustre l'ampleur des objets de catégorisation, lesquels peuvent être de niveau « processus » ou « regroupement d'actifs informationnels ».

Phase 2 - Identification des objets de catégorisation

L'identification des objets de catégorisation se fait dans le cadre d'un atelier de travail réunissant l'équipe de projet et les détenteurs responsables des processus déterminés dans le cadre de la définition de l'étendue de l'exercice de catégorisation (consulter le point 4.2.4). Le formulaire présenté à l'Annexe VI et la fiche présentée à l'Annexe VII peuvent être utilisés à cet effet.

Figure 9 : Approche d'identification des objets de catégorisation



Comme l'illustre la figure 9, présentée ci-dessus, l'approche préconisée pour la phase 2, soit l'identification des objets de catégorisation, s'appuie sur la mission de l'organisme pour en dégager, selon le niveau de granularité retenu à la phase 1 (consulter le point 4.3.1), les processus ou les actifs informationnels qui les soutiennent.

Quel que soit le niveau de granularité retenu pour l'identification des objets de catégorisation (processus ou regroupement d'actifs informationnels), les personnes participant à l'atelier peuvent prendre appui sur les éléments de réponse apportés aux questions suivantes :

- ✓ Les activités de chaque processus déterminé dans le cadre de la définition de l'étendue de l'exercice de catégorisation ont-elles des niveaux de criticité semblables? Sinon, quelle serait la décomposition du processus en question en d'autres processus qui répondraient à ce critère?

- ✓ Quelles sont les exigences légales et contractuelles à considérer pour chaque processus déterminé?
- ✓ Quels sont les processus pour lesquels les enjeux de sécurité peuvent engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, la perturbation de ses services ou de ceux fournis par d'autres organismes, l'incapacité de l'organisme à rendre un ou plusieurs services indispensables à la population?
- ✓ Quels sont les processus pour lesquels les enjeux de sécurité peuvent engendrer des conséquences telles que l'atteinte à l'image de marque de l'organisme, la perte de confiance de sa clientèle ou l'infraction aux lois et règlements?
- ✓ Quels sont les processus pour lesquels les enjeux de sécurité peuvent mettre en danger la santé, la vie ou le bien-être des personnes?
- ✓ Quels sont les processus pour lesquels les enjeux de sécurité peuvent affecter le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée?
- ✓ Quels sont les niveaux de gravité à attribuer aux conséquences établies précédemment?
- ✓ Quelles sont les interdépendances entre les processus déterminés et les autres processus internes ou externes?

Dans le cas où le niveau de granularité retenu pour l'identification des objets de catégorisation est de niveau « regroupement d'actifs informationnels », les questions suivantes compléteront la collecte d'information :

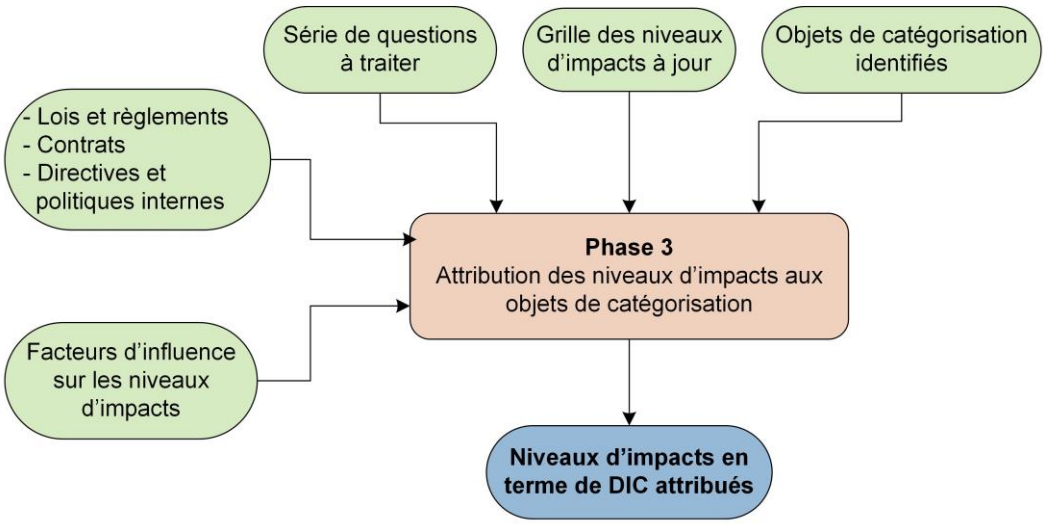
- ✓ Quelles sont les actifs informationnels (document, application, base de données, etc.) qui soutiennent chacun des processus précédemment déterminés?
- ✓ Les actifs informationnels répondant aux critères de la question précédente peuvent-ils être regroupés en sous-ensembles d'actifs ayant des similarités et nécessitant le même niveau de protection? Si oui, quels sont les objets de catégorisation qui en résultent?
- ✓ Les objets de catégorisation identifiés répondent-ils aux consignes de regroupement présentées à l'Annexe VIII?
- ✓ Parmi les objets de catégorisation identifiés, quels sont ceux échangés entre processus?

Un exemple d'identification d'objets de catégorisation est présenté à l'Annexe XII.

Phase 3 - Attribution des niveaux d'impact aux objets de catégorisation

L'attribution des niveaux d'impact est l'étape la plus délicate et la plus exigeante du processus de catégorisation. Elle se fait généralement dans le cadre d'un atelier de travail, de concert avec les détenteurs.

Figure 10 : Attribution des niveaux d'impact aux objets de catégorisation



Comme l'illustre la figure 10, présentée ci-dessus, les personnes participant à l'atelier prennent appui sur :

- ✓ la grille des niveaux d'impact, conforme au contexte de l'organisme (consulter le point 4.2.3);
- ✓ le contexte réglementaire et contractuel de l'organisme;
- ✓ les objets de catégorisation identifiés au point 4.3.2;
- ✓ les facteurs susceptibles d'influencer les niveaux d'impact sur le plan de la DIC, notamment les facteurs temps et agrégation (consulter le point 3.4);
- ✓ les réponses à une série de questions permettant d'évaluer les impacts découlant d'un bris de la DIC des objets de catégorisation. Cette série de questions est présentée à l'Annexe IX.

À l'issue de la phase 3, un niveau d'impact est attribué à chaque objet de catégorisation, ce qui permet de remplir les colonnes « niveau d'impact » du formulaire présenté à l'Annexe VI

Les tableaux présentés ci-après donnent deux exemples d'attribution de niveaux d'impact, selon la grille des niveaux d'impact de la Figure 3.

a) Attribution des niveaux d'impact à un objet de catégorisation de type « processus » (Obj-Cat1)

	Question	Réponse	Observation	Niveau d'impact attribué
Disponibilité	La non-disponibilité de certains actifs informationnels soutenant le processus pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes ou causer une interruption de services indispensables à la population?	Non	Le niveau d'impact associé à cette réponse est inférieur à « 4 ».	3 (L'Obj-Cat1 hérite du niveau d'impact le plus élevé)
	La non-disponibilité de certains actifs informationnels soutenant le processus pourrait-elle causer une infraction aux lois ou aux règlements? Si oui, quelles en seraient les conséquences?	Non	Le niveau d'impact associé à cette réponse est « 3 ».	
	La non-disponibilité de certains actifs informationnels soutenant le processus pourrait-elle causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?	Oui. Plusieurs secteurs d'activités de l'organisme peuvent être touchés. Les services fournis par d'autres organismes peuvent être très peu touchés.	Le niveau d'impact associé à cette réponse est « 2 ».	
Intégrité	Une modification non autorisée ou la destruction de certains actifs informationnels soutenant le processus pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes ou causer une interruption de services indispensables à la population?	Non	Le niveau d'impact associé à cette réponse est inférieur à « 4 ».	3 (L'Obj-Cat1 hérite du niveau d'impact le plus élevé)
	Une modification non autorisée ou la destruction de certains actifs informationnels soutenant le processus pourrait-elle affecter de manière significative la qualité de services indispensables à la population?	Oui	Le niveau d'impact associé à cette réponse est « 3 ».	
	Une modification non autorisée ou la destruction de certains actifs informationnels soutenant le processus pourrait-elle affecter de manière significative le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?	Oui. Atteinte à l'image de marque de l'organisme, avec médiatisation, et perte de confiance de la clientèle découlant d'une atteinte à leurs droits à la protection des renseignements personnels et au respect de leur vie privée, mais la santé, la vie ou le bien-être de ces personnes n'est pas touché.	Le niveau d'impact associé à cette réponse est « 3 ».	

	Question	Réponse	Observation	Niveau d'impact attribué
	Les extrants du processus engagent-ils, directement ou indirectement, la responsabilité de l'organisme ou d'un tiers avec lequel l'organisme transige? Si oui, quelle serait la conséquence d'une modification non autorisée de ces extrants?	Oui. Affecte deux secteurs d'activités de l'organisme qui ne sont pas critiques. Aucun impact sur les organismes externes.	Le niveau d'impact associé à cette réponse est « 1 ».	
Confidentialité	Un accès non autorisé ou la divulgation de certains actifs informationnels soutenant le processus pourrait-il engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à l'image de marque de l'organisme ou la perte de confiance de sa clientèle?	Non	Le niveau d'impact associé à cette réponse est inférieur à « 4 ».	4 (L'Obj-Cat1 hérite du niveau d'impact le plus élevé)
	Un accès non autorisé ou la divulgation de certains actifs informationnels soutenant le processus pourrait-il affecter de manière significative le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?	Oui, Le bien-être ou la santé de certaines personnes sera touché. Cela pourra générer une perte de confiance de la clientèle envers l'organisme.	Le niveau d'impact associé à cette réponse est « 4 ».	
	Les actifs informationnels soutenant le processus traitent-ils de renseignements autres que personnels dont la confidentialité est régie par des lois et règlements? Si oui, quelle serait la conséquence d'un accès non autorisé ou de la divulgation de ces actifs à des tiers non autorisés par la loi?	Oui. Atteinte à l'image de marque de l'organisme, avec médiatisation, ainsi que la perte de confiance de la clientèle à l'égard de l'organisme	Le niveau d'impact associé à cette réponse est « 3 ».	
	Un accès non autorisé ou la divulgation de certains actifs informationnels soutenant le processus pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes ou causer une interruption de services indispensables à la population?	Oui	Le niveau d'impact associé à cette réponse est « 4 ».	

b) Attribution des niveaux d'impact à un objet de catégorisation de type « regroupement d'actifs informationnels » (Obj-Cat2)

	Question	Réponse	Observation	Niveau d'impact attribué
Disponibilité	Quel serait l'impact de la non-disponibilité de l'objet sur les processus qu'il soutient et sur l'organisme en général?	Peut causer un retard pour certaines activités, mais sans incidence majeure.	Le niveau d'impact associé à cette réponse est « 1 ».	2 (L'Obj-Cat2 hérite du niveau d'impact le plus élevé)
	La non-disponibilité de l'objet pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes ou causer une interruption de services indispensables à la population?	Non	Le niveau d'impact associé à cette réponse est inférieur à « 4 ».	
	Quelle est la période de tolérance au manque de disponibilité de l'objet?	De 1 à 2 semaines	Le niveau d'impact associé à cette réponse est « 2 ».	
Intégrité	L'objet représente-t-il une valeur financière importante pour l'organisme? Si oui, quelle serait la conséquence de son altération?	Oui. Un seul secteur d'activité peut être touché.	Le niveau d'impact associé à cette réponse est « 1 ».	4 (L'Obj-Cat2 hérite du niveau d'impact le plus élevé)
	L'objet a-t-il une valeur authentique ou à caractère officiel? Si oui, quelle serait la conséquence de son altération?	Oui L'image de marque de l'organisme est atteinte, et il y a possibilité de médiatisation.	Le niveau d'impact associé à cette réponse est « 3 ».	
	Une modification non autorisée ou la destruction de l'objet pourrait-elle affecter de manière significative la qualité de services indispensables à la population?	Non	Le niveau d'impact associé à cette réponse est inférieur à « 3 ».	

	Question	Réponse	Observation	Niveau d'impact attribué
	Une modification non autorisée ou la destruction de l'objet pourrait-elle affecter de manière significative le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?	Oui. Atteinte à l'image de marque de l'organisme, avec médiatisation, et perte de confiance de la clientèle à l'égard de l'organisme. Le bien-être ou la santé de certaines personnes sera touché.	Le niveau d'impact associé à cette réponse est « 4 ».	
	Une modification non autorisée ou la destruction de l'objet pourrait-elle causer une interruption de services indispensables à la population?	Non	Le niveau d'impact associé à cette réponse est inférieur à « 4 ».	
Confidentialité	Un accès non autorisé ou la divulgation de l'objet pourrait-il causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?	Oui. Un secteur d'activité de l'organisme est touché. Les activités des autres organismes ne sont pas touchées.	Le niveau d'impact associé à cette réponse est « 1 ».	« Obj-Cat2_non_ Diffusé » hérite du niveau d'impact le plus élevé : « 4 » Et « Obj-Cat2_ Diffusé » est de niveau d'impact « 1 »
	L'objet traite-t-il de renseignements personnels dont la confidentialité est régie par la loi? Si oui, quelle serait la conséquence d'un accès non autorisé ou de leur divulgation à des tiers non autorisés par la loi?	Oui. Le bien-être de certaines personnes sera touché ainsi que le respect des droits fondamentaux des personnes à l'égard de la protection des renseignements personnels qui les concernent et de leur vie privée. Cela pourra générer la perte de la confiance de la clientèle envers l'organisme.	Le niveau d'impact associé à cette réponse est « 4 ».	
	L'objet traite-il de renseignements autres que personnels dont la confidentialité est régie par des lois et règlements? Si oui, quelle serait la conséquence de leur divulgation?	Oui. Atteinte à l'image de marque de l'organisme, avec médiatisation, ainsi que la perte de confiance de sa clientèle.	Le niveau d'impact associé à cette réponse est « 3 ».	
	Le niveau de confidentialité de l'objet est-il inchangé durant tout son cycle de vie?	Non. Une fois la preuve diffusée, elle devient publique. Ce changement d'état n'a aucun effet sur le plan de l'intégrité et sur celui de la disponibilité.	Le niveau d'impact associé après diffusion sera « 1 ». Pour mettre en évidence ce changement, on doit distinguer entre « Obj-Cat2_non_ Diffusé » et « Obj-Cat2_Diffusé ».	

Phase 4 - Validation des résultats de la catégorisation

Le niveau d'impact attribué à un objet de catégorisation reflète la perception du détenteur par rapport au processus qu'il soutient. Il peut être évalué différemment lorsqu'il est utilisé par un autre processus.

La présente phase de validation a pour objet d'homogénéiser l'attribution des niveaux d'impact à l'échelle de l'organisation. Elle est réalisée dans le cadre d'un atelier regroupant l'équipe de projet, les détenteurs et d'autres intervenants, notamment le responsable de l'accès aux documents et de la protection des renseignements personnels (RADPRP) ou la personne le représentant. Le formulaire présenté à l'Annexe IX peut être utilisé à cet effet.

Un exemple de validation est présenté à l'Annexe IAnnexe XII

À l'issue de cet atelier, les niveaux d'impact retenus à l'échelle de l'organisation sont consignés au registre de catégorisation, par le détenteur de celui-ci. Un modèle de contenu du registre de catégorisation est présenté à l'Annexe XI.

Étape 4 : Maintien du registre de catégorisation

Certains facteurs peuvent influer sur les niveaux d'impact déjà attribués aux objets de catégorisation. De ce fait, les détenteurs devront veiller à la validité du registre de catégorisation, notamment dans les cas suivants :

- ✓ modification des lois et règlements;
- ✓ modification d'une ou de plusieurs fonctionnalités d'un processus;
- ✓ ajout ou retrait d'actif informationnel;
- ✓ modification de la grille des niveaux d'impact propre à l'organisme;
- ✓ changement de détenteur de l'information;
- ✓ changement organisationnel;
- ✓ révision périodique des niveaux d'impact consignés au registre de catégorisation. Il est à noter que, pour s'assurer de la validité des niveaux d'impact déjà consignés au registre de catégorisation, le détenteur de ce registre transmet périodiquement aux détenteurs de l'information une demande de confirmation des niveaux d'impact attribués aux actifs informationnels dont ils ont la responsabilité.

Le tableau suivant présente les différentes actions à poser à la suite de chacun des événements survenus.

Événement survenu	Actions à poser
Modification apportée aux lois et règlements	✓ Vérifier si les modifications apportées aux lois et règlements ont une influence sur les enjeux d'affaires de l'organisme et les critères de définition des niveaux d'impact en matière de sécurité de l'information de l'organisme. ✓ Si oui, revoir les critères de niveaux d'impact et, par conséquent, la grille des niveaux d'impact sur le plan de la DIC (consulter l'événement suivant : Modification de la grille des niveaux d'impact sur le plan de la DIC propre à l'organisme).
Modification de la grille des niveaux d'impact sur le plan de la DIC propre à l'organisme	✓ Revoir les niveaux d'impact sur le plan de la DIC attribués aux objets de catégorisation par leurs détenteurs. ✓ Valider les modifications apportées aux niveaux d'impact à l'échelle de l'organisme. ✓ Mettre à jour le registre de catégorisation, au besoin.
Modification d'une ou de plusieurs fonctionnalités d'un processus	✓ Vérifier si la modification des fonctionnalités est en lien avec l'ajout d'un actif informationnel au processus ou le retrait d'un actif informationnel du processus. Si oui, consulter, selon le cas, l'événement « ajout d'un actif informationnel » ou l'événement « retrait d'un actif informationnel ». ✓ Vérifier si la modification des fonctionnalités occasionne un changement dans les flux informationnels en entrée ou en sortie du processus considéré. Si oui, valider les niveaux d'impact sur le plan de la DIC des objets de catégorisation touchés par ce changement, auprès des détenteurs des processus visés par ces échanges. ✓ Mettre à jour le registre de catégorisation, au besoin.
Ajout d'un actif informationnel	✓ Vérifier si le nouvel actif informationnel fait partie d'un objet de catégorisation déjà consigné au registre. Si oui, vérifier si les niveaux d'impact déjà attribués à cet objet correspondent aux besoins en sécurité du processus considéré et, le cas échéant, ajuster le niveau d'impact. ✓ Si l'actif informationnel n'est utilisé par aucun processus déjà catégorisé, le détenteur procèdera à sa catégorisation, conformément à l'étape 3 du processus de catégorisation décrite précédemment (consulter le point 4.3). ✓ Mettre à jour le registre de catégorisation, au besoin.
Retrait d'un actif informationnel	✓ Vérifier si le retrait de l'actif informationnel occasionne un changement du niveau d'impact de l'objet de catégorisation dont il fait partie. Si oui, ajuster le niveau d'impact en conséquence. ✓ Vérifier si le retrait de l'actif informationnel entraîne un changement dans les flux informationnels échangés avec d'autres processus. Si oui, ajuster le niveau d'impact en conséquence et valider cet ajustement auprès des détenteurs des processus visés par ces échanges. ✓ Mettre à jour le registre de catégorisation, au besoin.
Changement de détenteur de l'information	✓ Mettre à jour le registre de catégorisation pour y consigner le nom du nouveau détenteur.

Événement survenu	Actions à poser
Changement organisationnel	✓ Vérifier si le changement organisationnel a un impact sur les processus de l'organisme et sur les responsabilités des détenteurs de l'information à l'égard des objets de catégorisation. Si oui, s'assurer, auprès des détenteurs touchés par la réorganisation, que les niveaux d'impact sur le plan de la DIC attribués aux actifs informationnels sous leur responsabilité sont valides. ✓ Valider, auprès des détenteurs concernés, les modifications apportées aux niveaux d'impact. ✓ Mettre à jour le registre de catégorisation, au besoin.
Demande de confirmation périodique des niveaux d'impact attribués	✓ Valider, auprès des détenteurs de l'information, les niveaux d'impact sur le plan de la DIC attribués aux objets de catégorisation consignés au registre de catégorisation. ✓ Mettre à jour le registre de catégorisation, au besoin.

5. Outil de catégorisation

Le présent guide de catégorisation est accompagné d'un outil *Excel*, composé de trois formulaires :

- ✓ un formulaire d'identification des objets de catégorisation, présenté à l'Annexe VII;
- ✓ un formulaire de validation des résultats de catégorisation, présenté à l'Annexe IX;
- ✓ un modèle de registre de catégorisation, présenté à l'Annexe XI.

Références

ANSSI/ACE/BAC, Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS), Méthode de gestion des risques, janvier 2010.

CIGREF, Protection de l'information, Enjeux, gouvernance et bonnes pratiques, 2008.

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS (CLUSIF), MEHARI 2010, Guide de l'analyse des enjeux et de la classification, janvier 2010.

ISO/CEI 27002, Code de bonne pratique pour la gestion de la sécurité de l'information, 2e édition, juin 2005.

JAMES F. STEVENS, *Information Asset Profiling*, juin 2005.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Volume I: Guide for mapping types of information and information systems to security categories, août 2008.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Standards for Security Categorization of Federal Information and Information Systems, février 2004.

OFFICE OF CYBER SECURITY & CRITICAL INFRASTRUCTURE COORDINATION, Information Classification and Control, décembre 2008.

QUEENSLAND GOVERNMENT ENTREPRISE ARCHITECTURE, ICT POLICY AND COORDINATION OFFICE, DEPARTMENT OF PUBLIC WORKS, Queensland Government Information Security Classification Framework, novembre 2010.

SOFTWARE ENGINEERING INSTITUTE, Introducing OCTAVE Allegro: Improving the information Security Risk Assessment Process, mai 2007.

ANNEXE I Définitions

Actif informationnel : tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1). À titre de rappel, cette loi définit le document comme étant :
« Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.
[...] est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »

Catégorisation : Processus permettant de déterminer le niveau de criticité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs sur l'organisme et sa clientèle ou sur d'autres organismes.

Confidentialité : Propriété d'une information de n'être accessible ou divulguée qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information : L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme public.
[Source : Directive sur la sécurité de l'information gouvernementale, 2014]

Détenteur de l'information : Employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.
[Source : Directive sur la sécurité de l'information gouvernementale, 2014]

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Intégrité : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation.

Objet de catégorisation : Un objet de catégorisation peut être assimilé à un processus, un regroupement d'actifs informationnels ou un actif informationnel. C'est l'élément auquel on attribue les niveaux d'impact sur le plan de la DIC.

Niveau d'impact : Le niveau d'impact traduit l'importance des conséquences qu'un bris de sécurité d'un actif informationnel peut avoir sur l'organisme et sa clientèle ou d'autres organismes.

Registre d'autorité : Répertoire, recueil ou fichier, dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information. Dans ce registre sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information.

Registre de catégorisation : Répertoire dans lequel sont consignés les niveaux d'impact, sur le plan de la DIC, des actifs informationnels.

Risque de sécurité de l'information à portée gouvernementale : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image de marque du gouvernement, ou sur la prestation de services d'autres organismes publics. [Source : Directive sur la sécurité de l'information gouvernementale, 2014].

Service indispensable ou essentiel : Service dont la perturbation pourrait mettre en péril la vie, la sécurité, la santé ou le bien-être économique de la personne dans une partie ou dans la totalité de la population. [Guide sur la gestion de la continuité des services, janvier 2010]

ANNEXE II Cadre légal et normatif

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales.

Fondements légaux :

- ✓ la Directive sur la sécurité de l'information gouvernementale;
- ✓ la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- ✓ la Loi sur les archives (LRQ, chapitre A-21.1);
- ✓ les lois sectorielles régissant la mission de chaque organisme;
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2).

Fondements normatifs :

- ✓ le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ le cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ les normes internationales, notamment : ISO/CEI 27001 et 27002, ISO/CEI 27005;
- ✓ les politiques et directives de sécurité de l'information propres à chaque organisme;
- ✓ les pratiques gouvernementales en matière de sécurité de l'information.

ANNEXE III Explications des niveaux d'impact

Niveau 1 – Bas : impact négligeable

Ce niveau signifie que l'événement a des incidences d'ordre administratif plutôt négligeables qui sont traitées localement, sans affecter l'organisme sur le plan global ou les autres organismes.

Ces incidences n'empêchent pas l'organisme de réaliser sa mission et n'affectent ni son image de marque ni sa crédibilité. L'événement n'a aucun impact sur des services indispensables à la population ou sur la vie, la santé et le bien-être des personnes. Il n'affecte pas le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée.

Niveau 2 – Moyen : impact modéré

Ce niveau signifie que l'événement aurait des incidences sur plusieurs secteurs d'activités de l'organisme, mais pas sur son image de marque. L'événement n'a aucun impact sur des services indispensables à la population, sur les autres organismes, ou sur la vie, la santé ou le bien-être des personnes. Il n'affecte pas le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée.

À ce niveau, les incidences de l'événement peuvent se résorber facilement et rapidement.

Niveau 3 – Élevé : impact grave

Ce niveau signifie que l'événement aurait des incidences sérieuses et qu'il pourrait causer des dommages à l'organisme ou à sa clientèle. Il pourrait également nuire aux activités critiques de l'organisme ou à son image de marque, mais sans affecter l'image de marque du gouvernement.

Les incidences de l'événement dépassent le périmètre de l'organisme et affectent certaines activités propres à d'autres organismes.

Il est important de souligner que les incidences de l'événement peuvent affecter de manière significative des services indispensables à la population, mais qu'elles ne menacent pas la vie, la santé ou le bien-être des personnes.

L'événement peut également avoir un impact sur le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée, mais sans porter atteinte à la santé, à la vie ou au bien-être de ces personnes.

Niveau 4 – Très élevé : impact très grave

Ce niveau signifie que l'événement a des incidences extrêmement sérieuses sur l'organisme, les citoyens et les autres organismes.

L'événement peut affecter l'image de marque du gouvernement, avec ou sans médiatisation. Il peut également affecter le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée et mettre en danger la vie, la santé ou le bien-être de ces personnes.

Des services indispensables à la population et le fonctionnement de l'organisme ou d'autres organismes peuvent être paralysés ou compromis.

ANNEXE IV Exemple d'attribution de niveaux d'impact sur le plan de la DIC

a) Grille de niveaux d'impact, sur le plan de la DIC, d'un organisme fictif

Niveaux d'impact / Critères de sécurité	Niveau 1 (Bas)	Niveau 2 (Moyen)	Niveau 3 (Élevé)	Niveau 4 (Très élevé)
Disponibilité	La tolérance au délai de récupération est de quelques semaines.	La tolérance au délai de récupération est de quelques jours.	La tolérance au délai de récupération est de quelques heures.	Aucune tolérance au délai de récupération.
Intégrité	La fiabilité est compromise pour un actif informationnel servant à des activités administratives.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires non critiques.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires critiques, mais n'ayant aucune incidence sur la vie, la santé ou le bien-être des personnes ou sur l'image de marque du gouvernement.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires critiques et susceptibles de porter atteinte à la vie, la santé ou au bien-être des personnes, ou à la protection de leurs renseignements personnels et de leur vie privée, ou encore à l'image de marque du gouvernement.
Confidentialité	Actif informationnel ou renseignements à caractère public.	Actif informationnel dont la divulgation ou l'accès non autorisé est susceptible de mettre dans l'embarras le secteur administratif visé.	Actif informationnel dont la divulgation ou l'accès non autorisé est susceptible de causer un préjudice grave à l'organisme, à un autre organisme ou à sa clientèle.	Actif informationnel dont la divulgation ou l'accès non autorisé affecte le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée et met en danger la sécurité, la santé ou le bien-être de ces personnes, ou porte atteinte à l'image de marque du gouvernement, avec ou sans médiatisation.

b) Attribution des niveaux d'impact

DISPONIBILITÉ			
Niveau 1 (Bas)	**Niveau 2 (Moyen)**	**Niveau 3 (Élevé)**	**Niveau 4 (Très élevé)**
La tolérance au délai de récupération est de quelques semaines.	La tolérance au délai de récupération est de quelques jours.	La tolérance au délai de récupération est de quelques heures.	Aucune tolérance au délai de récupération.
Exemples			
Statistiques sur l'utilisation d'un site Internet Statistiques relatives à la gestion du personnel Actifs informationnels internes disponibles sous différentes formes, telles que : bottin des employés modèles de lettres, de formulaires, de rapports	Plan de projet Documents de travail internes Suivi du budget et de l'avancement d'un projet Documents faisant l'objet d'une demande d'accès (documents ou renseignements)	Dossiers des fournisseurs Documents d'appui à la gestion de certains paiements à la clientèle (primes, allocations, indemnités, rentes, aide financière) Ententes avec les fournisseurs	Plan de relève d'un service indispensable Documents de publicité des droits des citoyens, registres publics (publicité des droits, état civil) Document à l'appui de services indispensables offerts par l'organisme, tels que : dossier de santé d'un patient, d'un enfant faisant l'objet d'un signalement ou d'une personne dont la santé ou la sécurité est menacée dans l'immédiat documents utilisés directement par les policiers avis et planification des interventions de protection contre les incendies de forêt

INTÉGRITÉ

Niveau 1 (Bas)	Niveau 2 (Moyen)	Niveau 3 (Élevé)	Niveau 4 (Très élevé)
La fiabilité est compromise pour un actif informationnel servant à des activités administratives.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires non critiques.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires critiques, mais n'ayant aucune incidence sur la vie, la santé ou le bien-être des personnes ou sur l'image de marque du gouvernement.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires critiques et susceptibles de porter atteinte à la vie, à la santé ou au bien-être des personnes ou à la protection de leurs renseignements personnels et de leur vie privée, ou encore à l'image de marque du gouvernement.
Exemples			
Statistiques relatives à la gestion du personnel Documents ayant une valeur juridique ou financière négligeable, tels que : courriels entre employés travaillant sur un dossier rapports d'avancement d'un dossier	Normes et procédures opérationnelles relatives à des activités d'affaires non critiques Documents ayant une valeur juridique ou financière limitée, tels que : transactions courantes non signées ou en cours	Résultats d'examens ou de tests d'admissibilité Rapport de décisions de l'organisme Acte sous seing privé (contrat d'achat de biens mobiliers tels que machinerie, véhicules, etc.) État des résultats de l'administration d'un fonds	Document contenant des résultats d'inspection ou d'étude sur la qualité d'un produit pouvant mettre en danger la santé ou la sécurité des personnes Actes officiels opposables aux tiers tels que le registre foncier Document contenant des données médicales pouvant mettre en péril la santé ou la sécurité des citoyens

CONFIDENTIALITÉ

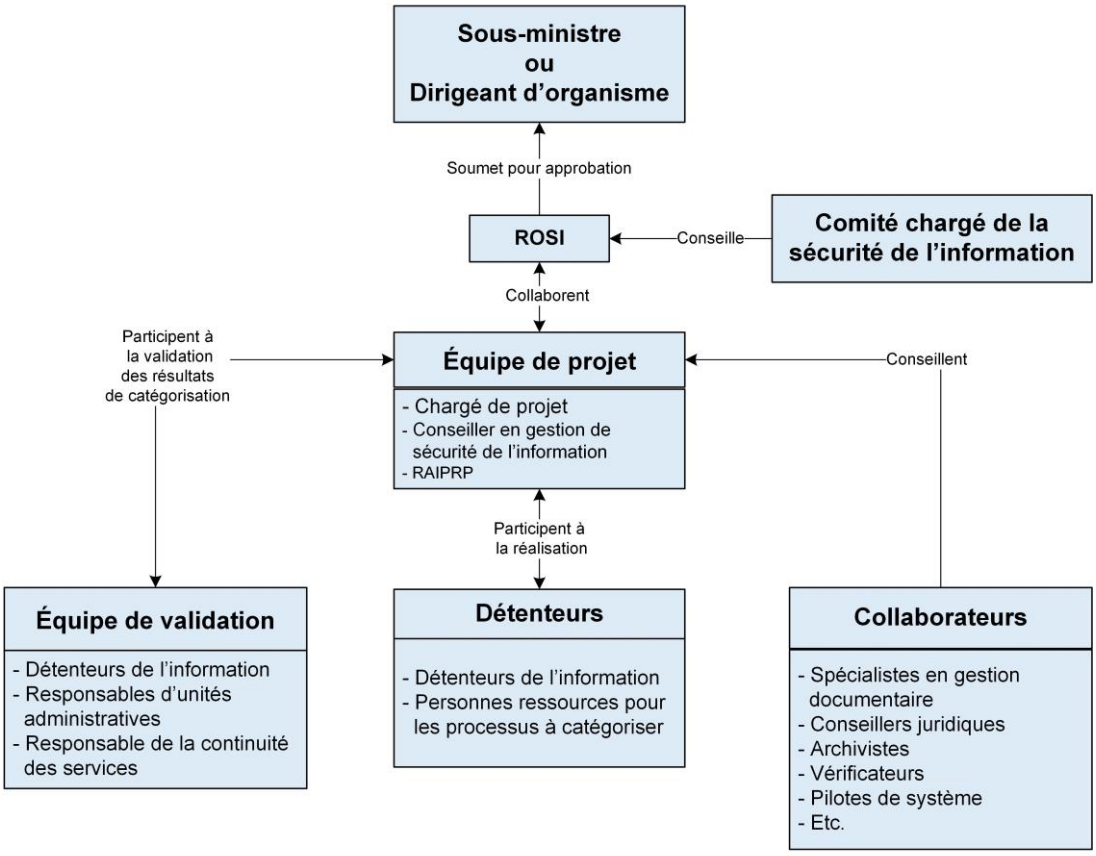
Niveau 1 (Bas)	Niveau 2 (Moyen)	Niveau 3 (Élevé)	Niveau 4 (Très élevé)
Actif informationnel ou renseignements à caractère public.	Actif informationnel dont la divulgation ou l'accès non autorisé est susceptible de mettre dans l'embarras le secteur administratif visé.	Actif informationnel dont la divulgation ou l'accès non autorisé est susceptible de causer un préjudice grave à l'organisme, à un autre organisme ou à sa clientèle.	Actif informationnel dont la divulgation ou l'accès non autorisé affecte le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée et met en danger la sécurité, la santé ou le bien-être de ces personnes ou porte atteinte à l'image de marque du gouvernement, avec ou sans médiatisation.
Exemples			
Renseignements personnels à caractère public, selon la définition de l'article 57 de la Loi sur l'accès Documents à caractère public (n'étant soumis à aucune restriction d'accès prévue à la loi) Document contenant des données statistiques ou dont on a enlevé le caractère nominatif sur la clientèle de l'organisme	Document ayant des incidences sur les négociations entre l'organisme et son partenaire d'affaires Dans certaines circonstances, des documents concernant un secteur d'activité de l'organisme et contenant une opinion juridique, un avis, une analyse Stratégie de négociation de conventions collectives	Renseignements industriels, commerciaux, scientifiques ou syndicaux de nature confidentielle, fournis par un tiers (soumission, solvabilité financière, résultat de recherche) et habituellement traités par un tiers de façon confidentielle Rapports préliminaires d'enquête sur certains membres de la clientèle ou du personnel Détails des ententes établies avec les partenaires Documents contenant des renseignements nominatifs sur la clientèle ou le personnel	Document contenant des renseignements sur des enquêtes criminelles tels que le nom et les coordonnées d'une personne agissant à titre d'informateur auprès des services de police ou bénéficiant du régime de protection des témoins Rapports préliminaires d'enquête sur certains membres de la clientèle ou du personnel Documents contenant des renseignements nominatifs susceptibles de causer un tort irréparable à une personne (diagnostic du VIH, divulgation du nom du parent biologique d'un enfant adopté, etc.) Document contenant des renseignements ayant des incidences sur l'administration de la justice et de la sécurité publique

ANNEXE V Organisation et planification du projet de catégorisation

Cette étape définit la structure fonctionnelle du projet, les rôles et les responsabilités des intervenants ainsi que le calendrier des ateliers de travail. La structure proposée peut être adaptée par l'organisme public en fonction de son contexte.

a) Structure fonctionnelle d'un projet de catégorisation

Figure 11 : Structure fonctionnelle d'un projet de catégorisation



La figure 11, présentée ci-dessus, illustre un modèle de structure fonctionnelle d'un projet de catégorisation. Cette structure est mise en place pour la durée du projet.

b) Rôles et responsabilités des intervenants

Le responsable organisationnel de la sécurité de l'information (ROSI)

Le ROSI collabore avec l'équipe de projet, pour s'assurer du bon déroulement de l'exercice de catégorisation. Il intervient auprès des responsables des unités administratives visées par

l'exercice de catégorisation. Il joue également le rôle d'intermédiaire entre la haute direction, le comité chargé de la sécurité de l'information et l'équipe de projet.

Le responsable de l'accès aux documents et de la protection des renseignements personnels (RADPRP)

Le RADPRP joue un rôle de soutien et de conseiller auprès de l'équipe de projet, notamment à l'égard de l'attribution des niveaux d'impact sur le plan de la DIC, eu égard :

- ✓ aux restrictions à l'accès aux documents établies par la Loi sur l'accès et aux obligations relativement à la protection des renseignements personnels;
- ✓ à l'information devant être diffusée en vertu du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels.

Le chargé de projet

Le chargé de projet est désigné par le dirigeant d'organisme. Il est responsable de la gestion et de la coordination du projet, depuis l'étape de planification jusqu'à l'approbation finale des niveaux d'impact attribués aux objets de catégorisation.

Le détenteur

Le détenteur joue un rôle clé dans le processus de catégorisation. Il est appelé à fournir à l'équipe de projet les renseignements pertinents sur les processus d'affaires et les actifs informationnels qui les sous-tendent, relevant de sa responsabilité. Il est également sollicité pour participer aux ateliers, commenter les documents de travail et, au besoin, proposer des pistes de solutions. C'est le détenteur qui doit ultimement approuver les résultats de la catégorisation.

L'équipe de projet

L'équipe de projet est animée par le chargé de projet. Elle peut être composée du ROSI et de conseillers en gestion de la sécurité de l'information. Elle est chargée, notamment :

- ✓ de procéder à la collecte de l'information requise pour la catégorisation;
- ✓ de définir l'étendue du projet de catégorisation;
- ✓ de planifier les activités et les échéanciers de réalisation;
- ✓ d'organiser et d'animer les entrevues et les ateliers de travail;
- ✓ de produire les documents de travail nécessaires à l'exercice de catégorisation;
- ✓ de consolider et de présenter les résultats de la catégorisation.

Les collaborateurs

L'équipe de projet peut s'adjoindre toute personne qui est en mesure de l'appuyer dans ses travaux. Citons, à titre d'exemple, les pilotes de systèmes ou toute personne-clé ayant une bonne connaissance de son unité administrative, de ses processus d'affaires et de leurs interrelations ou, encore, les conseillers juridiques, les spécialistes en gestion documentaire, les vérificateurs internes ou le répondant de l'organisme public (OP) pour les données ouvertes.

L'équipe de validation

Cette équipe collabore avec l'équipe de projet lors de la validation des résultats des travaux de catégorisation. Elle est généralement constituée des détenteurs de l'information, des responsables des unités administratives et, au besoin, du responsable de la continuité des services ou de tout autre intervenant qui est en mesure de contribuer aux travaux de validation.

c) Planification des ateliers de travail

L'équipe de projet élabore une planification des ateliers de travail, qu'elle communique aux gestionnaires des unités administratives visées. Ces ateliers servent, notamment, à :

- ✓ définir ou réviser la grille des niveaux d'impact;
- ✓ valider l'étendue de l'exercice de catégorisation;
- ✓ choisir le niveau de granularité souhaité pour l'exercice de catégorisation;
- ✓ identifier les objets de catégorisation;
- ✓ attribuer les niveaux d'impact aux objets de catégorisation identifiés;
- ✓ valider les résultats de la catégorisation.

Réunion de démarrage

Une réunion de démarrage est organisée par l'équipe de projet, en vue d'expliquer aux détenteurs :

- ✓ les objectifs de l'exercice de catégorisation;
- ✓ la démarche de catégorisation retenue;
- ✓ leur rôle dans le processus de catégorisation;
- ✓ le choix du niveau de granularité à retenir pour l'exercice de catégorisation;
- ✓ les techniques d'identification des objets de catégorisation;
- ✓ la planification et l'objectif visé par les ateliers de travail.

ANNEXE VI Formulaire d'identification des objets de catégorisation

Secrétariat du Conseil du trésor
Québec

Formulaire d'identification des objets de catégorisation

Ministère ou organisme:	
Nom détenteur:	
Date d'identification:	

Objet de catégorisation	Unité administrative	Processus	Détenteur	Description objet[1]	Type Objet[2]	Localisation[3]	Émetteur[4]	Type émetteur[5]	Destinataire	Type destinataire	Exigences spécifiques	Date de catégorisation (jj/mm/aaaa)	Niveau d'impact par processus			Références des justificatifs[6]
													D	I	C	

1. Description objet : décrit les actifs informationnels regroupés dans un objet de catégorisation de type « regroupement d'actifs informationnels » ou les activités regroupées dans un objet de catégorisation de type « processus ».
2. Type Objet : précise si l'objet de catégorisation est de type « électronique », « papier » ou « processus ».
3. Localisation : précise l'emplacement physique de l'objet de catégorisation. Cet emplacement peut être une application informatique sur un serveur, un dossier dans un classeur, etc.
4. Émetteur, Destinataire : ne prend pas de valeur dans le cas où l'objet de catégorisation est de type « processus ».
   Dans le cas où l'objet de catégorisation est de type « regroupement d'actifs informationnels », il peut prendre la valeur d'un processus, d'une unité administrative de l'organisme, du nom d'un organisme externe ou d'un partenaire externe, ou la valeur « client » ou « citoyen ». Cette information est importante pour l'étape de validation des résultats de catégorisation.
5. Type émetteur, Type destinataire : ne prend pas de valeur dans le cas où l'objet de catégorisation est de type « processus ».
   Dans le cas où l'objet de catégorisation est de type « regroupement d'actifs informationnels, il peut prendre la valeur « interne », « partenaire externe » ou « citoyen ».
6. Références des justificatifs : indique les numéros des fiches justificatives d'attribution des niveaux d'impact associées à l'objet de catégorisation, tout au long de son cycle de vie.

ANNEXE VII Fiche justificative d'attribution des niveaux d'impact

Secrétariat du Conseil du trésor
Québec

Fiche justificative d'attribution des niveaux d'impact

Numéro fiche	
Objet de catégorisation	
Unité administrative	
Nom du détenteur	
Date de catégorisation	

Critères de sécurité	Niveau d'impact	Justificatifs
Disponibilité		
Intégrité		
Confidentialité		

ANNEXE VIII Règles d'identification des objets de catégorisation

Les objets de catégorisation[11] sont identifiés selon un niveau de granularité choisi, qui peut être de niveau « processus » ou de niveau « regroupement d'actifs informationnels » (consulter le point 4.3.1).

Du point de vue de la sécurité de l'information, le niveau de granularité adéquat est atteint lorsqu'il est possible d'identifier les mesures de sécurité pouvant atténuer les risques encourus par un objet de catégorisation. Citons, à cet égard, quelques règles d'identification des objets de catégorisation.

- ✓ Dans le cas où le niveau de granularité choisi est de type « processus », il est recommandé de faire des regroupements d'activités dont la criticité est semblable pour constituer les objets de catégorisation de type « processus ».
- ✓ Dans le cas où le niveau de granularité retenu est de type « regroupement d'actifs informationnels », il est recommandé de regrouper les actifs informationnels ayant des similarités et nécessitant le même niveau de protection. Pour ce faire, on peut être amené à :
  - étendre le regroupement à un niveau de granularité supérieur : si une banque de données contient des données dont le degré de sensibilité est différent, l'objet à catégoriser est généralement la banque de données, préférablement à chacune de ses données. En effet, il est souvent plus efficient d'appliquer les mesures de sécurité propres à la banque de données plutôt que de protéger chacun de ses éléments. Le niveau d'impact le plus élevé est alors attribué à la banque de données, même si certains de ses éléments nécessitent des mesures de sécurité moins élevées.
  - restreindre le regroupement à un objet de catégorisation propre à l'emplacement d'un ensemble d'objets : si un rapport contenant de l'information confidentielle se trouve dans un dossier contenant plusieurs autres documents de nature moins sensible, l'objet de catégorisation est plutôt le rapport.
  - associer des actifs informationnels distincts à chacune des étapes du cycle de vie de l'information : plutôt que de catégoriser un rapport indépendamment de son cycle de vie, on peut être amené à distinguer entre l'ébauche de ce rapport, le rapport diffusé aux fins d'approbation, le rapport approuvé et diffusé à l'intérieur de l'organisme et le rapport publié à l'intention du grand public. À chacune de ces étapes, un niveau d'impact différent peut être attribué.

De plus, certaines questions aident à déterminer si des éléments d'information peuvent être regroupés de manière à former un seul objet de catégorisation, dont les suivantes :

- ✓ Les éléments d'information sont-ils destinés à des personnes ou à des processus différents?
- ✓ Les niveaux d'approbation différents sont-ils nécessaires pour mettre à jour les éléments constituant l'objet de catégorisation?

11. Objet de catégorisation : un objet de catégorisation peut être assimilé à un processus, un regroupement d'actifs informationnels ou un actif informationnel. C'est l'élément auquel on attribue les niveaux d'impact sur le plan de la DIC.

- ✓ Certains éléments d'information de l’objet sont-ils communiqués à d’autres applications par des interfaces ou des états imprimés?
- ✓ Certains éléments d'information de l’objet nécessitent-ils un niveau de disponibilité, d’intégrité ou de confidentialité différent des autres éléments d'information de l’objet?
- ✓ Des exigences légales ou contractuelles particulières régissent-elles une partie des éléments d'information de l’objet?
- ✓ Les éléments d'information sont-ils destinés à d’autres organismes?
- ✓ Certains éléments d'information de l’objet doivent-ils être stockés sur des supports différents?
- ✓ Toute autre question jugée pertinente, compte tenu du contexte.

Il peut également être pertinent, lors de l’identification des objets de catégorisation, de se demander si l’information répond à certains critères, notamment :

- ✓ renseignements concernant une personne physique, un organisme public ou une entreprise;
- ✓ renseignements techniques, financiers, commerciaux ou scientifiques, ainsi que d’autres documents dont la confidentialité est assurée par la Loi sur l’accès (restrictions obligatoires ou facultatives);
- ✓ renseignements liés à la fonction d’un employé de l’organisme;
- ✓ renseignements personnels d’un employé;
- ✓ Information régie par des lois particulières.

ANNEXE IX Questionnaire d'évaluation des niveaux d'impact sur le plan de la DIC

Les questions proposées dans la présente annexe sont basées sur les critères d'évaluation des niveaux d'impact, présentés au point 3.2, et sur la grille des niveaux d'impact, présentée à la figure 2 de la même section. L'organisme peut les adapter en fonction de ses propres critères d'évaluation et d'une grille de niveaux d'impact qui tient compte de son contexte.

Volet disponibilité

- ✓ Dans le cas où le niveau de granularité retenu est de niveau « processus », les questions à se poser pour chaque processus sont les suivantes :
  - La non-disponibilité de certains actifs informationnels à l'appui du processus pourrait-elle engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à son image de marque ou la perte de confiance de sa clientèle?
  - La non-disponibilité de certains actifs informationnels à l'appui du processus pourrait-elle causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?
  - La non-disponibilité de certains actifs informationnels à l'appui du processus pourrait-elle causer une infraction aux lois ou aux règlements? Si oui, quelle en serait la conséquence?
  - La non-disponibilité de certains actifs informationnels à l'appui du processus pourrait-elle limiter l'exercice du droit d'accès des citoyens aux documents ou aux renseignements qui les concernent? Pourrait-elle limiter le suivi des demandes d'accès?
  - La non-disponibilité de certains actifs informationnels à l'appui du processus pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes, ou causer une interruption de services indispensables à la population?
  - La non-disponibilité de certains actifs informationnels à l'appui du processus pourrait-elle affecter de manière significative la qualité de services indispensables à la population?
  - Le manque de disponibilité des extrants du processus peut-il avoir un effet en cascade, c'est–à-dire que les impacts seront de plus en plus importants à mesure que ce manque de disponibilité se prolonge?
  - Y a-t-il des périodes pendant lesquelles le manque de disponibilité du processus est plus critique pour l'organisme?
  - Quelle est la période de tolérance au manque de disponibilité du processus?
- ✓ Dans le cas où le niveau de granularité retenu est de niveau « regroupement d'actifs informationnels», les questions à se poser sont les suivantes :
  - Serait-il facile de reconstituer un objet inaccessible ou détruit?
  - Quel serait l'impact de la non-disponibilité d'un objet sur les processus qu'il soutient et sur l'organisme en général?

- Le manque de disponibilité d'un objet peut-il avoir un effet en cascade, c'est–à-dire que les impacts seront de plus en plus importants à mesure que ce manque de disponibilité se prolonge?
- Y a-t-il des périodes pendant lesquelles le manque de disponibilité d'un objet est plus critique pour l'organisme?
- Quelle est la période de tolérance au manque de disponibilité de l'objet?
- La non-disponibilité de l'objet pourrait-elle engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à son image de marque ou la perte de confiance de sa clientèle?
- La non-disponibilité de l'objet pourrait-elle causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?
- La non-disponibilité de l'objet pourrait-elle limiter l'exercice du droit d'accès des citoyens aux documents ou aux renseignements qui les concernent? Pourrait-elle limiter le suivi des demandes d'accès?
- La non-disponibilité de l'objet pourrait-elle causer une infraction aux lois ou aux règlements? Quelle en serait la conséquence?
- La non-disponibilité de l'objet pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes, ou causer une interruption de services indispensables à la population?
- La non-disponibilité de l'objet pourrait-elle affecter de manière significative la qualité de services indispensables à la population?

Volet intégrité

- ✓ Dans le cas où le niveau de granularité retenu est de niveau « processus », les questions à se poser pour chaque processus sont les suivantes :
  - Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à son image de marque ou la perte de confiance de sa clientèle?
  - Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités de l'organisme seraient-ils touchés?
  - Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle affecter de manière significative la qualité de services indispensables à la population?
  - Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes, ou causer une interruption de services indispensables à la population?
  - Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle affecter de manière significative le respect des droits fondamentaux des personnes à la protection des renseignements personnels

qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?

- Les extrants du processus engagent-ils, directement ou indirectement, la responsabilité de l'organisme ou d'un tiers avec lequel l'organisme transige? Si oui, quelle serait la conséquence d'une modification non autorisée de ces extrants?
- Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle engendrer une infraction aux lois ou aux règlements? Si oui, quelle en serait la conséquence?
- Certains extrants du processus pourraient-ils être utilisés pour prendre des décisions critiques?
- Certains extrants du processus pourraient-ils représenter une valeur financière importante pour l'organisme?
- Certains actifs informationnels à l'appui du processus ont-ils une valeur authentique ou un caractère officiel?

✓ Dans le cas où le niveau de granularité retenu est de niveau « regroupement d'actifs informationnels», les questions à se poser sont les suivantes :

- Quel serait l'impact d'une modification non autorisée d'un objet sur les processus qu'il soutient et sur l'organisme en général?
- L'objet a-t-il une valeur authentique ou un caractère officiel? Si oui, quelle serait la conséquence de son altération?
- L'objet représente-t-il une valeur financière importante pour l'organisme? Si oui, quelle serait la conséquence de son altération?
- L'objet pourrait-il être utilisé pour prendre des décisions critiques?
- L'objet engage-t-il, directement ou indirectement, la responsabilité de l'organisme ou d'un tiers avec lequel l'organisme transige? Si oui, quelle serait la conséquence d'une modification non autorisée de ces extrants?
- A-t-on besoin de prouver l'authenticité de l'objet? Doit-on démontrer formellement qu'il n'a pas été modifié?
- L'intégrité de l'objet est-elle régie par des lois ou règlements?
- Une modification non autorisée ou la destruction de l'objet pourrait-elle engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à son image de marque ou la perte de confiance de sa clientèle?
- Une modification non autorisée ou la destruction de l'objet pourrait-elle causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?
- Une modification non autorisée ou la destruction de l'objet pourrait-elle mettre en danger la santé, la vie ou le bien-être des personnes, ou causer une interruption de services indispensables à la population?
- Une modification non autorisée ou la destruction de l'objet pourrait-elle affecter de manière significative le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?

- Une modification non autorisée ou la destruction de certains actifs informationnels à l'appui du processus pourrait-elle affecter de manière significative la qualité de services indispensables à la population?
- Une modification non autorisée ou la destruction de l'objet pourrait-elle causer une infraction aux lois ou aux règlements? Si oui, quelle en serait la conséquence?

Volet confidentialité

- ✓ Dans le cas où le niveau de granularité retenu est de niveau « processus », les questions à se poser pour chaque processus sont les suivantes :
  - La confidentialité de certains actifs informationnels à l'appui du processus est-elle régie par des lois ou règlements?
  - Un accès non autorisé ou la divulgation de certains actifs informationnels à l'appui du processus pourrait-il engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à son image de marque ou la perte de confiance de sa clientèle?
  - Un accès non autorisé ou la divulgation de certains actifs informationnels à l'appui du processus pourrait-il causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?
  - Un accès non autorisé ou la divulgation de certains actifs informationnels à l'appui du processus pourrait-il engendrer une infraction aux lois ou aux règlements? Si oui, quelle en serait la conséquence?
  - Un accès non autorisé ou la divulgation de certains actifs informationnels à l'appui du processus pourrait-il mettre en danger la santé, la vie ou le bien-être des personnes, ou causer une interruption de services indispensables à la population?
  - Un accès non autorisé ou la divulgation de certains actifs informationnels à l'appui du processus pourrait-il affecter de manière significative le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?
  - Un accès non autorisé ou la divulgation de certains actifs informationnels à l'appui du processus pourrait-il affecter de manière significative la qualité de services indispensables à la population?
  - Les actifs informationnels à l'appui du processus traitent-ils de renseignements autres que personnels dont la confidentialité est régie par des lois? Si oui, quelle serait est la conséquence d'un accès non autorisé ou de la divulgation de ces actifs à des tiers non autorisés par la loi?
  - Les actifs informationnels à l'appui du processus doivent-ils être accessibles au public?
- ✓ Dans le cas où le niveau de granularité retenu est de niveau « regroupement d'actifs informationnels», les questions à se poser sont les suivantes :
  - L'objet traite-il ou contient-il des renseignements personnels dont la confidentialité est régie par des lois? Si oui, quelle serait la conséquence d'un accès non autorisé ou de la divulgation de ces renseignements à des tiers non autorisés par la loi?

- L'objet traite-il ou contient-il des renseignements autres que personnels devant rester confidentiels? Si oui, quelle serait la conséquence de leur divulgation?
- La confidentialité de l'objet est-elle régie par des lois ou règlements? Si oui, quelle serait la conséquence de sa divulgation?
- Un accès non autorisé ou la divulgation de l'objet pourrait-il engendrer des conséquences telles que l'incapacité de l'organisme à remplir sa mission, l'atteinte à son image de marque ou la perte de confiance de sa clientèle?
- Un accès non autorisé ou la divulgation de l'objet pourrait-il causer la perturbation des services de l'organisme ou de ceux fournis par d'autres organismes? Si oui, plusieurs secteurs d'activités seraient-ils touchés?
- Un accès non autorisé ou la divulgation de l'objet pourrait-il causer une infraction aux lois ou aux règlements? Si oui, quelle en serait la conséquence?
- Un accès non autorisé ou la divulgation de l'objet pourrait-il mettre en danger la santé, la vie ou le bien-être des personnes, ou causer une interruption de services indispensables à la population?
- Un accès non autorisé ou la divulgation de l'objet pourrait-il affecter le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée? Si oui, la santé, la vie ou le bien-être de ces personnes serait-il touché?
- Un accès non autorisé ou la divulgation de l'objet pourrait-il affecter de manière significative la qualité de services indispensables à la population?
- Cet objet doit-il être accessible au public?
- Le niveau de confidentialité de l'objet est-il inchangé durant tout son cycle de vie?

ANNEXE X Formulaire de validation des résultats de catégorisation

Secrétariat du Conseil du trésor
Québec

Formulaire de validation des résultats de catégorisation

Ministère ou organisme:	
Équipe de validation:	
Date de validation:	

Objet de catégorisation	Unité administrative	Processus	Détenteur	Description objet	Type Objet	Localisation	Émetteur	Type émetteur	Destinataire	Type destinataire	Exigences spécifiques	Date de catégorisation (jj/mm/aaaa)	Niveau d'impact par processus			Niveau d'impact global			Références des justificatifs
													D	I	C	D	I	C	

ANNEXE XI Registre de catégorisation

Secrétariat du Conseil du trésor
Québec

Registre de catégorisation

Ministère ou organisme:	
Nom du responsable du registre:	
Date de dernière mise à jour:	

Objet de catégorisation	Unité administrative	Processus	Détenteur	Description objet	Type Objet	Localisation	Exigences spécifiques	Date de catégorisation (jj/mm/aaaa)	Niveau d'impact			Références des justificatifs
									D	I	C	

Le niveau d'impact du registre de catégorisation correspond au niveau d'impact global du formulaire de validation des résultats de catégorisation.

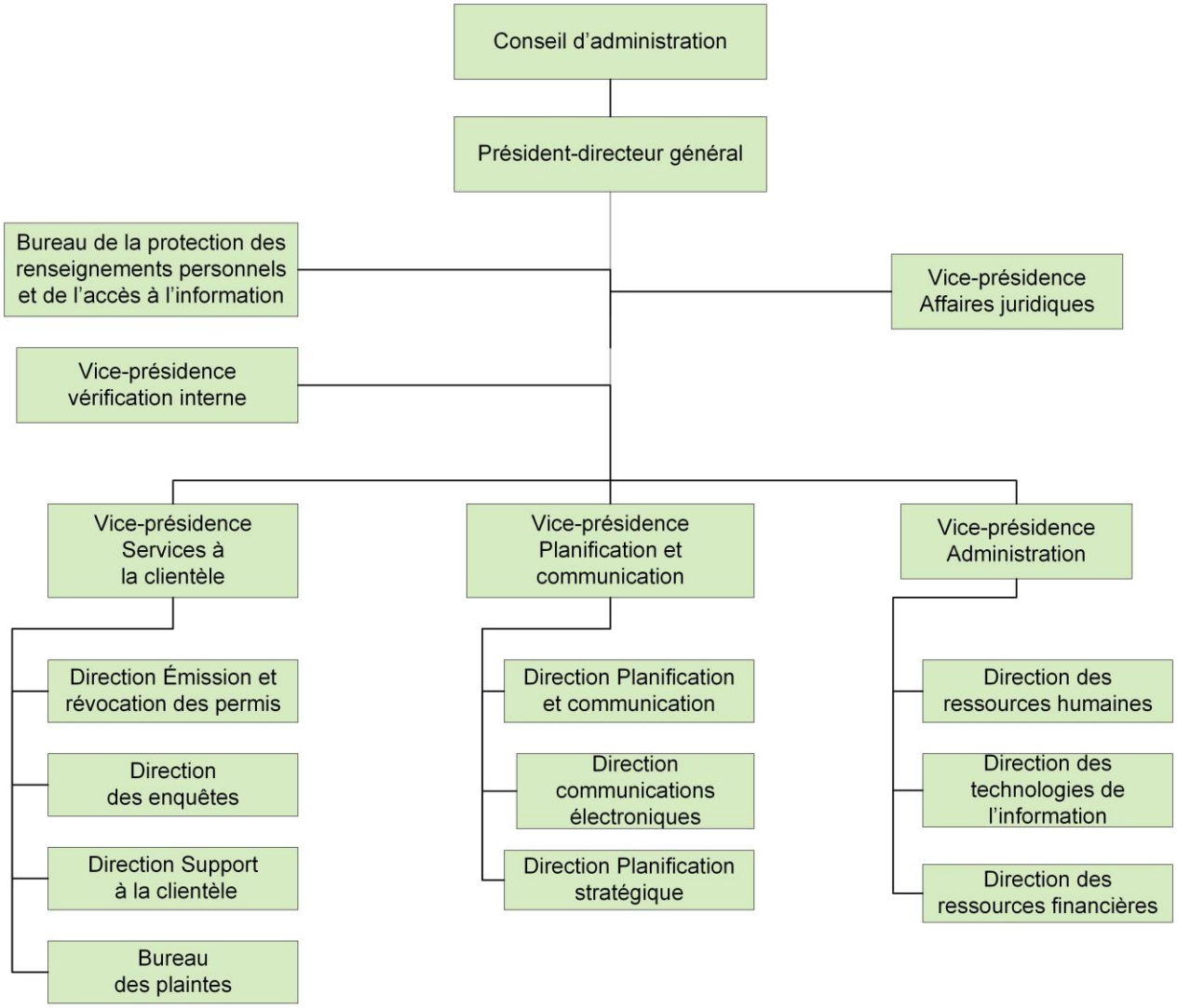
ANNEXE XII Étude de cas

La présente étude de cas permet d'illustrer, par l'exemple, la démarche de catégorisation préconisée tout au long de ce guide. Les résultats de cet exercice sont présentés en intégralité dans le chiffrier *Excel* « Outil_Catégorisation_2013_Etude_De_Cas », qui accompagne le présent guide.

Mise en contexte de l'exemple

Cet exemple porte sur un organisme fictif qui a pour mission de délivrer des permis à des citoyens et dont l'organigramme est présenté à la figure suivante.

Figure 12 : Organigramme de l'organisme (exemple)



Dans le cadre de cet exemple, l'organisme :

- ✓ gère des demandes de permis;
- ✓ offre un service de soutien à la clientèle;
- ✓ traite des plaintes;
- ✓ réalise des enquêtes sur les situations particulières ou irrégulières;
- ✓ met à la disposition de ses clients un site Internet présentant :
  - l'organisation de l'organisme (organigramme, mission, lois et règlements applicables, conseil d'administration, services offerts, coordonnées des différents bureaux, etc.)
  - la description des différents types de permis délivrés par l'organisme;
  - les conditions d'admissibilité à l'obtention d'un permis;
  - le processus de contestation.

Les citoyens peuvent faire une demande de permis à partir du site Internet de l'organisme. Ils reçoivent une confirmation de délivrance de permis par courriel, et le permis est transmis par la poste.

Étape 1 : Étude préliminaire

Le ROSI de l'organisme, d'après plusieurs éléments de contexte, a réalisé la présente étude préliminaire.

Étude préliminaire

Nom projet

Catégorisation des actifs informationnels de l'organisme

Chargé de l'étude préliminaire

Mme une telle, responsable organisationnelle de la sécurité de l'information

Date d'élaboration

mai 2013

Mise en contexte

Plusieurs éléments de contexte justifient l'importance de procéder à la catégorisation des actifs informationnels de l'organisation.

- ✓ Seuls les actifs informationnels sur support numérique sont actuellement catégorisés alors que la Directive sur la sécurité de l'information gouvernementale oblige les organismes publics à assurer la sécurité de l'information, quel que soit son support.
- ✓ Certaines unités administratives n'ont jamais catégorisé les actifs informationnels dont elles sont responsables. Il s'agit de la Direction des enquêtes, de la Direction support à la clientèle et du Bureau des plaintes.
- ✓ La mission de l'organisme est régie par des règlements dont le non-respect pourrait engendrer des conséquences graves, voire très graves, pour l'organisme, notamment des poursuites judiciaires, des amendes, la perte de confiance des citoyens et des partenaires et l'atteinte à l'image de marque de l'organisme.

- ✓ Plusieurs règlements sont récemment entrés en vigueur à la suite de l'intégration de services de délivrance de nouveaux types de permis et de paiement des frais de services par Internet.

Objectifs du projet

- ✓ évaluer les impacts que pourraient engendrer des bris de sécurité de l'information sur le bon déroulement des processus d'affaires de l'organisme;
- ✓ prendre conscience du degré de criticité des actifs informationnels que l'organisme détient dans le cadre de sa mission;
- ✓ disposer d'une grille de niveaux d'impact en matière de sécurité de l'information, en fonction du contexte actuel de l'organisme;
- ✓ homogénéiser l'évaluation des niveaux d'impact, sur le plan de la DIC, pour l'ensemble des actifs informationnels et quels que soit leurs détenteurs;
- ✓ fournir les intrants fondamentaux (niveaux d'impact des actifs informationnels) à l'ensemble des processus concourant à la gestion de la sécurité de l'information, principalement le processus de gestion de risques de sécurité de l'information.

Portée du projet

Compte tenu des éléments de contexte présentés ci-dessus, il est pertinent de procéder à la catégorisation de l'ensemble des actifs informationnels de l'organisation. La démarche proposée est la suivante :

- ✓ Scénario 1 : Considérer tous les processus d'affaires de l'organisme dont un bris de sécurité de l'information pourrait engendrer des impacts de niveau grave, voire très grave.

Le niveau de granularité suggéré pour l'identification des objets de catégorisation est de type « processus ».

- ✓ Scénario 2 : Considérer les processus d'affaires qui interagissent directement avec les citoyens ou partenaires, soit :
  - le processus d'émission et de révocation des permis;
  - le processus de gestion des enquêtes;
  - le processus de gestion des plaintes;
  - le processus de soutien à la clientèle;
  - le processus des communications électroniques.

Le niveau de granularité suggéré pour l'identification des objets de catégorisation est de type « regroupement d'actifs informationnels ».

- ✓ Scénario 3 : Procéder de façon incrémentielle :
  - Phase 1 : considérer les processus cités dans le scénario 2;
  - Phase 2 : élargir l'étendue du projet aux autres processus de l'organisme.

Le niveau de granularité suggéré pour l'identification des objets de catégorisation est de type « regroupement d'actifs informationnels ».

Biens livrables attendus et intervenants requis

Biens livrables attendus	Réalisateurs du bien livrable	Validation requise
Grille des niveaux d'impact en matière de sécurité de l'information	Équipe de projet Détenteurs de processus	Comité chargé de la sécurité de l'information
Étendue de projet	Équipe de projet Détenteurs de processus	s. o.
Actifs informationnels catégorisés	Équipe de projet Détenteurs de processus à catégoriser Autres collaborateurs	s. o.
Registre de catégorisation à jour	Détenteur du registre de catégorisation	s. o.

Il est à noter que le chargé de projet peut solliciter d'autres intervenants des domaines connexes tels que le RADPRP ainsi que les spécialistes en affaires juridiques, en gestion documentaire, en gestion de continuité des services, etc.

Évaluation des ressources nécessaires : Le tableau suivant présente une évaluation approximative des coûts et des ressources, selon les scénarios présentés précédemment :

Scénario 1

Ressources internes (j-p)				Ressources externes (j-p)			Calendrier de réalisation
Ressources	N^bre personnes	j-p	Total	N^bre personnes	j-p	Coût (j-p)	
Équipe de projet	4	30	120	2	10	10,000 $	Du 01-06-2012 au 30-06-2012
Détenteurs	10	5	50				
Autres collaborateurs	2	1	2				

Scénario 2

Ressources internes (j-p)				Ressources externes (j-p)			Calendrier de réalisation
Ressources	Nbre personnes	j-p	Total	Nbre personnes	j-p	Coût (j-p)	
Équipe de projet	4	15	60	Aucune			Du 01-06-2012 au 30-06-2012
Détenteurs	5	5	25				
Autres collaborateurs	2	1	2				

Scénario 3

Ressources internes (j-p)				Ressources externes (j-p)			Calendrier de réalisation
Ressources	Nbre personnes	j-p	Total	Nbre personnes	j-p	Coût (j-p)	
Équipe de projet	4	40	160	2	20	20,000 $	Du 01-06-2012 au 31-08-2012
Détenteurs	10	8	80				
Autres collaborateurs	2	1	2				

Validation de l'étude préliminaire

Le ROSI présente l'étude préliminaire au comité chargé de la sécurité de l'information, lequel a recommandé son approbation par la haute direction.

Officialisation du projet

Sur la recommandation du comité chargé de la sécurité de l'information, la haute direction approuve l'étude préliminaire et retient le scénario 2. Celui-ci tient compte des contraintes et répond le mieux aux objectifs d'affaires de l'entreprise. La haute direction officialise le projet en émettant un avis aux entités administratives de l'organisme. Cet avis indique :

- ✓ qu'un projet de catégorisation des actifs informationnels débutera le jj/mm/aaaa, sous la responsabilité de Mme une telle, chargée de projet;
- ✓ que les détenteurs de l'information de chaque direction sont les premiers responsables de la catégorisation des actifs informationnels dont ils ont la responsabilité et que leur participation active au projet est un gage de succès pour le projet et pour la gestion efficace de la sécurité de l'information de l'organisme.

Étape 2 : Préparation de l'exercice de catégorisation

a) Constitution de l'équipe de projet

Une fois l'étude préliminaire approuvée et le scénario 2 retenu par la haute direction, le chargé de projet constitue son équipe. Celle-ci regroupe un conseiller en gestion de la sécurité de l'information, le RADPRP, ou son représentant, et le responsable de la gestion documentaire.

b) Analyse de contexte

L'équipe de projet procède à l'analyse détaillée de plusieurs éléments de contexte de l'organisme (l'énoncé de mission, les renseignements publiés sur l'intranet et le site Internet, les principaux programmes encadrant les besoins d'affaires, la déclaration de services aux citoyens, etc.).

L'organisme n'avait antérieurement procédé à aucune analyse de risques de sécurité de l'information et ne dispose pas d'une grille des niveaux d'impact.

L'organisme est régi par une loi sectorielle, et certaines de ses activités sont encadrées par des délais de rigueur, notamment le traitement des plaintes, le traitement des contestations, la mise à jour du contenu du site Internet, etc.

L'organisme n'offre pas de services essentiels au sens de la Loi sur la sécurité civile et n'est pas lié par des ententes contractuelles lui imposant des contraintes supplémentaires.

c) Définition de la grille des niveaux d'impact sur le plan de la DIC

À l'issue de l'analyse présentée ci-dessus, l'équipe de projet a retenu la grille des niveaux d'impact proposée à la figure 2 du point 3.2 du présent guide. S'en est suivi un atelier de travail avec les détenteurs, en vue de :

- ✓ valider la grille retenue;
- ✓ définir une grille de niveaux d'impact, sur le plan de la DIC, propre à l'organisme.

Grille des niveaux d'impact sur le plan de la DIC, propre à l'organisme

Niveaux d'impact / Critères de sécurité	Niveau 1 (Bas)	Niveau 2 (Moyen)	Niveau 3 (Élevé)	Niveau 4 (Très élevé)
Disponibilité	Actifs informationnels dont l'indisponibilité est tolérable pour quelques semaines. Exemple : Indisponibilité d'éléments d'information complémentaires sur l'émission de permis sur le site Internet de l'organisme.	Actifs informationnels dont l'indisponibilité est tolérable pour quelques jours. Exemple : Indisponibilité des rapports d'enquête pour la révocation de permis.	Actifs informationnels dont l'indisponibilité est tolérable pour quelques heures. Exemple : Indisponibilité de la base de données des formulaires de demande de permis.	Actifs informationnels dont l'indisponibilité n'est aucunement tolérable. Aucun actif dans cette catégorie, puisque l'organisme n'offre pas de services essentiels.
Intégrité	La fiabilité est compromise pour un actif informationnel servant à des activités administratives. Exemple : Modification non autorisée d'éléments d'information générale de sensibilisation, destinés au public et publiés sur le site Internet de l'organisation.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires non critiques. Exemple : Modification non autorisée d'éléments d'information sur les conditions d'admissibilité à un permis, destinés au public et publiés sur le site Internet de l'organisation.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires critiques, mais n'ayant aucune incidence sur la vie, la santé ou le bien-être des personnes ou encore sur l'image de marque du gouvernement. Exemple : Modification non autorisée d'un ou de plusieurs formulaires de plainte.	La fiabilité est compromise pour un actif informationnel servant à des activités d'affaires critiques et susceptibles de porter atteinte à la vie, à la santé ou au bien-être des personnes, ou à la protection de leurs renseignements personnels et de leur vie privée, ou encore à l'image de marque du gouvernement. Exemple : Modification non autorisée d'un rapport d'enquête nécessaire à la délivrance d'un permis.

Confidentialité	Actifs informationnels ou renseignements à caractère public.	Actifs informationnels dont la divulgation ou l’accès non autorisé peut mettre dans l'embarras la ou les directions visées. Exemple : Divulgation au public, avant la date officielle, de statistiques non confirmées sur le taux d’émissions et de révocations des permis.	Actifs informationnels dont la divulgation ou l’accès non autorisé peut causer un préjudice grave à l’organisme, à un autre organisme ou à sa clientèle. Exemple : Divulgation des motifs de non-admissibilité d’un citoyen à l’obtention d’un permis.	Actifs informationnels dont la divulgation ou l’accès non autorisé affecte le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée et met en danger la sécurité, la santé ou le bien-être de ces personnes, ou encore porte atteinte à l’image de marque du gouvernement, avec ou sans médiatisation. Aucun actif dans cette catégorie.

d) Définition de l'étendue du projet

Un atelier de travail est organisé avec les détenteurs, en vue d'apporter des précisions à la définition de l'étendue de projet énoncée dans le scénario 2 de l'étude préliminaire.

Les conclusions de cet atelier sont consignées dans le tableau suivant :

Unité administrative	Processus	Nom du détenteur	Impacts possibles d'un bris de sécurité de l'information	À catégoriser – oui ou non
Direction émission et révocation des permis	Émission des permis	D1	Atteinte à l'image de marque de l'organisme Perte de confiance envers l'organisme Atteinte à la protection des renseignements personnels (PRP) et au respect à la vie privée	Oui
Direction émission et révocation des permis	Révocation des permis	D1	Atteinte à l'image de marque de l'organisme Perte de confiance envers l'organisme Atteinte à la PRP et au respect de la vie privée	Oui
Direction des plaintes	Gestion des plaintes	D3	Perte de confiance envers l'organisme Atteinte à la sécurité des personnes Atteinte à la PRP et au respect de la vie privée	Oui
Direction des enquêtes	Gestion des enquêtes	D2	Atteinte à l'image de marque de l'organisme Perte de confiance envers l'organisme Atteinte à la sécurité des personnes Atteinte à la PRP et au respect de la vie privée	Oui
Direction support à la clientèle	Soutien à la clientèle	D5	Aucun	Non
Direction communications électroniques	Gestion des communications électroniques	D4	Non-conformité à la règlementation en vigueur	Oui

e) Planification du projet

Sur la base de la définition de l'étendue de projet précédemment validée, l'équipe de projet établit le calendrier suivant des réalisations :

Objet de l'atelier	Processus visé	Intervenants	Date et durée de l'atelier	Bien livrable attendu
Identification des objets de catégorisation	Émission des permis Révocation des permis	Équipe de projet Détenteur D1	Le 4 juin 2013 De 13 h à 16 h 30	Formulaire d'identification des objets de catégorisation rempli par chaque détenteur
	Gestion des enquêtes	Équipe de projet Détenteur D2	Le 5 juin 2013 De 13 h à 15 h 30	
	Gestion des plaintes	Équipe de projet Détenteur D3	Le 6 juin 2013 De 13 h à 15 h 30	
	Gestion des communications électroniques	Équipe de projet Détenteur D4	Le 7 juin 2013 De 13 h à 16 h	
Catégorisation des objets de catégorisation identifiés	Émission des permis Révocation des permis	Équipe de projet Détenteur D1	Le 11 juin 2013 De 13 h à 16 h 30	Niveaux d'impact complétés pour chaque formulaire d'identification des objets de catégorisation
	Gestion des enquêtes	Équipe de projet Détenteur D2	Le 12 juin 2013 De 13 h à 15 h 30	
	Gestion des plaintes	Équipe de projet Détenteur D3	Le 13 juin 2013 De 13 h à 15 h 30	
	Gestion des communications électroniques	Équipe de projet Détenteur D4	Le 14 juin 2013 De 13 h à 16 h 30	
Validation des résultats de catégorisation	Tous les processus	Équipe de projet Détenteurs D1, D2, D3 et D4 Responsable des affaires juridiques Responsable de la gestion documentaire Responsable du registre de catégorisation	Le 19 juin 2013 De 13 h à 16 h 30	Formulaire de validation des résultats de catégorisation validé

f) Démarrage du projet

Le chargé de projet communique aux détenteurs le calendrier des ateliers les concernant et les invite à assister à la réunion de démarrage, l'objectif étant d'échanger sur la démarche de catégorisation à adopter.

Étape 3 : Exercice de catégorisation

a) Identification des objets de catégorisation et attribution des niveaux d'impact

En préparation des ateliers de travail planifiés, les détenteurs concernés ont rempli le « formulaire d'identification des objets de catégorisation » pour les processus relevant de leur responsabilité. Ils ont ainsi réalisé leur propre exercice d'identification des objets de catégorisation et d'attribution des niveaux d'impact correspondants.

Ces formulaires remplis ont par la suite été examinés et ajustés lors d'ateliers de travail avec l'équipe de projet. À l'issue de ces ateliers, quatre formulaires ont été remplis :

- ✓ un formulaire pour le détenteur de la Direction émission et révocation des permis;
- ✓ un formulaire pour le détenteur de la Direction des enquêtes;
- ✓ un formulaire pour le Bureau des plaintes;
- ✓ un formulaire pour la Direction des communications électroniques.

Le formulaire d'identification des objets de catégorisation rempli par le détenteur « D2 » pour le processus « gestion des enquêtes » est présenté ci-après.

Secrétariat du Conseil du trésor
Québec

Formulaire d'identification des objets de catégorisation

Ministère ou organisme:	Organisme fictif
Nom détenteur:	D2
Date d'identification:	juillet 2013

Objet de catégorisation	Unité administrative	Processus	Détenteur	Description objet	Type objet	Localisation	Émetteur	Type émetteur	Destinataire	Type destinataire	Exigences spécifiques	Date de catégorisation (jj/mm/aaaa)	Niveau d'impact par processus			Références des justificatifs
													D	I	C	
Demande d'enquête	Direction des enquêtes	Gestion des enquêtes	D2	Demandes d'enquête pour émission de permis, Demandes d'enquêtes pour révocation de permis et demandes d'enquête pour plaintes	Électronique	Base de données de gestion des permis (Serveur XXX)	Émission de permis, Révocation de permis, Gestion des plaintes	Interne			PRP	juil-13	3	3	2	
Résultat d'analyse	Direction des enquêtes	Gestion des enquêtes	D2		Électronique	Base de données de gestion des permis (Serveur XXX)					PRP	juil-13	3	3	3	
Rapport d'enquête	Direction des enquêtes	Gestion des enquêtes	D2	Tests et certificats d'admissibilité de la clientèle, rapports d'enquête pour révocation de permis et rapports d'enquête pour plaintes	Papier	Dossier des enquêtes (Classeur EE)			Émission de permis, Révocation de permis, Gestion des plaintes	Interne	PRP	juil-13	2	4	3	
Dossier des enquêtes	Direction des enquêtes	Gestion des enquêtes	D2		Papier	Classeur EE					PRP	juil-13	3	4	3	
Base de données de renseignements	Direction des enquêtes	Gestion des enquêtes	D2	Toutes les bases de données externes utilisées pour les recherches de renseignements	Électronique	Externe	Entités externes	Partenaire externe			Respect des autorisations convenues	juil-13	3	4	3	

b) Validation des résultats de catégorisation

Une fois les objets de catégorisation identifiés et les niveaux d'impact correspondants attribués pour tous les processus visés par l'exercice de catégorisation, l'équipe de projet a procédé au regroupement des contenus des différents formulaires d'identification dans le « formulaire de validation des résultats de catégorisation », sans remplir les colonnes « D », « I » et « C », correspondant au « niveau d'impact global ».

Lors d'un atelier, l'équipe de projet, en présence de l'ensemble des détenteurs, a procédé à la vérification de la cohérence des niveaux d'impact attribués aux objets de catégorisation utilisés par plusieurs processus.

À l'issue de cet atelier, les colonnes « D », « I » et « C », correspondant au « niveau d'impact global » du « formulaire de validation des résultats de catégorisation » sont remplies et validées. De plus, le chargé de projet a sensibilisé les détenteurs à l'importance de veiller à la validité des résultats de catégorisation, en prêtant particulièrement attention aux cas suivants :

- ✓ modification d'un processus à la suite d'un changement dans la mission de l'organisme, ou de l'ajout ou du retrait d'une ou de plusieurs de ses fonctionnalités;
- ✓ modification apportée aux lois et règlements;
- ✓ ajout ou retrait d'objets de catégorisation;
- ✓ modification de la grille des niveaux d'impact de l'organisme;
- ✓ changement organisationnel significatif.

Il est également convenu de réviser les niveaux d'impact attribués aux objets de catégorisation après une période de quatre ans.

Un extrait du formulaire de validation des résultats de catégorisation est présenté ci-après.

Secrétariat du Conseil du trésor
Québec

Formulaire de validation des résultats de catégorisation

Ministère ou organisme:	Organisme fictif
Équipe de validation:	Équipe de projet, D1, D2, D3, D4
Date de validation:	Juillet 2013

Objet de catégorisation	Unité administrative	Processus	Détenteur	Description objet	Type objet	Localisation	Émetteur	Type émetteur	Destinataire	Type destinataire	Exigences spécifiques	Date de catégorisation (jj/mm/aaaa)	Niveau d'impact par processus			Niveau d'impact global			Références des justificatifs
													D	I	C	D	I	C	
Demande d'enquête	Bureau des plaintes	Gestion des plaintes	D3		Électronique	Base de données de gestion des permis (Serveur XXX)			Gestion des enquêtes	Interne	PRP	juil-13	1	3	3	2	3	3	
Demande d'enquête	Direction des enquêtes	Gestion des enquêtes	D2	Demandes d'enquête pour émission de permis, demandes d'enquête pour révocation de permis et demandes d'enquête pour plaintes	Électronique	Base de données de gestion des permis (Serveur XXX)	Émission de permis, Révocation de permis, Gestion des plaintes	Interne			PRP	juil-13	3	3	2	2	3	3	
Demande d'enquête	Direction Émission et révocation des permis	Émission de permis	D1		Électronique	Base de données de gestion des permis (Serveur XXX)			Gestion des enquêtes	Interne		juil-13	1	3	3	2	3	3	
Demande d'enquête	Direction Émission et révocation des permis	Révocation de permis	D1		Électronique	Base de données de gestion des permis (Serveur XXX)			Gestion des enquêtes	Interne		juil-13	1	3	3	2	3	3	
Rapport d'enquête	Bureau des plaintes	Gestion des plaintes	D3		Papier	Dossier des enquêtes (Classeur EE)	Gestion des enquêtes	Interne			PRP	juil-13	3	3	3	2	4	3	
Rapport d'enquête	Direction des enquêtes	Gestion des enquêtes	D2	Tests et certificats d'admissibilité de la clientèle, rapports d'enquête pour révocation de permis et rapports d'enquête pour plaintes	Papier	Dossier des enquêtes (Classeur EE)			Émission de permis, Révocation de permis, Gestion des plaintes	Interne	PRP	juil-13	2	4	3	2	4	3	
Rapport d'enquête	Direction Émission et révocation des permis	Émission de permis	D1		Papier	Dossier du client (Classeur EP-XX)	Direction des enquêtes	Interne			PRP	juil-13	3	3	3	2	4	3	
Rapport d'enquête	Direction Émission et révocation des permis	Révocation de permis	D1		Papier	Dossier des révocations (Classeur RR)	Direction des enquêtes	Interne			PRP	juil-13	3	3	3	2	4	3	

Étape 4 : Maintien du registre de catégorisation

Les résultats de catégorisation validés sont consignés dans le registre de catégorisation. Il est important de préciser que certaines colonnes du « formulaire de validation des résultats de catégorisation » ne figurent pas dans le registre de catégorisation, puisqu'elles ne sont nécessaires que pour les étapes antérieures de l’exercice.

Il est à noter que les niveaux d’impact à intégrer au registre correspondent à la colonne « niveau d’impact global » du « formulaire de validation des résultats ».

Un extrait du registre de catégorisation résultant de cette étude de cas est présenté ci-après.

Secrétariat du Conseil du trésor
Québec

Registre de catégorisation

Ministère ou organisme:	Organisme fictif
Nom du responsable du registre:	RR1
Date de dernière mise à jour:	Juillet 2013

Objet de catégorisation	Unité administrative	Processus	Détenteur	Description objet	Type objet	Localisation	Exigences spécifiques	Date de catégorisation (jj/mm/aaaa)	Niveau d'impact			Références des justificatifs
									D	I	C	
Avis de décision de révocation de permis	Direction Émission et de la révocation des permis	Révocation de permis	D1		Papier	Dossier des révocations (Classeur RR)		juil-13	1	4	3	
Avis de réponse au plaignant	Bureau des plaintes	Gestion des plaintes	D3		Papier	Dossier des plaintes (Classeur PP)		juil-13	1	4	3	
Base de données de renseignements	Direction des enquêtes	Gestion des enquêtes	D2	Toutes les bases de données externes utilisées pour les recherches de renseignements	Électronique	Externe		juil-13	3	4	3	
Certificats d'émission de permis	Direction Émission et révocation des permis	Émission de permis	D1		Papier	Dossier du client (Classeur EP-XX)		juil-13	1	4	3	
Conditions d'admissibilité à un permis	Direction Émission et révocation des permis	Émission de permis	D1		Électronique	Site Internet (Serveur web)		juil-13	2	3	1	
Contenu à valider	Direction Communications électroniques	Gestion des communications électroniques	D4		Électronique			juil-13	2	3	2	
Contenu diffusé	Direction Communications électroniques	Gestion des communications électroniques	D4		Papier			juil-13	3	3	1	

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique