Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

GUIDE SUR LA CATÉGORISATION DE LA SÉCURITÉ DES SERVICES FONDÉS SUR L'INFONUAGIQUE

ITSP.50.103

Mai 2020

SÉRIE PRATICIENS

Canada

AVANT-PROPOS

L'ITSP.50.103, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique*, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements ou pour des suggestions de modifications, prière de communiquer avec l'équipe des Services à la clientèle du Centre pour la cybersécurité :

Centre d'appel
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 20/05/2020.

APERÇU

Le présent document vise à aider les organisations à catégoriser la sécurité des services fondés sur l'infonuagique. Il facilite également la sélection du profil de contrôle de sécurité qui permettra de protéger l'information et les activités opérationnelles, ainsi que le choix des modèles de déploiement en nuage et de service infonuagique.

La catégorisation de la sécurité est une étape essentielle pour ce qui est d'assurer la protection contre les risques associés à l'utilisation de l'infonuagique. Elle aide les organisations à déterminer les possibles préjudices découlant de la compromission de leurs processus opérationnels ou de leurs biens d'information. Le présent document vise à aider les clients de services infonuagiques à :

- catégoriser la sécurité des services fondés sur l'infonuagique;
- sélectionner le profil de contrôle de sécurité qui permettra de protéger le renseignement commercial;
- sélectionner les modèles de déploiement en nuage et de service infonuagique.

Le présent document et ses annexes :

- passent en revue les termes et les définitions de la catégorisation de la sécurité qui sont énoncés dans l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, du Centre canadien pour la cybersécurité [1][1];
- recommandent un processus de catégorisation de la sécurité susceptible d'aider les organisations à déterminer les niveaux de préjudice prévu qui découlent des compromissions associées à chaque menace;
- recommandent l'approche à adopter pour l'inventaire des processus opérationnels et des biens d'information;
- décrivent la façon de déterminer les préjudices prévus et le niveau de préjudice causé par des menaces de compromission;
- décrivent les facteurs spéciaux qui influent sur le niveau de préjudice prévu;
- décrivent l'approche à adopter pour déterminer les domaines opérationnels;
- décrivent la façon de sélectionner un profil de contrôle de la sécurité infonuagique d'après la catégorie de sécurité de l'activité opérationnelle;
- décrivent la façon de sélectionner les modèles de déploiement en nuage et de service infonuagique d'après la catégorie de sécurité de l'activité opérationnelle;
- fournissent les profils de contrôle de sécurité recommandés pour les catégories de sécurité FAIBLE et MOYEN.

Le présent document fait partie d'une série de documents préparés par le Centre pour la cybersécurité dans le but de promouvoir les services fondés sur l'infonuagique. La catégorisation de la sécurité, la sélection du profil de contrôle de sécurité et le choix des modèles de déploiement en nuage et de service infonuagique constituent les trois premières étapes de l'approche à la gestion des risques à la sécurité infonuagique énoncée dans l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique* [2].

---

[1] Les chiffres entre crochets renvoient aux références citées dans la section Contenu complémentaire du présent document.

TABLE DES MATIÈRES

1 Introduction 7

1.1 Politiques déterminantes 7

1.2 Environnements concernés 8

1.3 Rapport avec la gestion des risques liés à l'infonuagique 8

2 Catégorisation de la Sécurité 10

3 Tableau d'évaluation des préjudices 12

3.1 Détermination des types de préjudices 14

3.2 Niveaux de préjudice et descriptions 16

4 Inventaire des processus opérationnels et des biens d'information 19

4.1 Niveau de détail de l'inventaire 20

4.2 Éléments d'inventaire d'un processus opérationnel et des biens d'information 21

5 Évaluation du préjudice 23

5.1 Définition de préjudice 23

5.2 Éléments de l'évaluation du préjudice 25

5.3 Rapport sur la catégorisation de la sécurité 31

6 Domaines opérationnels 32

6.1 Identification des domaines opérationnels 34

6.2 Services d'entreprise 35

7 Sélection du profil de contrôle de sécurité 37

7.1 Contexte opérationnel 38

7.2 Contexte technique 38

7.3 Contexte de menace 38

7.4 Adaptation 39

7.5 Attributions de contrôles 39

8 Choix des modèles de déploiement en nuage et de service infonuagique 40

8.1 Modèles de déploiement en nuage 42

8.2 Modèles de service infonuagique 45

9 Résumé 47

9.1 Aide et renseignements 47
10 Contenu complémentaire 48
10.1 Liste d'abréviations, d'acronymes et de sigles 48
10.2 Glossaire 49
10.3 Références 50

LISTE DES FIGURES

Figure 1– **Rapport entre la catégorisation de la sécurité et la gestion des risques organisationnels** 8
Figure 2– **Rapport entre la catégorisation de la sécurité et les activités associées au niveau du système d'information** 9
Figure 3 - **Processus de catégorisation de la sécurité : Étape 1 - Élaborer un tableau d'évaluation des préjudices** 12
Figure 4 - **Processus de catégorisation de la sécurité : Étape 2 – Inventaire des activités opérationnelles, des processus et des biens d'information connexes** 19
Figure 5– **Inventaire des processus opérationnels et des biens d'information** 20
Figure 6– **Exemple d'inventaire d'un processus opérationnel et des biens d'information** 21
Figure 7 - **Processus de catégorisation de la sécurité – Étape 3 – Évaluer les préjudices** 23
Figure 8– **Évaluation du préjudice attribuable aux objectifs de sécurité** 24
Figure 9 - **Processus de catégorisation de la sécurité : Étape 4 – Analyse de domaine** 32
Figure 10– **Options des domaines de sécurité** 34
Figure 11– **Sélection du profil de contrôle de la sécurité infonuagique** 37
Figure 12– **Modèles de services infonuagiques** 40
Figure 13– **Choix des modèles de déploiement en nuage et de service infonuagique** 42
Figure 14– **Modèles de déploiement en nuage** 43

LISTE DES TABLEAUX

Tableau 2– **Tableau des préjudices selon l'ITSG-33** 13
Tableau 3– **Exemple de tableau des préjudices pour les organisations du secteur privé** 15
Tableau 4– **Exemple de tableau des préjudices pour les organismes à but non lucratif** 15

Tableau 5– **Définitions des niveaux de préjudice et exemples de descriptions** 16
Tableau 6– **Exemple de tableau des préjudices dûment rempli pour une organisation du secteur privé** 17
Tableau 7– **Exemple de tableau des préjudices dûment rempli pour un organisme à but non lucratif** 18
Tableau 8– **Exemple d'activité opérationnelle** 22
Tableau 9– **Exemple de composante de processus opérationnel** 22
Tableau 10– **Scénarios de défaillance ne s'appliquant pas au type « processus » de l'activité opérationnelle** 26
Tableau 11– **Exemple d'un scénario de défaillance visant l'objectif de confidentialité** 26
Tableau 12– **Exemple de scénario de défaillance visant l'objectif d'intégrité** 27
Tableau 13– **Sélection du niveau de préjudice dans le tableau des préjudices** 28
Tableau 14– **Exemple d'analyse de l'évaluation du préjudice d'un élément d'une activité opérationnelle** 31
Tableau 15– **Exemple de rapport de catégorisation sommaire** 31
Tableau 16– **Valeur maximale d'une évaluation du préjudice** 33

LISTE DES ANNEXES

Annexe A Profil de contrôle de la sécurité infonuagique – FAIBLE 51
Annexe B Profil de contrôle de la sécurité infonuagique – MOYEN 52
Annexe C Résumé des points à considérer à la sélection du modèle de déploiement en nuage 53

1 INTRODUCTION

Le présent document peut aider les organisations à assurer la catégorisation de la sécurité des systèmes d'information, la sélection du profil de contrôle de sécurité requis et le choix des modèles de déploiement en nuage et de service infonuagique de manière à protéger leur information et leurs activités opérationnelles.

Les activités de catégorisation de la sécurité jouent un rôle essentiel dans l'assurance du niveau de protection qui convient aux solutions infonuagiques. Ces solutions infonuagiques proposent aux organisations publiques et privées des options souples, polyvalentes et efficaces en ce qui concerne les technologies de l'information. Les solutions infonuagiques peuvent toutefois faire l'objet de menaces susceptibles de perturber sérieusement les activités opérationnelles. La compromission des services fondés sur l'infonuagique entraîne des coûts de réparation importants et constitue une menace à la disponibilité, à la confidentialité et à l'intégrité des renseignements commerciaux.

Les contrôles de sécurité représentent des éléments essentiels de l'élaboration des services fondés sur l'infonuagique. Alors qu'une protection trop grande peut mener à une hausse des coûts et à une perte de ressources, une protection insuffisante peut faire peser des risques sur l'information et les processus opérationnels. La catégorisation de la sécurité revêt une importance capitale puisqu'elle sert de fondement à la sélection des capacités infonuagiques, du profil de contrôle de sécurité et des modèles de déploiement en nuage et de service infonuagique[2].

Pour obtenir de plus amples renseignements sur l'établissement des contrôles de sécurité visant les architectures sécurisées, prière de consulter l'ITSG-33 [1].

1.1 POLITIQUES DÉTERMINANTES

La nécessité d'avoir recours à la catégorisation de la sécurité est généralement déterminée en fonction des politiques, des directives, des règles ou des normes applicables à chaque organisation[3]. Ces lignes directrices établissent le niveau de protection nécessaire pour contrer les cybermenaces et les vulnérabilités touchant les services fondés sur l'infonuagique. Les publications énumérées ci-dessous sont des documents de référence sur lesquels les organisations peuvent compter pour obtenir les éléments essentiels à la création de politiques et à l'établissement des principes qui orienteront la catégorisation de la sécurité dans le cadre de leurs pratiques et de leurs programmes de gestion des risques liés à la sécurité infonuagique :

- *Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada* [4];
- *Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS)* [5];
- *Politique sur les services et le numérique* [6];

---

[2] *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada* [3]

[3] Les politiques, les directives, les normes, les lignes directrices et les réglementations en matière de sécurité pourraient ne pas toujours utiliser le terme « catégorisation de la sécurité ». De tels documents font souvent mention du niveau de préjudice, de dommage ou de sensibilité. Par exemple, l'un des principes de la LPRPDE stipule que « [l]es renseignements personnels doivent être protégés par des mesures de sécurité correspondant à leur degré de sensibilité » [7].

1.2 ENVIRONNEMENTS CONCERNÉS

L'information fournie dans le présent document d'orientation sur la sécurité concerne les organisations des secteurs privé et public. Le processus de catégorisation de la sécurité décrit peut s'appliquer à l'ensemble des processus opérationnels et aux biens d'information connexes.

Le processus de catégorisation de la sécurité doit tenir compte des processus opérationnels sensibles et des biens d'information d'intérêt national des partenaires du gouvernement du Canada et des autres ordres de gouvernement. Le présent document fait également mention de certaines considérations relatives à la sécurité nationale.

1.3 RAPPORT AVEC LA GESTION DES RISQUES LIÉS À L'INFONUAGIQUE

Les lignes directrices du guide ITSG-33 [1] décrivent un ensemble d'activités menées à deux niveaux distincts de l'organisation : au niveau organisationnel et au niveau du système d'information.

Les activités associées au niveau organisationnel sont intégrées au programme de sécurité de l'organisation pour planifier, gérer, évaluer et améliorer la gestion des risques liés à la sécurité des TI. Comme l'illustre la figure 1, la catégorisation de la sécurité soutient la gestion des risques organisationnels en définissant le contexte opérationnel des profils de contrôle de sécurité.

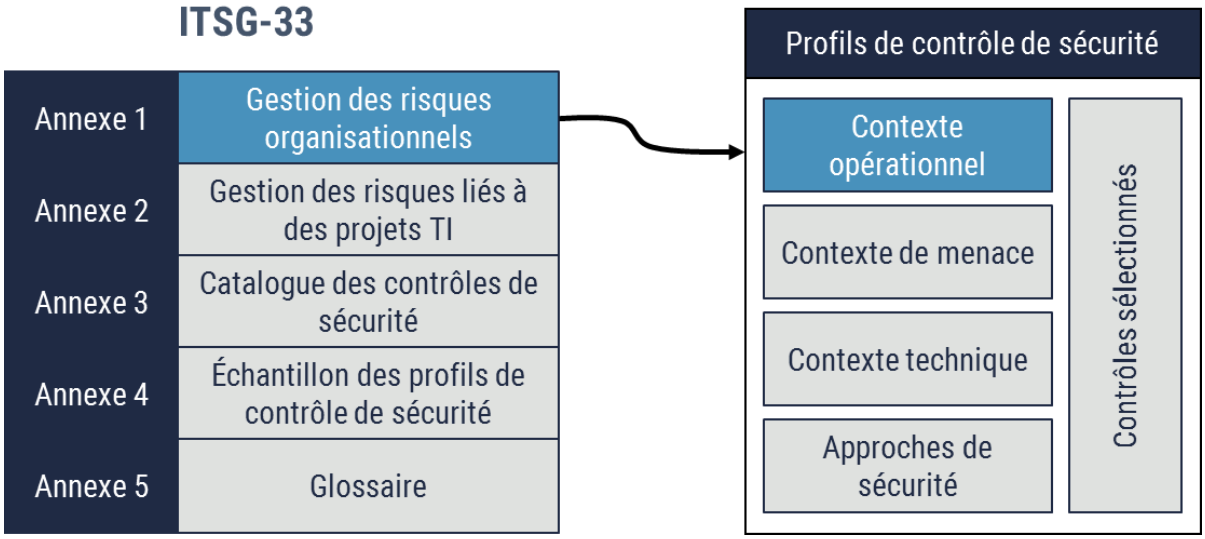


Figure 1– **Rapport entre la catégorisation de la sécurité et la gestion des risques organisationnels**

Les activités associées au niveau du système d'information sont intégrées à un cycle de développement des systèmes (CDS). Ces activités comprennent l'ingénierie de la sécurité, l'évaluation des menaces et des risques, l'évaluation de la sécurité et l'autorisation des systèmes d'information. L'approche à la gestion des risques liés à la sécurité infonuagique du Centre pour la cybersécurité cadre avec les activités associées au niveau du système d'information énoncées dans l'ITSG-33. Comme l'illustre la figure 2, la catégorisation de la sécurité, la sélection du profil de contrôle de la sécurité infonuagique et le choix des modèles de déploiement en nuage et de service infonuagique appuient les trois premières étapes de l'approche à la gestion des risques liés à la sécurité infonuagique. La catégorisation des services fondés sur l'infonuagique offre l'information nécessaire pour déterminer les exigences en matière de sécurité et les contrôles de sécurité auxquels le fournisseur de service infonuagique (FSI) et le client devront se conformer.

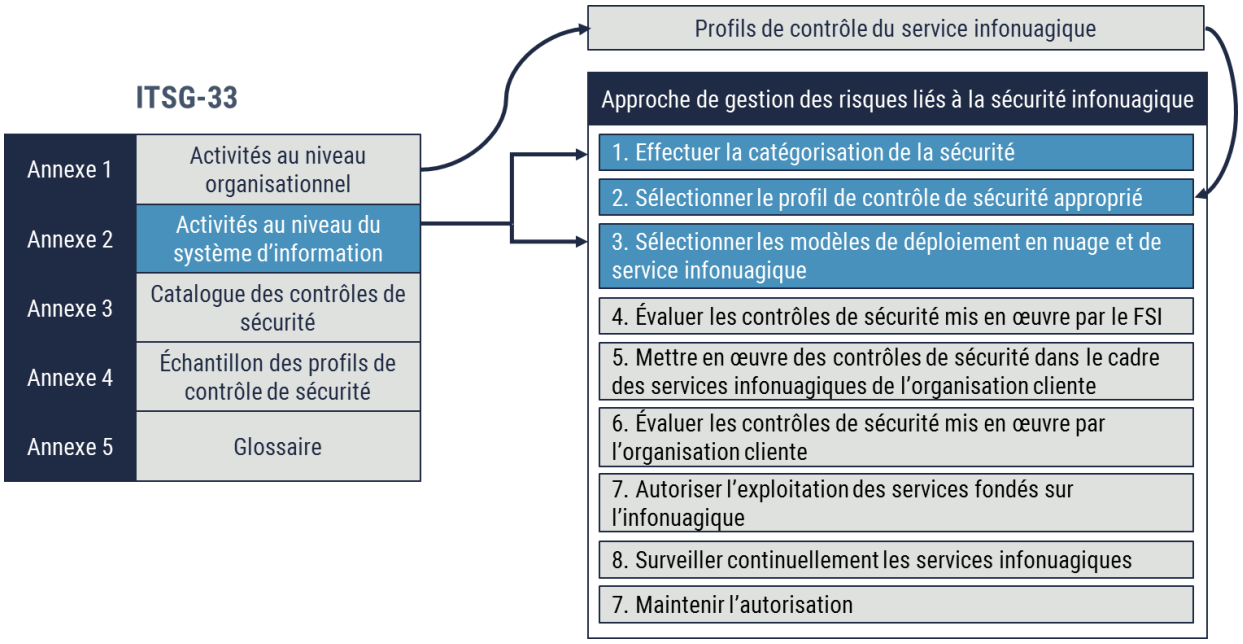


Figure 2– **Rapport entre la catégorisation de la sécurité et les activités associées au niveau du système d'information**

2 CATÉGORISATION DE LA SÉCURITÉ

Le présent document décrit les activités de catégorisation de la sécurité associées à l'adoption des services fondés sur l'infonuagique. Le processus inclut les activités suivantes :

1. élaboration d'un tableau d'évaluation des préjudices;
1. inventaire des activités opérationnelles, des processus et des biens d'information;
2. évaluation des préjudices causés par la défaillance des processus opérationnels et des biens d'information;
3. analyse du domaine.

Par catégorisation de la sécurité, on entend le processus permettant d'identifier le possible préjudice lié à la compromission des processus opérationnels et de l'information connexe. Les activités opérationnelles sont d'abord catégorisées d'après la détermination du préjudice prévu qui découle des menaces de compromission des TI, puis d'après la détermination du niveau de ce préjudice.

Dans le cadre de ce processus, les activités opérationnelles qui seront prises en charge par les services fondés sur l'infonuagique sont établies et classées par catégorie, et le service hérite de la catégorie de sécurité attribuée. Les clients de services infonuagiques choisissent alors le profil de contrôle de sécurité qui convient à la catégorie de sécurité et à leur tolérance au risque. La catégorie de sécurité est également l'un des facteurs pris en compte au moment de sélectionner les modèles de déploiement en nuage et de service infonuagique.

Une catégorie de sécurité exprime les niveaux les plus élevés de préjudices prévus qui découlent des menaces de compromission par rapport aux objectifs de sécurité liés à la confidentialité, l'intégrité et la disponibilité.

Objectifs de sécurité	Définition
Confidentialité	Fait d'être divulgué uniquement aux mandants autorisés
Intégrité	État de ce qui est précis, complet, authentique et intact
Disponibilité	Fait d'être accessible et utilisable intégralement et en temps opportun

Tableau 1- **Objectifs de sécurité**

Les organisations devraient affecter un analyste des activités à la coordination et à la facilitation des activités de catégorisation de la sécurité. L'analyste des activités devrait mener à bien le processus de catégorisation de la sécurité en tant qu'activité globale avec l'appui d'un conseiller en sécurité et la participation des propriétaires des systèmes d'information, des propriétaires de l'information, des dirigeants principaux de l'information, des agents principaux de sécurité de l'information et des propriétaires opérationnels[4]. Les membres de la haute direction et les autres principaux cadres peuvent assurer la surveillance essentielle au processus de catégorisation de la sécurité pour veiller à ce que les

[4] ITSG-33, Annexe 4A, profil de contrôle, conseils supplémentaires RA-2 [1]

activités de gestion des risques liés à l'infonuagique soient menées efficacement et uniformément dans l'ensemble de l'organisation[5]. Si la catégorisation de la sécurité n'est pas effectuée en tant qu'activité globale, l'analyste des activités devra reprendre l'activité pour chaque projet.

[5] NIST 800-60, Vol. 1 – *Guide for Mapping Types of Information and Information Systems to Security Categories* [8]

3 TABLEAU D'ÉVALUATION DES PRÉJUDICES

Pour déterminer le niveau de préjudice, il vaut mieux utiliser un tableau pour se guider.

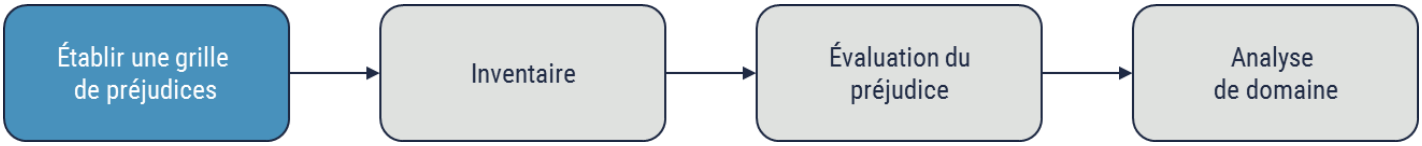


Figure 3 - **Processus de catégorisation de la sécurité : Étape 1 - Élaborer un tableau d'évaluation des préjudices**

« Le tableau 2 est un exemple de tableau de préjudices auquel vous pouvez vous référer afin d'assurer une cohérence lors de l'identification des types de préjudices (répertoriés le long de l'axe vertical) et de leurs niveaux (répertoriés le long de l'axe horizontal). Une description est présentée à des fins de comparaison lorsque le type de préjudice croise les différents niveaux de préjudices ». Les neuf types de préjudices proposés dans l'ITSG-33 décrivent les préjudices graves courants qui sont susceptibles d'avoir un impact sur la mission de l'organisation. Par contre, comme le profil de tolérance au risque diffère d'une organisation à l'autre, un tableau d'évaluation des préjudices ne peut s'appliquer de manière universelle. Les organisations devraient confirmer que l'exemple de tableau des préjudices fourni dans l'ITSG-33 fait mention des types de préjudices les plus susceptibles d'avoir une incidence sur la confidentialité, l'intégrité ou la disponibilité de leurs activités opérationnelles. Si le tableau ne tient pas compte des types de préjudices prévus et des critères de tolérance aux risques, elles devraient créer leur propre tableau d'évaluation des préjudices.

Type de préjudice	Description et niveau				
	Très faible	Faible	Moyen	Élevé	Très élevé
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, entraves publiques	Émeute	Actes de sabotage à l'égard de biens essentiels (p. ex. infrastructure essentielle)	Émeute générale ou actes de sabotage nécessitant l'imposition de la loi martiale
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Préjudice physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse, traumatisme psychologique	Maladie mentale ou physique	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress ou inconfort	Incidence sur la qualité de vie	Sécurité financière compromise	s.o.
Perte financière pour des entreprises canadiennes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	s.o.
Perte financière pour le gouvernement du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement des programmes	Incidence sur les résultats des programmes	Viabilité des programmes compromise	Viabilité des programmes essentiels compromise
Préjudice causé à l'économie canadienne	s.o.	s.o.	Incidence sur le rendement	Perte de compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Préjudice causé à la réputation du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Perte de la confiance du public	Embarras (au Canada ou à l'étranger)	Relations fédérales-provinciales compromises	Relations diplomatiques et internationales compromises
Perte de la souveraineté canadienne	s.o.	s.o.	Entrave à l'établissement de politiques gouvernementales importantes	Entraves à l'application efficace de la loi Cessation des activités du gouvernement	Perte de la souveraineté territoriale

Tableau 2– **Tableau des préjudices selon l'ITSG-33**

3.1 DÉTERMINATION DES TYPES DE PRÉJUDICES

La première étape de la création d'un tableau des préjudices consiste à déterminer les types de préjudices les plus susceptibles d'avoir une incidence sur les fonctions essentielles ou la réputation de l'organisation. On peut déterminer les types de préjudices en passant en revue les évaluations des répercussions, les évaluations des facteurs relatifs à la vie privée, les évaluations des risques opérationnels et les évaluations des menaces et des risques préalablement effectuées. L'examen des instruments réglementaires, tels les lois, les politiques et les règlements, peut également s'avérer utile, puisque la non-conformité à ces exigences réglementaires peut entraîner des pénalités ou des sanctions, et mener à un accroissement du préjudice.[6]

Si elles ne peuvent se référer à de tels documents, les organisations peuvent définir les types de préjudices en se basant sur les objectifs organisationnels et les énoncés de rendement indiqués dans les plans d'activités et les rapports sur le rendement.

Les types de préjudices comprennent, entre autres :

- la perte de réputation;
- l'atteinte à la vie privée;
- des amendes pour infraction aux réglementations (gouvernementales);
- les pénalités contractuelles (non-respect des contrats existants);
- une atteinte à la satisfaction des clients;
- la perte de propriété intellectuelle;
- la perte de revenus;
- une perte en matière de part de marché;
- la hausse des coûts d'exploitation;
- la hausse des exigences en matière de personnel;
- la perte de capacité essentielle;
- la perte d'avantage concurrentiel;
- la perte de la confiance des actionnaires;
- la hausse des frais juridiques;
- la perte de vie;
- un danger à la santé;
- d'autres types de préjudices.

[6] ITSG-33 [1], Annexe 1, page 37.

Après avoir passé en revue les évaluations des répercussions sur les opérations, les évaluations des facteurs relatifs à la vie privée et les autres rapports sur les risques opérationnels, les organisations sont en mesure de déterminer les types de préjudices qui s'appliquent à elles. Les tableaux 3 et 4 décrivent les types de préjudices applicables, respectivement, à une organisation du secteur privé et à un organisme à but non lucratif. Les types de préjudices applicables sont indiqués dans un tableau des préjudices qui illustre plus fidèlement les préjudices pouvant découler de la compromission de ces organisations.

Type de préjudice	Niveau de préjudice		
	Faible	Moyen	Élevé
Préjudice financier			
Infraction au règlement			
Atteinte à la réputation			
Atteinte à la vie privée			
Dommage à la propriété intellectuelle			

Tableau 3– **Exemple de tableau des préjudices pour les organisations du secteur privé**

Type de préjudice	Niveau de préjudice		
	Faible	Moyen	Élevé
Atteinte à la vie privée			
Préjudice financier			
Atteinte à la réputation			
Préjudice aux bénéficiaires			
Infraction au règlement			

Tableau 4– **Exemple de tableau des préjudices pour les organismes à but non lucratif**

3.2 NIVEAUX DE PRÉJUDICE ET DESCRIPTIONS

La deuxième étape de l'élaboration d'un tableau des préjudices consiste à déterminer les descriptions de chaque niveau de préjudice. Les descriptions décrivent les critères de sélection pour chacun des niveaux de préjudice correspondant à tous les types de préjudices. La détermination des descriptions exige une bonne compréhension de la définition de ces niveaux. Le tableau 5 propose des définitions et des exemples de chacun des niveaux de préjudice.

	Niveau de préjudice		
	Faible	Moyen	Élevé
Définition	Le préjudice possible est FAIBLE si la divulgation non autorisée, la modification ou la perte des accès à l'information ou aux services utilisés par le secteur d'activités ne causerait pas, selon toute vraisemblance, de préjudice ou ne causerait qu'un préjudice limité aux personnes ou à l'organisation.	Le préjudice possible est MOYEN si la divulgation non autorisée, la modification ou la perte des accès à l'information ou aux services utilisés par le secteur d'activités causerait, selon toute vraisemblance, un préjudice grave à une personne et à une organisation, ou un préjudice limité à un groupe de personnes.	Le préjudice possible est ÉLEVÉ si la divulgation non autorisée, la modification ou la perte des accès à l'information ou aux services utilisés par le secteur d'activités causerait, selon toute vraisemblance, un préjudice extrêmement grave à une personne et à une organisation, ou un préjudice grave à un groupe de personnes.
Exemples de description	• Incidence faible sur les bénéfices annuels • Perte mineure résultant de la vente • Manquement mineur à la conformité • Atteinte à la vie privée d'une personne • Incidence sur le rendement des programmes • Stress • Préjudice physique • Désobéissance civile • Perte de confiance	• Incidence importante sur les bénéfices annuels • Perte de comptes importants • Défection des clients • Manquement évident à la conformité • Atteinte à la vie privée de centaines de gens • Incidence sur les résultats des programmes • Détresse, traumatisme psychologique • Incidence sur la qualité de vie • Émeutes • Embarras (au Canada ou à l'étranger) • Incidence sur la compétitivité des entreprises	• Faillite • Dommages à la marque • Manquement à la conformité très médiatisé • Atteinte à la vie privée de milliers ou millions de gens • Incidence sur le rendement des programmes • Maladie mentale ou physique • Actes de sabotage • Atteinte à la réputation • Incidence sur la viabilité commerciale

Tableau 5– **Définitions des niveaux de préjudice et exemples de descriptions**

Une organisation du secteur privé et un organisme à but non lucratif ont déterminé les descriptions à attribuer à chaque niveau de préjudice en se basant sur les exemples fournis dans les tableaux 3 et 4. Une fois remplis, les tableaux 6 et 7 peuvent être utilisés par chacun d'entre eux pour soutenir les activités de catégorisation de la sécurité. Il sera ainsi possible d'assurer l'uniformité du processus de sélection du niveau de préjudice.

Type de préjudice	Niveau de préjudice		
	Faible	**Moyen**	**Élevé**
Préjudice financier	• Incidence faible sur les bénéfices annuels • Perte mineure résultant de la vente	• Incidence importante sur les bénéfices annuels	• Faillite
Infraction au règlement	• Sanction mineure	• Sanction importante	• Dommages à la marque • Dépréciation des noms commerciaux • Perte de comptes importants
Atteinte à la réputation	• Perte de confiance	• Perte de comptes importants	• Dommages à la marque • Dépréciation des noms commerciaux
Atteinte à la vie privée	• Stress • Atteinte à la vie privée d'une personne	• Atteinte à la vie privée de centaines de gens	• Atteinte à la vie privée de milliers de gens
Dommage à la propriété intellectuelle	Perte potentielle d'avantage concurrentie	• Incidence sur la compétitivité des entreprises	• Incidence sur la viabilité commerciale

Tableau 6– **Exemple de tableau des préjudices dûment rempli pour une organisation du secteur privé**

Type de préjudice	Niveau de préjudice		
	Faible	**Moyen**	**Élevé**
Atteinte à la vie privée	• Stress • Atteinte à la vie privée d'une personne	• Atteinte à la vie privée de centaines de gens	• Atteinte à la vie privée de milliers de gens
Préjudice financier	• Incidence faible sur le financement	• Incidence importante sur le financement	• Faillite
Atteinte à la réputation	• Perte de confiance	• Perte de donateurs importants	• Dommages à la marque
Préjudice aux bénéficiaires	• Incidence sur le rendement des programmes	• Incidence sur les résultats des programmes	• Viabilité des programmes compromise
Infraction au règlement	• Sanction mineure	• Sanction importante	• Dommages à la marque • Perte de donateurs importants

Tableau 7– **Exemple de tableau des préjudices dûment rempli pour un organisme à but non lucratif**

4 INVENTAIRE DES PROCESSUS OPÉRATIONNELS ET DES BIENS D'INFORMATION

À la deuxième étape du processus, le client détermine les processus opérationnels et les biens d'information associés à l'activité opérationnelle prise en charge par le service fondé sur l'infonuagique.

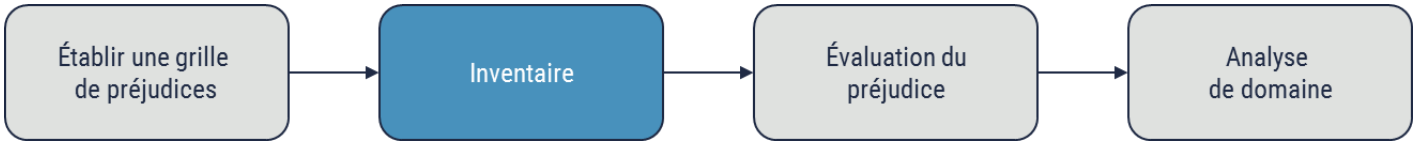


Figure 4 - **Processus de catégorisation de la sécurité : Étape 2 – Inventaire des activités opérationnelles, des processus et des biens d'information connexes**

Lors de l'inventaire, il est primordial que les conseillers en sécurité sollicitent l'appui de la collectivité des analystes des activités au sein de l'organisation. Le rôle des conseillers en sécurité est de mettre en place des groupes de discussion dans la mesure du possible, de décrire la tâche à accomplir, de souligner l'importance de leurs contributions, ainsi que de consigner les résultats obtenus et de les valider.

Cette activité exigera plusieurs niveaux de préparation. Si les activités opérationnelles sont mal documentées, il pourrait être nécessaire de faire appel à plusieurs groupes de discussion pour brosser un portrait homogène et fidèle de l'ensemble des activités opérationnelles. Dans le cas des vastes organisations comportant plusieurs programmes, on ne pourra mener à bien le processus d'inventaire qu'en le divisant en fonction des programmes. Les groupes de discussion pourraient être inutiles si les activités opérationnelles sont bien documentées et comprises. Dans certains cas, les processus opérationnels et les biens d'information seront bien documentés, actuels, validés et facilement transférés. Dans d'autres, il peut être possible de tirer des déductions à ce sujet en consultant la documentation.

Les sources suivantes permettront de déterminer et de décrire les processus opérationnels et les biens d'information connexes :

- analyses de rentabilisation;
- concept d'opérations;
- spécifications opérationnelles fonctionnelles;
- documentation de l'architecture d'entreprise qui inclut normalement une description suffisamment détaillée;
- des processus opérationnels et des biens d'information;
- discussions ou entrevues avec des analystes fonctionnels et d'autres représentants;
- des collectivités opérationnelles concernées.

Les ministères du gouvernement du Canada peuvent consulter les sources suivantes :

- le Rapport sur les plans et les priorités (RPP);
- l'architecture d'alignement des programmes (AAP);
- les Comptes publics du Canada.

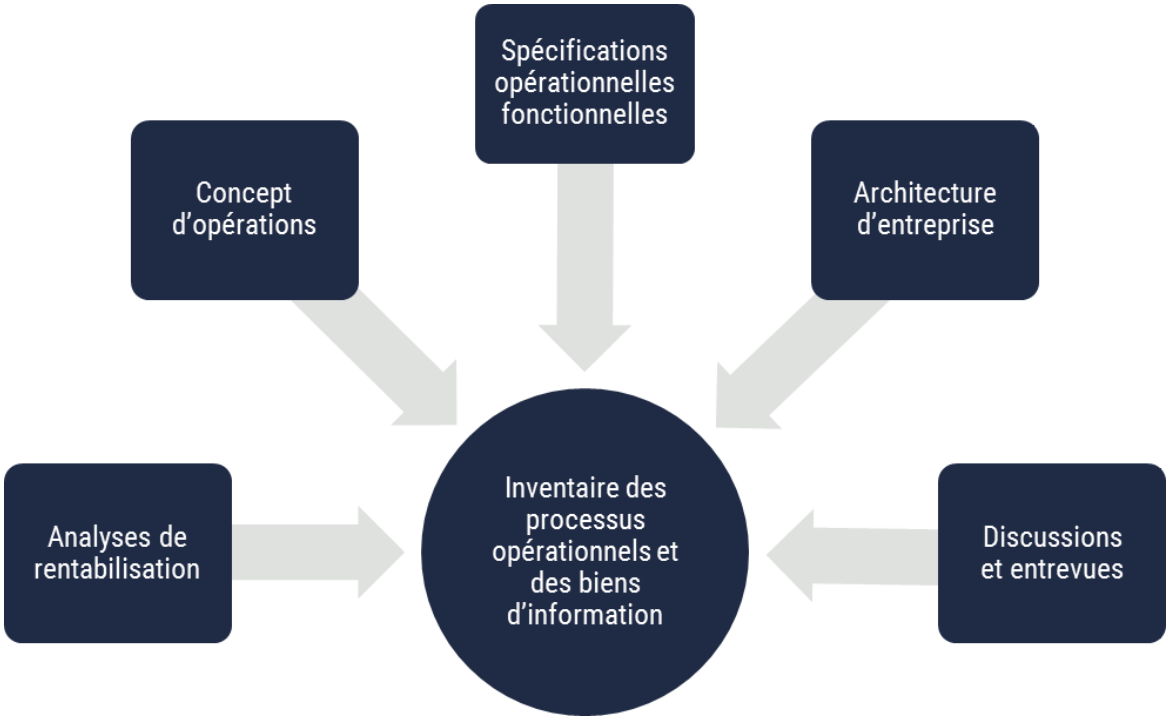


Figure 5– **Inventaire des processus opérationnels et des biens d'information**

Prendre l'inventaire des processus opérationnels et des biens d'information est une étape clé du processus visant à déterminer les conséquences de la compromission des services fondés sur l'infonuagique pour les organisations qui en dépendent.

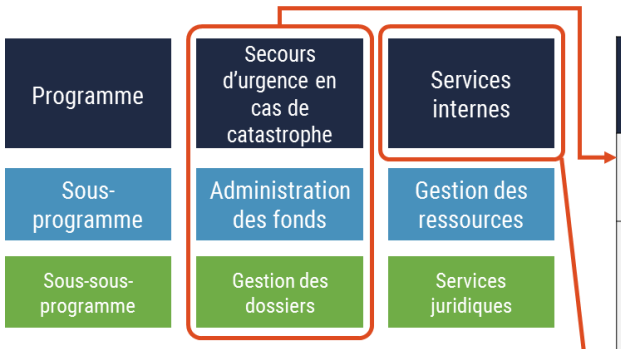
4.1 NIVEAU DE DÉTAIL DE L'INVENTAIRE

La détermination du niveau de détail de l'inventaire est un des enjeux associés au processus d'inventaire. L'ITSG-33 [1] définit les grandes lignes de l'activité opérationnelle afin d'offrir à chaque organisation la souplesse nécessaire pour décrire plus fidèlement leurs activités opérationnelles. Les organisations établissent typiquement le niveau de détails du processus opérationnel et des biens d'information en fonction de facteurs courants, comme la taille de l'organisation, l'ampleur de ses activités et le niveau de risque de ses opérations.

Qu'il soit effectué à un niveau général ou hautement détaillé, l'inventaire fournit des observations utiles sur la catégorisation de la sécurité. Alors que l'inventaire détaillé peut s'avérer utile pour orienter les investissements en sécurité vers la composante la plus critique des processus opérationnels, il est également sensible aux changements apportés à ces processus opérationnels. Par ailleurs, un niveau général d'inventaire permettra d'établir les exigences de sécurité au niveau des programmes et des sous-programmes sans qu'elles soient nécessairement touchées par le processus opérationnel.

Dans le cas de vastes organisations comportant plusieurs programmes, on ne peut effectuer l'inventaire des processus opérationnels et des composantes de ces processus opérationnels qu'en le divisant en programme, en sous-programme ou en sous-sous-programme. Il est ainsi possible d'offrir à ces organisations le niveau de détail nécessaire pour établir les exigences de sécurité tant au niveau de la composante du processus opérationnel qu'au niveau du programme.

La figure 6 donne un exemple d'inventaire basé sur les initiatives opérationnelles, les missions et les mandats documentés d'une organisation.



Programme	Sous-programme	Sous-sous-programme	Processus opérationnel	Composante du processus opérationnel
Secours d'urgence en cas de catastrophe	Administration des fonds	Gestion des dossiers	Ouverture d'un nouveau dossier	Réception de la demande et ouverture du nouveau dossier
			Ouverture d'un nouveau dossier	Renseignements personnels du demandeur
			Ouverture d'un nouveau dossier	Renseignements non personnels du demandeur
			Ouverture d'un nouveau dossier	Évaluation de l'admissibilité au paiement d'urgence
			Ouverture d'un nouveau dossier	Approbation du paiement d'urgence
			Paiement	*Voir Service de paiement*
		Recherche et analyse comparative	Recherche et analyse comparative	Réalisation de la recherche
			Recherche et analyse comparative	Données de recherche
			Recherche et analyse comparative	Données de l'analyse comparative
	Gestion des appels		Gestion des demandes d'appel	Réception et traitement des demandes d'appel
			Gestion des demandes d'appel	Renseignements relatifs au dossier d'appel
Services internes	Gestion des ressources	Ressources financières	Service de paiement	Émission du paiement d'urgence

Figure 6– **Exemple d'inventaire d'un processus opérationnel et des biens d'information**

4.2 ÉLÉMENTS D'INVENTAIRE D'UN PROCESSUS OPÉRATIONNEL ET DES BIENS D'INFORMATION

Quel que soit le niveau de détail observé lors de l'inventaire des processus opérationnels et des biens d'information, chacun des processus et des biens d'information est caractérisé par les éléments suivants :

- le nom du processus opérationnel ou une description (ou encore un numéro);
- une composante du processus opérationnel;
- une description de la composante;
- un type;
- des remarques.

Une activité opérationnelle peut correspondre à un processus ou à un groupe de processus qui appuie les objectifs de l'organisation. Dans le tableau 8, par exemple, trois processus opérationnels ont été relevés dans le sous-sous-programme Gestion des dossiers :

- ouverture d'un nouveau dossier;
- examen du dossier;
- paiement.

Inventaire des processus opérationnels et des biens d'information		
Sous-sous-programme	**Processus opérationnel**	**Composante du processus opérationnel**
Gestion des dossiers	Ouverture d'un nouveau dossier	Réception de la demande et ouverture du nouveau dossier
	Examen du dossier	Approbation du paiement d'urgence
	Paiement	*Voir Service de paiement*

Tableau 8– **Exemple d'activité opérationnelle**

Chacun des processus opérationnels et des biens d'information est décrit en fonction de la ou des composantes ayant été décrites. On en détermine ensuite le type. Dans le tableau 9, le type de la composante **Renseignements personnels du demandeur** est *Information*, et celui de **Réception de la demande et ouverture du nouveau dossier** est *Processus*. Si la situation l'exige, les organisations devraient définir d'autres types de composantes à inclure dans l'inventaire.

Inventaire des processus opérationnels et des biens d'information					
Sous-sous-programme	**Processus opérationnel**	**Composante du processus opérationnel**	**Description de la composante**	**Type**	**Remarques**
Gestion des dossiers	Ouverture d'un nouveau dossier	Réception de la demande et ouverture du nouveau dossier	Processus qui consiste à recevoir une demande pour l'allocation de fonds d'urgence, à créer un dossier et à obtenir des renseignements sur le demandeur	Processus	
	Ouverture d'un nouveau dossier	Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille touchés, nature de l'urgence, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Information	

Tableau 9– **Exemple de composante de processus opérationnel**

Les analystes des activités devraient indiquer dans la colonne *Remarques* les suppositions formulées, la source des données d'inventaire et toute autre information permettant de mettre en contexte chacun des éléments de l'inventaire.

5 ÉVALUATION DU PRÉJUDICE

La troisième étape du processus de sécurisation de la sécurité est l'évaluation du préjudice. L'objectif de l'évaluation du préjudice est de déterminer le préjudice prévu lié aux menaces de compromission pour chaque processus opérationnel et chaque bien d'information déterminé à l'étape précédente.

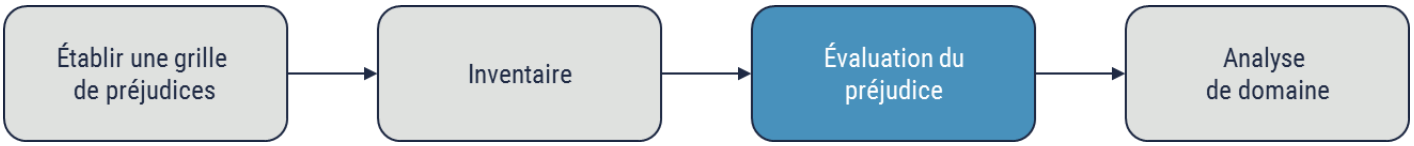


Figure 7 - **Processus de catégorisation de la sécurité – Étape 3 – Évaluer les préjudices**

Le processus d'évaluation du préjudice devrait être confié à des équipes multidisciplinaires composées de représentants des secteurs responsables des opérations, des questions juridiques, de l'accès à l'information, de la sécurité et du respect de la vie privée. Le propriétaire opérationnel ou son délégué devrait également faire partie de ces équipes, de même que le responsable de l'autorisation (si cette tâche n'a pas été confiée au propriétaire opérationnel) et les représentants et analystes opérationnels de chaque programme ou secteur d'activités. Dans la présente, on désigne ce groupe par le nom collectif « comité d'évaluation ».

5.1 DÉFINITION DE PRÉJUDICE

On définit un préjudice en fonction de l'étendue et de l'ampleur des dommages pouvant résulter de la compromission de biens de TI d'une organisation. Un préjudice peut causer des dommages tant aux intérêts nationaux qu'aux intérêts non nationaux. Les dommages causés aux intérêts nationaux concernent la sécurité et la stabilité sociopolique et économique du Canada. Les dommages causés aux intérêts non nationaux concernent la sûreté, la santé et le bien-être des personnes, ainsi que la situation financière et la réputation des citoyens et des organisations canadiennes. Au sein du gouvernement du Canada, les ministères et les organismes catégorisent et classent les informations en fonction des dommages qui pourraient résulter d'un compromis. Cet exercice de catégorisation de la sensibilité des informations se reflètent dans l'attribution d'étiquettes de classification et de protection telles que NON CLASSIFIÉ, CONFIDENTIEL, SECRET, TRÈS SECRET et PROTÉGÉ A, PROTÉGÉ B, PROTÉGÉ C. Dans le secteur privé, le préjudice est généralement associé aux dommages causés à la rentabilité et à la réputation des entreprises. Dans ce contexte, les informations peuvent être étiquetées comme étant confidentielles ou exclusives pour refléter leur niveau de sensibilité.

De plus, les organisations gouvernementales et privées peuvent bénéficier de l'utilisation du protocole TLP (Traffic Light Protocol) pour assurer et encourager un meilleur partage d'informations. Bien qu'il ne soit pas une échelle de niveaux de préjudices en tant que telle, le TLP consiste en un code d'étiquettes de couleur (rouge, ambré, vert et blanc) utilisé pour indiquer comment et avec qui les informations devraient être partagées.

Tel qu'il est illustré à la figure 8, le préjudice associé à chacune des composantes d'une activité opérationnelle est évalué par rapport à trois objectifs de sécurité : la confidentialité, l'intégrité et la disponibilité.

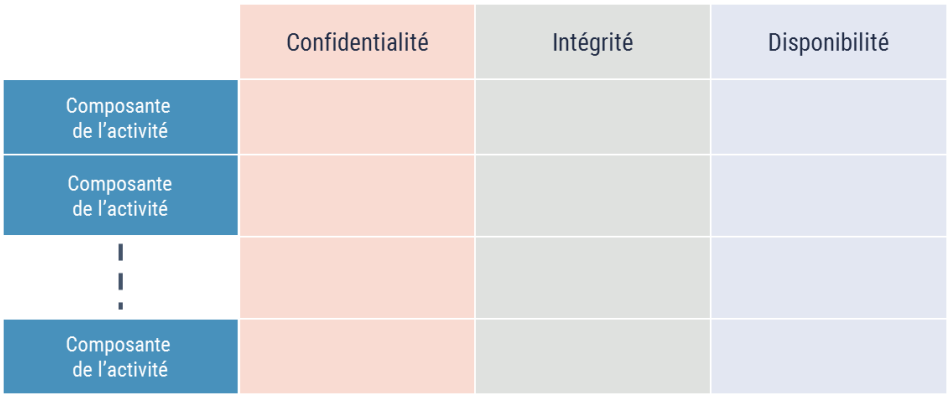


Figure 8– **Évaluation du préjudice attribuable aux objectifs de sécurité**

Une définition des niveaux de préjudice FAIBLE, MOYEN et ÉLEVÉ est fournie à la section 2.3[7].

[7] Bien que cette publication et le profil de contrôle de la sécurité infonuagique connexe classent les niveaux de préjudice comme étant FAIBLE, MOYEN et ÉLEVÉ au sein du gouvernement du Canada, on fait appel à des étiquettes de confidentialité pour exprimer un non-respect d'un objectif de sécurité lié à la confidentialité. NON CLASSIFIÉ correspond à un niveau de préjudice FAIBLE, PROTÉGÉ B à un niveau de préjudice MOYEN et PROTÉGÉ B à un niveau de préjudice ÉLEVÉ.

5.2 ÉLÉMENTS DE L'ÉVALUATION DU PRÉJUDICE

Une évaluation du préjudice inclut les étapes suivantes :

1. **Scénario de défaillance** : détermination d'une ou plusieurs situations où un préjudice pourrait être causé advenant la défaillance d'un processus opérationnel ou d'une composante;
2. **Type et niveau de préjudice** : sélection du type et du niveau de préjudice dans le tableau des préjudices;
3. **Facteurs spéciaux** : modification du niveau de préjudice pour tenir compte de l'incidence d'un facteur spécial;
4. **Analyse** : proposition de remarques, d'analyses et de justifications supplémentaires pour le type et niveau sélectionnés.

> NOTA : Les quatres étapes de l'évaluation du préjudice sont effectuées par rapport à chacun des objectifs de sécurité : la confidentialité, l'intégrité et la disponibilité.

5.2.1 DÉTERMINATION DU SCÉNARIO DE DÉFAILLANCE

Le premier élément de l'évaluation du préjudice consiste à documenter les possibles scénarios de défaillance pour chaque composante des activités opérationnelles. La détermination des scénarios de défaillance vise à tenir compte des différentes façons dont une composante peut faire l'objet d'une défaillance et causer un préjudice. Plus d'un scénario de défaillance peut être attribué à chacune des composantes d'une activité opérationnelle.

Bien que l'évaluation du préjudice puisse être effectuée pour chacun des objectifs de sécurité (confidentialité, intégrité et disponibilité), la détermination du scénario de défaillance associé à la confidentialité ne s'applique généralement pas au type « Processus » des composantes de l'inventaire des activités opérationnelles. Dans un tel cas, le comité d'évaluation devrait établir que le scénario de défaillance ne s'applique pas, tel qu'il est indiqué dans le tableau 10. Il importe de souligner qu'il pourrait être nécessaire de faire exception à cette règle si un processus est confidentiel ou comporte des étapes confidentielles (p. ex., le processus relatif à la préparation d'une recette exclusive).

Inventaire des processus opérationnels et des biens d'information					
Processus opérationnel	**Composante du processus opérationnel**	**Description de la composante**	**Type**	**Remarques**	**Scénario de défaillance (en contexte)**
Ouverture d'un nouveau dossier	Réception de la demande et ouverture du nouveau dossier	Processus qui consiste à recevoir une demande pour l'allocation de fonds d'urgence, à créer un dossier et à obtenir des renseignements sur le demandeur	Processus		Ne s'applique pas
Ouverture d'un nouveau dossier	Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille touchés, nature de l'urgence, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Information		

Tableau 10– **Scénarios de défaillance ne s'appliquant pas au type « processus » de l'activité opérationnelle**

Le tableau 11 décrit l'un des scénarios de défaillance les plus courants : la divulgation non autorisée d'information à une personne aux intentions malveillantes.

Inventaire des processus opérationnels et des biens d'information					
Processus opérationnel	**Composante du processus opérationnel**	**Description de la composante**	**Type**	**Remarques**	**Scénario de défaillance (en contexte)**
Ouverture d'un nouveau dossier	Réception de la demande et ouverture du nouveau dossier	Processus qui consiste à recevoir une demande pour l'allocation de fonds d'urgence, à créer un dossier et à obtenir des renseignements sur le demandeur	Processus		Ne s'applique pas
Ouverture d'un nouveau dossier	Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille touchés, nature de l'urgence, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Information		Divulgation d'information personnelle (dont le NAS) à une personne non autorisée aux intentions malveillantes

Tableau 11 – **Exemple d'un scénario de défaillance visant l'objectif de confidentialité**

Le comité d'évaluation répète le processus jusqu'à ce que les scénarios de défaillance aient été déterminés pour toutes les composantes des activités opérationnelles et tous les objectifs de sécurité. Le tableau 12 donne un exemple de scénario de défaillance visant l'objectif d'intégrité d'une composante du processus.

Inventaire des processus opérationnels et des biens d'information					
Processus opérationnel	**Composante du processus opérationnel**	**Description de la composante**	**Type**	**Remarques**	**Scénario de défaillance (en contexte)**
Ouverture d'un nouveau dossier	Réception de la demande et ouverture du nouveau dossier	Processus qui consiste à recevoir une demande pour l'allocation de fonds d'urgence, à créer un dossier et à obtenir des renseignements sur le demandeur	Processus		Erreur ou omission dans la collecte et le traitement de l'information
Ouverture d'un nouveau dossier	Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille touchés, nature de l'urgence, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Information		

Tableau 12– **Exemple de scénario de défaillance visant l'objectif d'intégrité**

5.2.2 DÉTERMINATION DU TYPE ET DU NIVEAU DE PRÉJUDICE

Le comité d'évaluation devrait utiliser un tableau des préjudices pour déterminer le niveau possible de préjudice des composantes des activités opérationnelles. On retrouve à la section 2 du présent document la description d'un processus que le comité d'évaluation peut suivre pour mettre en place un tableau des préjudices adapté au niveau de tolérance de son organisation en matière de préjudice.

Une fois le tableau des préjudices mis en place par le comité d'évaluation en fonction du niveau de tolérance de l'organisation, on peut utiliser ce tableau pour uniformiser la détermination du niveau de préjudice. Tel qu'il est illustré dans le tableau 13, on détermine le niveau de préjudice associé à une composante d'une activité opérationnelle donnée de la façon suivante :

1. sélection du type de préjudice associé au scénario de défaillance (axe vertical du tableau des préjudices);
2. sélection, sur l'axe horizontal, de la description qui représente le plus fidèlement l'évaluation de ce qui risque de survenir advenant la réalisation du scénario de défaillance;
3. sélection du niveau de préjudice associé à la description choisie dans le tableau des préjudices.

La description et le type et niveau de préjudice obtenus lors de ce processus devraient être inscrits dans l'inventaire et serviront à déterminer la catégorie de sécurité globale des services infonuagiques qui soutiennent les processus opérationnels.

Type de préjudice	Description et niveau					
	Très faible	Faible	Moyen	3	Élevé	Très élevé

Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, entraves publiques	Émeute	Actes de sabotage à l'égard de biens essentiels (p. ex. infrastructure essentielle)	Émeute générale ou actes de sabotage nécessitant l'imposition de la loi martiale
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Préjudice physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes 1	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse, traumatisme psychologique 2	Maladie mentale ou physique	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress ou inconfort	Incidence sur la qualité de vie	Sécurité financière compromise	s.o.
Perte financière pour des entreprises canadiennes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	s.o.
Perte financière pour le gouvernement du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement des programmes	Incidence sur les résultats des programmes	Viabilité des programmes compromise	Viabilité des programmes essentiels compromise
Préjudice causé à l'économie canadienne	s.o.	s.o.	Incidence sur le rendement	Perte de compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Préjudice causé à la réputation du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Perte de la confiance du public	Embarras (au Canada ou à l'étranger)	Relations fédérales-provinciales compromises	Relations diplomatiques et internationales compromises
Perte de la souveraineté canadienne	s.o.	s.o.	Entrave à l'établissement de politiques gouvernementales importantes	Entraves à l'application efficace de la loi Cessation des activités du gouvernement	Perte de la souveraineté territoriale

Tableau 1– **Sélection du niveau de préjudice dans le tableau des préjudices**

5.2.3 FACTEURS SPÉCIAUX

L'élément suivant de l'évaluation du préjudice consiste à tenir compte des facteurs spéciaux qui pourraient forcer le comité d'évaluation à modifier le niveau de préjudice déterminé à l'étape précédente. Les facteurs spéciaux pourraient exiger une analyse plus poussée du niveau de préjudice prévu, notamment, le regroupement, l'inférence et l'interdépendance.

5.2.3.1 REGROUPEMENT

On peut attribuer un niveau de préjudice distinct à chaque processus opérationnel et bien d'information individuel. Toutefois, le niveau d'un préjudice résultant de la compromission d'un ensemble de processus et de biens d'information, considérés globalement, peut être supérieur à celui attribué à chaque préjudice individuel.

Par regroupement, on entend une situation où un ensemble de biens peut être catégorisé à un niveau de sensibilité plus élevé que les parties qu'il forme en raison du préjudice accru que pourrait causer toute compromission à ce bien. Il s'agit, en d'autres mots, d'une situation où les répercussions sur les opérations de la compromission d'un ensemble de biens sont plus importantes que les répercussions d'une compromission individuelles. Le regroupement s'applique généralement à la confidentialité, mais, dans certains cas, il peut également s'appliquer à la disponibilité et à l'intégrité.

Par exemple, la divulgation sans autorisation d'un seul dossier du personnel peut causer un certain embarras à l'intéressé et amener le public à s'inquiéter de la capacité de l'organisation de protéger les renseignements personnels. Si tous les dossiers des ressources humaines d'une grande société étaient divulgués de façon inopportune, cependant, les répercussions négatives pourraient être considérablement pires.

Du point de vue de la confidentialité, le regroupement a deux dimensions :

1. La sensibilité a tendance à augmenter avec le nombre de données ajoutées à un dossier;
2. La sensibilité du répertoire a tendance à augmenter avec le nombre de dossiers réunis dans un fichier ou une base de données.

La valeur de confidentialité de l'ensemble peut être plus grande que celle de ses diverses parties en raison du préjudice accru que causerait leur divulgation sans autorisation.

Le regroupement s'applique également aux valeurs de disponibilité et d'intégrité. Par exemple, la destruction d'un bien, comme un seul serveur, peut avoir des conséquences clairement définies, alors que la perte de tout un parc serait beaucoup plus sérieuse. La modification sans autorisation d'un seul dossier ou la corruption complète d'une grande base de données serait l'équivalent sur le plan de l'intégrité.

Lorsqu'elles traitent des informations regroupées, les organisations doivent réévaluer chaque dimension de la sécurité en tenant compte des nouveaux préjudices qui pourraient résulter du regroupement. Au sein des organisations, il conviendra d'envisager la confidentialité, l'intégrité et la disponibilité du point de vue du préjudice causé aux intérêts nationaux et non nationaux.

Comme il est difficile d'évaluer le préjudice aux intérêts nationaux associé à un ensemble de composantes opérationnelles, il conviendra de prendre en compte l'avis stratégique des organismes responsables.

5.2.3.2 INFÉRENCE

Dans certains cas, l'analyse de renseignements catégorisés à un niveau de sensibilité donné peut faire en sorte qu'un individu informé tire des conclusions de l'analyse et y donne suite sans se douter qu'il peut compromettre des renseignements plus sensibles. Par exemple, des dossiers de personnel catégorisés MOYEN aux fins de confidentialité peuvent contenir de l'information qui donne certaines indications sur le rôle de l'employé et, par le fait même, sur la mission ou la capacité opérationnelle de l'organisme d'attache – information qui peut compromettre les intérêts organisationnels.

Les organisations devraient tenir compte de la sensibilité non seulement des renseignements catégorisés, mais aussi de celle d'autres informations associées qui pourraient être inférées et ensuite exploitées par un auteur de menaces.

5.2.3.3 INTERDÉPENDANCE

Les interdépendances font en sorte que la perte ou la dégradation d'un processus opérationnel et de son information peut influer sur les autres processus et biens d'information. Le but de l'analyse des interdépendances est de déterminer s'il est possible qu'un effet de cascade important résultant de la compromission d'un processus opérationnel ou d'une information ait une incidence sur un autre processus et une autre information. Le niveau d'un préjudice résultant de la perte en cascade d'un élément peut être supérieur à celui attribué à n'importe lequel des éléments individuels, comme dans le cas du regroupement. On compte divers types d'interdépendance : l'interdépendance physique (le matériel produit par une infrastructure et utilisé par une autre infrastructure), l'interdépendance géographique (un couloir commun) et l'interdépendance logique (par l'entremise des marchés financiers).

5.2.4 ANALYSE

Après avoir évalué le niveau de préjudice, le praticien de la sécurité devrait s'efforcer de consigner l'essentiel des échanges. Les tierces parties seront ainsi en mesure de comprendre le motif des décisions liées à la sélection du type et du niveau de préjudice.

Dans cette analyse, le praticien de la sécurité pourrait, par exemple, apporter une justification, documenter les facteurs spéciaux qui ont permis de déterminer le niveau de préjudice, tenir compte de toute considération de nature urgente ou faire mention des règles ou politiques auxquelles se conformer.

Le tableau 14 propose un exemple de documentation des activités d'analyse d'un élément des activités opérationnelles.

Entorse à la disponibilité			
Quel type de préjudice une entorse à la disponibilité pourrait-elle causer?	**Quelle est l'ampleur du préjudice prévu?**	**Exemple de préjudices à ce niveau (représentatif)**	**Analyse**
Préjudice psychologique causé aux personnes	Faible	Stress	Le traitement efficace et opportun des demandes de paiement d'urgence est essentiel à la réalisation des résultats du

			programme. Toutefois, d'autres opérations de secours devraient veiller à répondre aux besoins fondamentaux des sinistrés.

Tableau 2– **Exemple d'analyse de l'évaluation du préjudice d'un élément d'une activité opérationnelle**

5.3 RAPPORT SUR LA CATÉGORISATION DE LA SÉCURITÉ

Une fois l'évaluation des préjudices effectuée, le comité d'évaluation peut choisir de produire un rapport de catégorisation complet ou sommaire afin de communiquer les résultats.

Le comité d'évaluation devrait documenter et accepter officiellement les résultats de l'activité de catégorisation de la sécurité. Les résultats peuvent être combinés comme suit dans un rapport sur la catégorisation de la sécurité :

- une brève description des processus opérationnels et des biens d'information connexes;
- une description des préjudices prévus découlant des compromissions associées à chaque menace;
- les niveaux de préjudices prévus en ce qui a trait à la confidentialité, l'intégrité et la disponibilité;
- la justification de l'attribution des niveaux de préjudice;
- la catégorie de sécurité associée à chaque activité opérationnelle;
- la catégorie de sécurité du service fondé sur l'infonuagique;
- une déclaration d'acceptation explicite de la catégorie de sécurité par le propriétaire du service fondé sur l'infonuagique.

Le tableau 15 présente un exemple de rapport de catégorisation sommaire.

Domaine opérationnel			Catégorie de sécurité		
			Confidentialité	Intégrité	Disponibilité
Programme de secours d'urgence en cas de catastrophe			Moyen	Faible	Faible
Répartition des composantes		Type			
1	Réception de la demande et ouverture du nouveau dossier	Processus		Faible	Faible
2	Renseignements personnels du demandeur	Information	Moyen	Faible	Faible

Tableau 35– **Exemple de rapport de catégorisation sommaire**

6 DOMAINES OPÉRATIONNELS

La quatrième étape de la catégorisation de la sécurité est la détermination du domaine opérationnel. Un domaine opérationnel est un environnement dans lequel une organisation mène des activités qui soutiennent des objectifs communs. Le profil de contrôle de la sécurité d'un domaine est associé à un domaine opérationnel particulier plutôt qu'à l'ensemble d'une organisation. De nombreux rapports pourraient être produits selon la méthode utilisée par le comité d'évaluation pour procéder à la catégorisation.

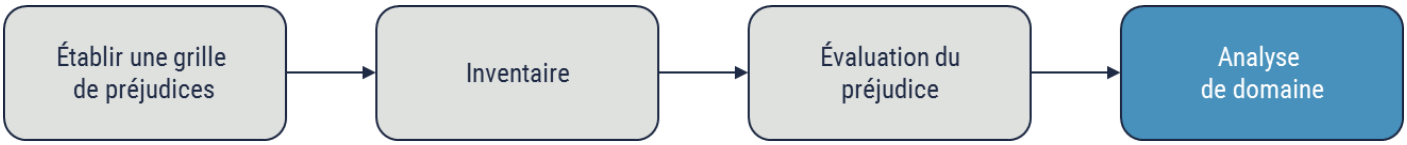


Figure 9 - **Processus de catégorisation de la sécurité : Étape 4 – Analyse de domaine**

À la fin du processus de catégorisation, le comité d'évaluation aura un ou plusieurs tableaux de processus opérationnels et de biens d'information. Le préjudice associé à chaque processus ou bien d'information sera évalué par rapport à la confidentialité, l'intégrité et la disponibilité.

Si toutes les activités doivent être prises en charge par un seul système d'information dans un domaine unique, on utilisera la catégorie globale correspondant à la valeur maximale[8] (le niveau le plus élevé de préjudice dans chacune des colonnes qui composent le tableau 16).

[8] Pour une description détaillée du concept de valeur maximale, se reporter à la section 3.2.1 du document intitulé *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada* [3].

Entorse à la confidentialité				
Scénario de défaillance	**Préjudice raisonnable causé par une entorse à la confidentialité**	**Niveau de préjudice prévu**	**Exemple de préjudice**	**Analyse**
Divulgation d'information personnelle (dont le NAS) à une personne non autorisée aux intentions malveillantes	Préjudice psychologique causé aux personnes	**Moyen**	Détresse, traumatisme psychologique	Pourrait causer de la détresse et mener à des pertes financières graves
Divulgation d'information à une personne non autorisée aux intentions malveillantes	Préjudice psychologique causé aux personnes	**Faible**	Stress	Certains renseignements personnels pourraient être divulgués, mais pas le NAS et les détails des comptes bancaires
Entorse à l'intégrité				
Scénario de défaillance	**Préjudice raisonnable causé par une entorse à l'intégrité**	**Niveau de préjudice prévu**	**Exemple de préjudice**	**Analyse**
Erreur ou omission dans la collecte et le traitement de l'information	Préjudice psychologique causé aux personnes	**Moyen**	Détresse, traumatisme psychologique	Un paiement pourrait être retardé, suscitant ou nourrissant un sentiment de détresse. Pourrait également occasionner de la douleur et de la souffrance.
L'information recueillie est inexacte ou incomplète	Préjudice psychologique causé aux personnes	**Moyen**	Détresse, traumatisme psychologique	Voir ci-dessus
Entorse à la disponibilité				
Scénario de défaillance	**Préjudice raisonnable causé par une entorse à la disponibilité**	**Niveau de préjudice prévu**	**Exemple de préjudice**	**Analyse**
Incapacité de traiter une demande initiale ou délai de traitement	Préjudice psychologique causé aux personnes	**Faible**	Stress	Le traitement efficace et opportun des demandes de paiement d'urgence est essentiel à la réalisation des activités opérationnelles
Perte ou destruction d'information	Préjudice psychologique causé aux personnes	**Moyen**	Détresse, traumatisme psychologique	Voir ci-dessus

Tableau 46– **Valeur maximale d'une évaluation du préjudice**

Une seule catégorie de sécurité peut être associée à un domaine opérationnel. Les contrôles utilisés dans le profil de contrôle de la sécurité d'un domaine sont choisis de manière à répondre à une catégorisation unique (p. ex. {M, M, M}, {M, F,

F}). Par conséquent, si les organisations disposent de plusieurs rapports de catégorisation pour les activités opérationnelles liées à un domaine donné, elles devront réfléchir à la pertinence de les regrouper.

6.1 IDENTIFICATION DES DOMAINES OPÉRATIONNELS

En règle générale, la meilleure approche consiste à attribuer une valeur maximale à un domaine opérationnel si l'objectif est de regrouper différents rapports de catégorisation. Par contre, le fait d'attribuer la valeur maximale au niveau de catégorisation sous-entend l'application et l'utilisation de plus amples contrôles de sécurité, ce qui se traduit par des coûts plus élevés. Tel qu'il est indiqué à la figure 10, on peut gérer comme suit les activités ayant une catégorisation inhabituellement élevée :

- **Option A :** En supposant le même contexte de menace, développer un profil de contrôle de sécurité propre à l'exception et soutenir les activités opérationnelles qui ont recours à un système d'information sur mesure;
- **Option B :** En supposant le même contexte de menace, développer un profil de contrôle de sécurité pour la catégorisation la plus élevée et mettre en place les autres activités opérationnelles sur le même système d'information (SI).

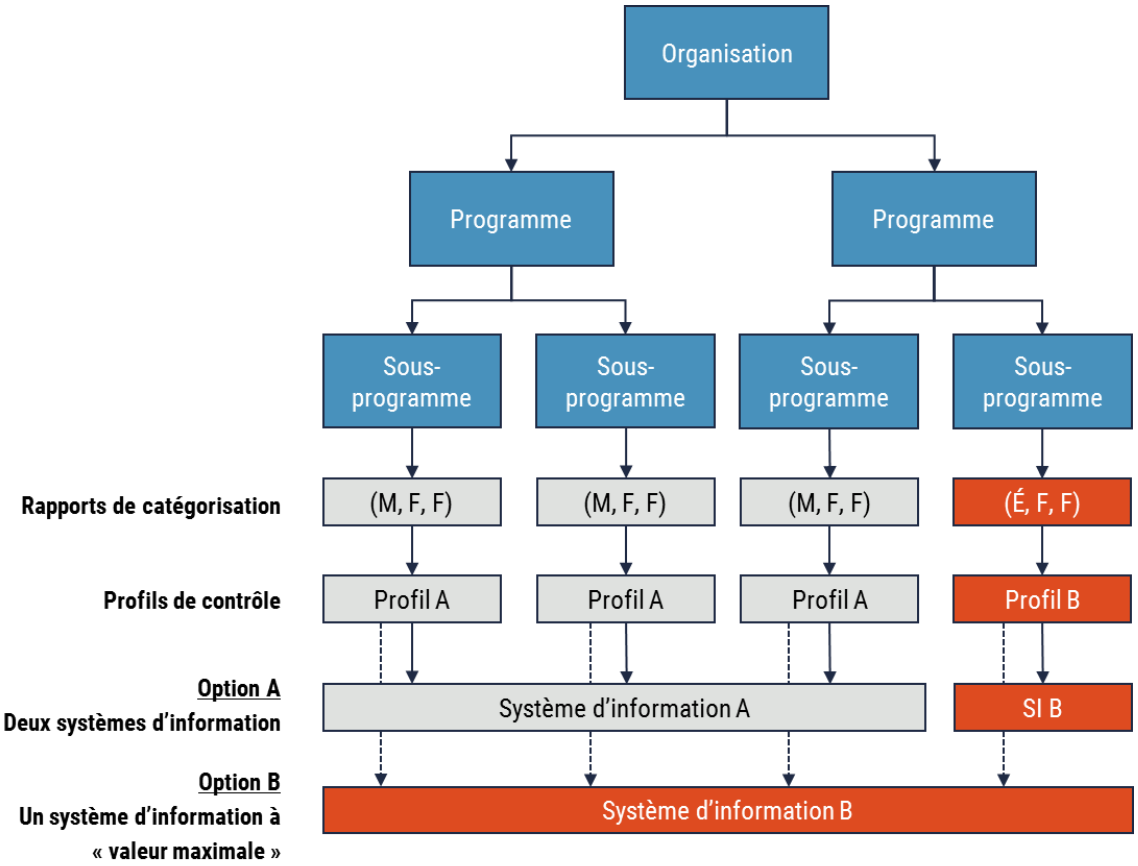


Figure 10– **Options des domaines de sécurité**

6.2 SERVICES D'ENTREPRISE

L'architecture d'entreprise pourrait permettre d'identifier les applications qui seront utilisées par les différents secteurs d'activités (p. ex. courrier électronique, RH, approvisionnement). Les fournisseurs de services pourraient également cibler plusieurs secteurs ou domaines en vue de leur offrir leurs solutions (p. ex. plateforme en tant que service [PaaS pour *Platform as a Service*] ou logiciel en tant que service [SaaS pour *Software as a Service*]). Ils pourraient faire appel à une approche par extraction (*pull*) ou par envoi de données (*push*) pour assurer la catégorisation de la sécurité.

6.2.1 APPROCHE PAR EXTRACTION DE DONNÉES

Si l'approche par extraction de données est adoptée, le fournisseur de service tente d'obtenir l'information relative à la catégorisation de la sécurité auprès de chaque client potentiel, et développe un profil susceptible d'offrir le niveau de préjudice prévu le plus élevé. Recueillir l'information relative à la catégorisation de la sécurité auprès de plusieurs organisations exige du temps et une planification minutieuse. Ces efforts devraient être déployés au lancement du projet en vue de déterminer :

- la faisabilité;
- la portée;
- le calendrier et les enveloppes budgétaires.

Les organisations qui adoptent l'approche par extraction de données devraient tenir compte de ce qui suit :

- veiller à ce que tous les secteurs utilisent le même modèle de catégorisation;
- veiller à ce que tous les secteurs évaluent le préjudice de façon uniforme;
- convenir qu'il pourrait être impossible de déterminer la catégorisation globale en raison du budget ou du calendrier. La portée proposée pourrait nécessiter d'importants changements (p. ex., exclusion de certaines organisations, obtention de fonds additionnels).

6.2.2 APPROCHE PAR ENVOI DE DONNÉES

Si l'approche par envoi de données est adoptée, le fournisseur de service établit la catégorisation de l'application ou du service, et développe un profil susceptible d'offrir le niveau de préjudice prévu le plus élevé. La catégorisation de l'application ou du service est une décision opérationnelle. Dans le cas des applications ou services non essentiels, les organisations peuvent évaluer leurs besoins par rapport aux solutions offertes et appliquer la catégorisation de la façon appropriée. En ce qui concerne les applications ou services essentiels (p. ex., les initiatives organisationnelles), les organisations doivent évaluer leurs besoins par rapport au service offert et déterminer quels sont les secteurs à risque.

Les organisations qui adoptent l'approche par envoi de données devraient tenir compte de ce qui suit :

- Les fournisseurs doivent fournir **tous** les artéfacts d'assurance de la sécurité sans quoi les organisations clientes ne seront pas en mesure de déterminer quels sont les secteurs de risques résiduels;
- Dans le cas des applications ou services essentiels, il est important que la détermination de la catégorie de la sécurité repose sur une compréhension approfondie du domaine opérationnel (ce que l'approche par extraction de données permet de faire).

7 SÉLECTION DU PROFIL DE CONTRÔLE DE SÉCURITÉ

Les profils de contrôle de sécurité associés aux services fondés sur l'infonuagique sont inspirés des profils de référence mentionnés à l'annexe 4 de l'ITSG-33 du Centre pour la cybersécurité. Les profils de contrôle de la sécurité infonuagique établissent les contrôles de sécurité recommandés que les FSI et les organisations clientes devraient mettre en œuvre pour la catégorie de sécurité évaluée associée à chacun des domaines opérationnels respectifs. Le profil de contrôle sélectionné sert aussi de base à l'évaluation des contrôles de sécurité.

Les clients de services infonuagiques devraient sélectionner un des profils de contrôle de la sécurité infonuagique développés par le Centre pour la cybersécurité, qui sont mentionnés aux annexes A et B de la présente. Au moment de sélectionner un profil de contrôle de la sécurité infonuagique, les responsables des projets devraient effectuer les tâches suivantes avec le soutien des praticiens de la sécurité[9] :

- valider l'applicabilité du contexte opérationnel;
- valider l'applicabilité du contexte technique;
- valider l'applicabilité du contexte de menace;
- personnaliser les contrôles de sécurité associés à leur secteur de responsabilité selon leurs besoins.

Le contexte opérationnel documenté pour chacun des profils de contrôle de la sécurité infonuagique détermine la catégorie de la sécurité qui peut être prise en charge par le profil. Après avoir effectué la catégorisation de la sécurité des activités opérationnelles, les clients de services infonuagiques sélectionnent le profil de contrôle de sécurité qui convient à la catégorie de sécurité du domaine opérationnel applicable.

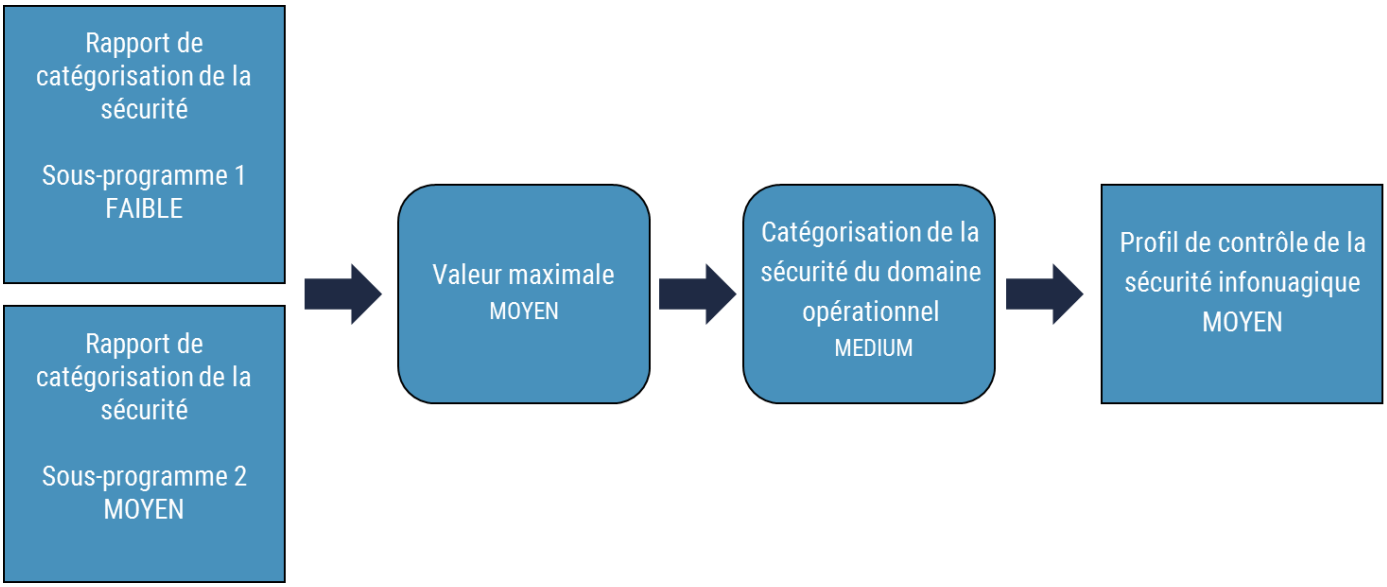


Figure 11– **Sélection du profil de contrôle de la sécurité infonuagique**

[9] *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada* [3]

7.1 CONTEXTE OPÉRATIONNEL

Les deux profils de contrôle de la sécurité infonuagique que l'on retrouve dans les annexes peuvent être appliqués aux services fondés sur l'infonuagique qui appuient les activités opérationnelles dont la catégorie de sécurité est FAIBLE et MOYEN. Dans le cas des activités opérationnelles ayant une catégorie de sécurité ÉLEVÉ, les organisations devraient communiquer avec le Centre pour la cybersécurité pour obtenir le profil de contrôle de la sécurité infonuagique recommandé.

7.2 CONTEXTE TECHNIQUE

Le contexte technique des profils de contrôle de la sécurité infonuagique mentionnés dans l'annexe est déterminé par les modèles de déploiement en nuage et de service infonuagique, les solutions offertes par le FSI et les services fondés sur l'infonuagique de l'organisation.

Le contexte technique est largement dicté par les services infonuagiques offerts par le FSI et se manifeste sous une multitude de formes. Les profils de contrôle de la sécurité infonuagique ne recommandent et n'excluent aucune technologie. Ils devraient généralement s'adapter à tout contexte technique proposé par les FSI dans les services infonuagiques qu'ils offrent[10].

7.3 CONTEXTE DE MENACE

Certains FSI publics offrent des services de sécurité de l'information ayant un niveau d'assurance suffisant pour assurer une défense constante contre les menaces supérieures à celles que posent les auteurs de menaces délibérées 4 (Md4), les menaces accidentelles 3 (Ma3) et les menaces naturelles, tel qu'il est stipulé dans l'ITSG-33 [1]. En d'autres mots, le niveau Md4 correspond aux auteurs de menace ayant une attitude défavorable au risque, comme les pirates informatiques sophistiqués qui possèdent les connaissances, les capacités et l'expérience nécessaires pour personnaliser et utiliser les outils à leur disposition pour exploiter les faiblesses des systèmes, trouver des vulnérabilités inconnues ou développer des exploits susceptibles d'exposer les organisations. Les menaces accidentelles 3 (Ma3) et les risques naturels comprennent des incidents tels que l'interruption des services de télécommunications, des pannes de courant prolongées, des inondations localisées et des dommages aux installations lors de séismes.

À ce titre, les organisations dont les activités doivent être protégées contre les auteurs de menaces délibérées 4 (Md4) et les menaces accidentelles 3 (Ma3) pourraient être tenus d'adapter de façon plus poussée les profils de contrôle mentionnés aux annexes, d'accepter des niveaux de risque résiduel plus élevés ou de sélectionner un profil de contrôle différent. Pour obtenir de plus amples conseils, les organisations doivent communiquer avec le Centre pour la cybersécurité.

---

[10] *Profil de mesures de sécurité pour les services du GC fondés sur l'informatique en nuage du gouvernement du Canada*

7.4 ADAPTATION

Les profils de contrôle de la sécurité infonuagique mentionnés dans la présente représentent les contrôles de sécurité de référence pour ce qui est d'assurer la protection des activités opérationnelles de l'organisation. L'adaptation du profil de contrôle de la sécurité infonuagique est nécessaire pour tenir compte des menaces uniques, des limitations techniques, des exigences opérationnelles, des lois, des réglementations ou des politiques.

Les organisations devraient envisager de combler les lacunes inhérentes aux contrôles de sécurité du FSI en mettant en place leurs propres contrôles ou en faisant appel à un autre FSI. Les organisations ayant recours au modèle d'infrastructure en tant que service (IaaS pour *Infrastructure as a Service*) seront en mesure de combler plus facilement ces lacunes avec leurs propres contrôles que celles qui utilisent le modèle SaaS[11]. Il est à noter que les lacunes inhérentes en matière de contrôles de sécurité pour le modèle PaaS sont semblables à celles que l'on retrouve avec le modèle IaaS.

Le praticien de la sécurité devrait adapter le profil de contrôle de sécurité de manière à tenir compte de menaces, d'exigences et de lacunes uniques. Il doit, pour ce faire, incorporer des contrôles de compensation, apporter des améliorations aux contrôles ou mettre en place des paramètres de contrôle propres à l'organisation. Le praticien de la sécurité devrait fournir une justification des activités d'adaptation qui ont été menées et motiver les décisions qui ont été prises à ce sujet.

Les profils de contrôle de la sécurité infonuagique mentionnés dans les annexes A et B tiennent compte des attributions de contrôles. Ces attributions déterminent qui est responsable des exigences de sécurité du profil de contrôle (le FSI ou le client). Il est également possible de procéder à l'attribution de contrôles par modèle de service.

7.5 ATTRIBUTIONS DE CONTRÔLES

Dans les annexes A et B, un « X » sous la colonne K, L, M ou N des feuilles de calcul indiquent dans quelle mesure le FSI ou le client du service infonuagique est responsable des exigences de sécurité énoncées dans le profil de contrôle de sécurité sélectionné.

Les responsabilités du client pour ce qui est des modèles IaaS et PaaS comprennent les exigences de sécurité associées aux systèmes qui sont configurés et gérés par le client dans le nuage, ainsi que tous les systèmes d'information que le client utilise pour accéder aux services infonuagiques connexes, les gérer ou en assurer la protection. Dans le cas du modèle SaaS, les responsabilités du client comprennent les exigences de sécurité associées à tous les systèmes d'information que le client utilise pour accéder aux services infonuagiques connexes et les gérer.

Les responsabilités du FSI en ce qui concerne chacun des modèles de service comprennent également les exigences de sécurité des services pris en charge. Par exemple, les responsabilités du FSI pour ses SaaS comprennent les exigences de sécurité associées aux systèmes basés sur les modèles IaaS et PaaS prenant en charge ce SaaS. Or, il est probable que d'autres évaluations existantes des services de soutien puissent être réutilisées pour déterminer si le FSI a exercé ses responsabilités relatives à la STI pour le service pris en charge.

---

[11] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4.0 [9].

8 CHOIX DES MODÈLES DE DÉPLOIEMENT EN NUAGE ET DE SERVICE INFONUAGIQUE

Lors de l'adoption de services infonuagiques, les organisations clientes doivent déterminer les modèles de déploiement en nuage et de service infonuagique qui conviennent à leurs services TI. Les modèles de déploiement en nuage décrivent le rapport entre le FSI et les clients du service infonuagique. Le NIST a identifié quatre modèles de déploiement en nuage : public, privé, communautaire et hybride. La figure 12 illustre les trois modèles de service infonuagique définis par le NIST : l'infrastructure en tant que service, la plateforme en tant que service et le logiciel en tant que service. Les modèles de déploiement en nuage et de service infonuagique sont décrits en détail dans le document intitulé *The NIST Definition of Cloud Computing* [10].

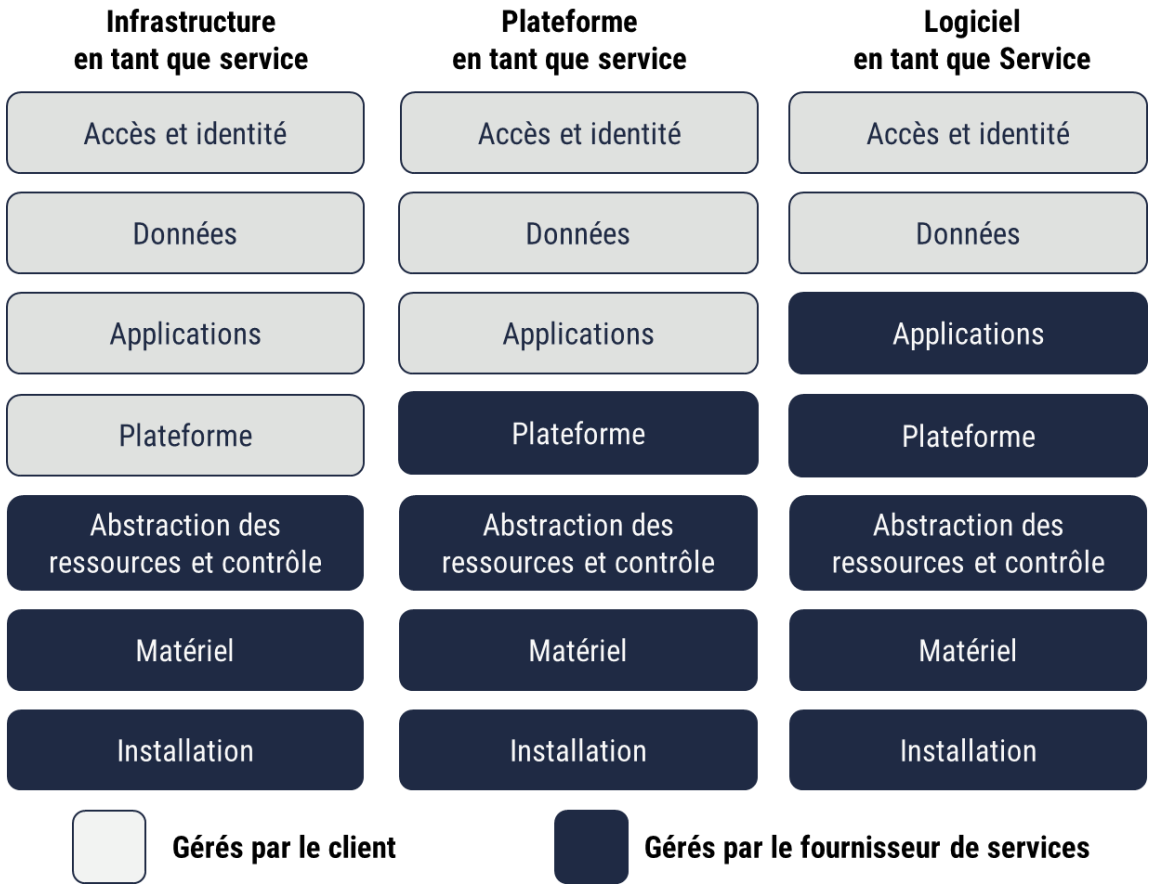


Figure 12– **Modèles de services infonuagiques**

Le choix des modèles de déploiement en nuage et de service infonuagique sera fondé sur la nature des services, le niveau de contrôle que l'organisme client veut conserver ainsi que le degré d'expertise et de maturité de l'organisme client dans le cadre de l'exploitation et de la maintenance des environnements des systèmes d'information fondés sur l'infonuagique.

L’information recueillie à l’étape de la catégorisation de la sécurité aide le client du service infonuagique à sélectionner les modèles de déploiement en nuage et de service infonuagique qui conviennent le mieux à son expertise interne et au niveau d’assurance qu’il est tenu de respecter. Les organisations devraient sélectionner un FSI et un modèle de service qui satisfont aux exigences en matière de catégorie de sécurité ayant été évaluées.

Les organisations devraient sélectionner les modèles de déploiement et de service qui permettent de corriger les lacunes associées à la mise en œuvre des contrôles de sécurité du FSI avec un minimum d’adaptation des contrôles et de contrôles de compensation. Tel qu’il est indiqué à la section 6.1, les organisations ayant recours au modèle IaaS seront en mesure de combler plus facilement les lacunes des contrôles de sécurité du FSI en mettant en place leurs propres contrôles que celles qui utilisent le modèle SaaS.

Tel qu’il est indiqué à la figure 13, les organisations devraient sélectionner ou déterminer le modèle de déploiement en nuage et de service infonuagique à utiliser en tenant compte des points suivants :

- les stratégies adoptées par l’organisation pour ses systèmes d’information;
- les capacités des services infonuagiques du FSI et les lacunes dans les contrôles de sécurité;
- la catégorie de sécurité du processus opérationnel qui sera pris en charge par le service infonuagique;
- les exigences relatives au profil de contrôle de sécurité sélectionné;
- les autres aspects des charges de travail des systèmes d’information.

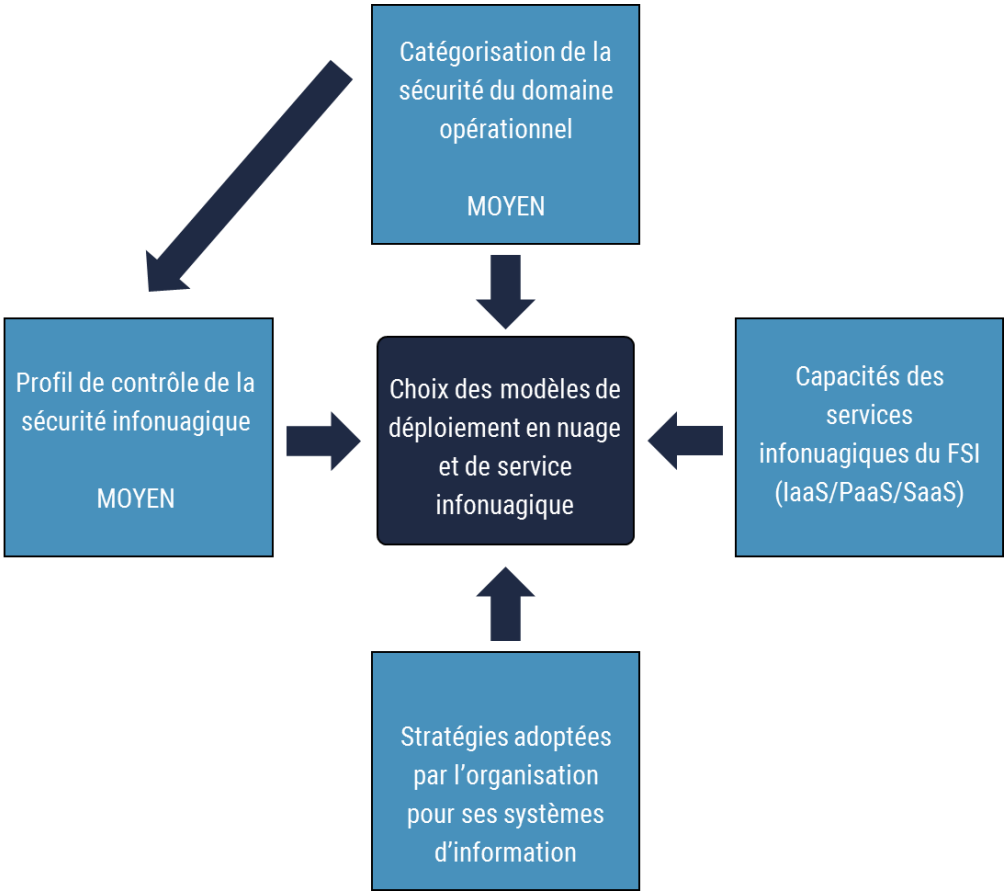


Figure 13– **Choix des modèles de déploiement en nuage et de service infonuagique**

8.1 MODÈLES DE DÉPLOIEMENT EN NUAGE

Au moment de sélectionner un modèle de déploiement en nuage, les organisations devraient considérer certains facteurs, notamment : la polyvalence, la sécurité, l'extensibilité, les coûts, l'automatisation, le niveau de contrôle sur l'infrastructure, l'emplacement et les niveaux de service offerts par chacun des modèles de déploiement en nuage[12]. À la figure 14, « Sur site » fait référence aux logiciels et technologies situés à l'intérieur des limites physiques de votre organisation. « Hors site » fait référence aux logiciels et technologies situés en dehors des limites physiques de votre organisation. Les sections suivantes font état des définitions, des avantages et des inconvénients de chaque modèle de déploiement. Un résumé des avantages et inconvénients est fourni à l'annexe C.

[12] *Cloud Standards Customer Council, Practical Guide to Hybrid Computing* [11].

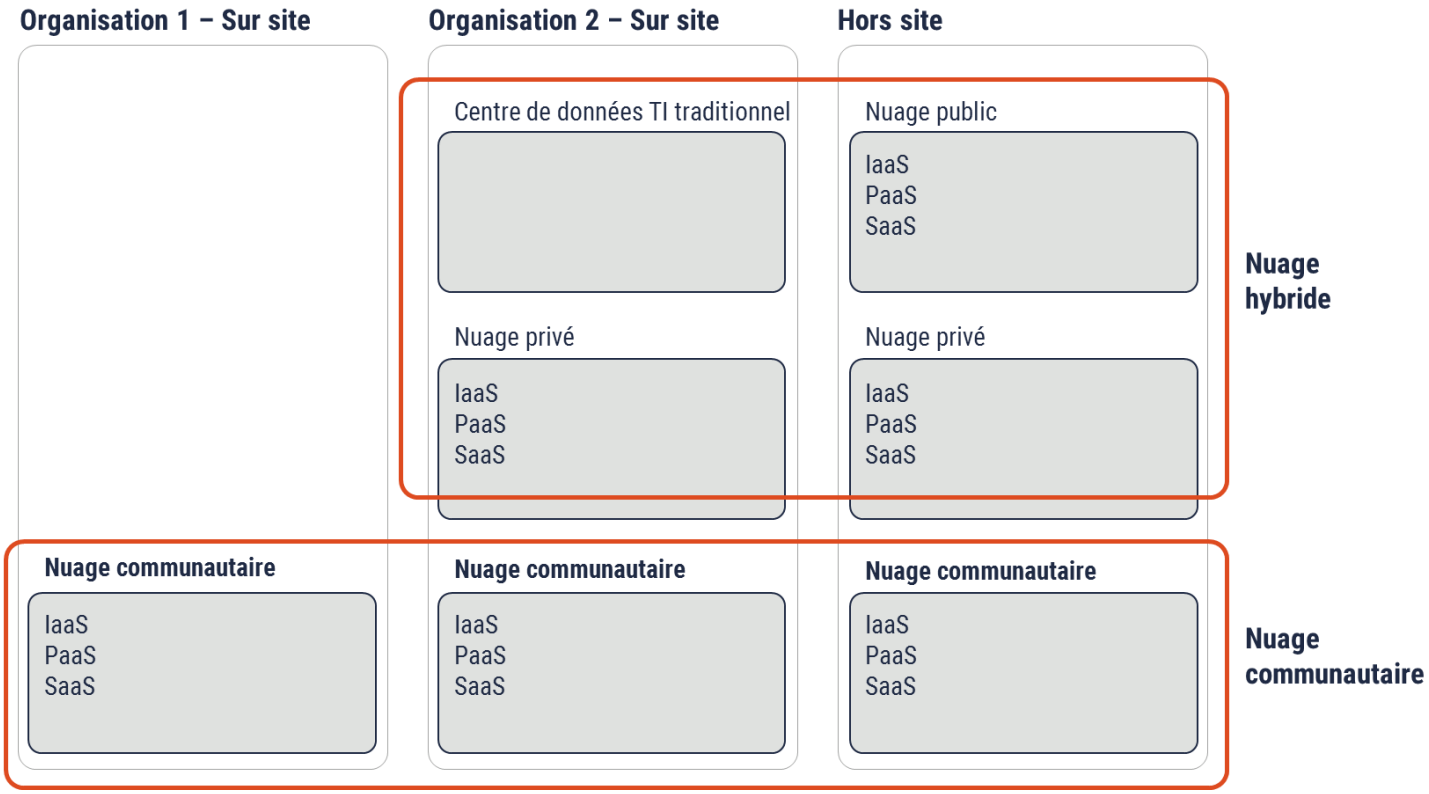


Figure 14– **Modèles de déploiement en nuage**

8.1.1 MODÈLE DE DÉPLOIEMENT EN NUAGE PUBLIC

Dans le cas d'un modèle de déploiement en nuage public, l'infrastructure infonuagique est ouverte à tous. Le nuage peut appartenir à une ou plusieurs entreprises, à un établissement scolaire ou à un organisme gouvernemental, ou encore à un regroupement de ces intervenants. Le ou les propriétaires se chargent de la gestion et de l'exploitation du nuage, lequel peut être hébergé localement ou dans les installations du fournisseur de service infonuagique.

Les capacités d'extensibilité et d'élasticité offertes par le déploiement en nuage public procurent aux organisations la souplesse nécessaire pour faire face aux pics de trafic et se traduisent par une plus grande fiabilité advenant des défaillances matérielles.

Dans ce modèle de déploiement, les FSI proposent des services infonuagiques, des solutions en matière de sécurité et des accords sur les niveaux de service standardisés et bien définis. Bien que ces services, standardisés par nature, permettent aux FSI de fournir les services à moindres coûts, il est peu probable que les organisations soient en mesure de négocier la personnalisation des services, des processus opérationnels ou des accords sur les niveaux de service. Les clients de services infonuagiques qui ont des exigences très strictes en matière de sécurité, d'opérations ou de gouvernance pourraient avoir à mettre en place des contrôles de compensation afin de combler les lacunes inhérentes aux solutions proposées par les FSI. Dans la mesure du possible, les clients de services infonuagiques devraient considérer d'autres modèles de déploiement.

Le modèle de déploiement en nuage public propose une architecture mutualisée. Une telle architecture ne permet pas aux organisations de vérifier la posture de sécurité de l'environnement du FSI. Elles doivent donc se fier aux évaluations effectuées par des tiers lorsqu'elles envisagent une telle utilisation.

Les services offerts par les fournisseurs de services en nuage public peuvent changer très rapidement. Ces nouveaux services ne peuvent être évalués par les évaluateurs de tierces parties qu'au cours du prochain cycle d'évaluation. Avant de faire appel à ces nouveaux services, les organisations devraient veiller à ce que la sécurité offerte par les FSI ait été évaluée par des évaluateurs de tierces parties.

8.1.2 MODÈLE DE DÉPLOIEMENT EN NUAGE PRIVÉ

Dans le cas d'un déploiement en nuage privé, l'infrastructure infonuagique est mise en place aux fins d'utilisation exclusive par une seule organisation formée de plusieurs clients (p. ex. unités opérationnelles). Le nuage peut appartenir à une organisation, à un tiers, ou aux deux. Le ou les propriétaires se chargent de gérer et d'exploiter le nuage, lequel peut être hébergé localement ou à distance.

Ce type de déploiement permet aux organisations de négocier plus facilement les exigences associées aux services, aux processus opérationnels, aux accords sur les niveaux de service, à la sécurité et à la gouvernance. Cette souplesse est généralement plus coûteuse et les organisations pourraient devoir se contenter des dispositions énoncées dans le contrat.

Le modèle de déploiement en nuage public peut être une solution avantageuse pour les organisations qui nécessitent une extensibilité et une élasticité élevées, ou encore des fonctions avancées qu'il serait trop coûteux de mettre en œuvre dans leurs installations.

8.1.3 MODÈLE DE DÉPLOIEMENT EN NUAGE HYBRIDE

Selon la définition du NIST, le modèle hybride est un environnement composé d'au moins deux infrastructures infonuagiques distinctes (nuage privé, communautaire ou public) qui demeurent des entités uniques, tout en étant liées par une technologie normalisée ou propriétaire permettant la portabilité des données et des applications. Lorsque l'infrastructure TI locale est combinée à un ou plusieurs nuages publics, privés ou communautaires, il s'agit d'un nuage hybride.

Les nuages hybrides proposent certains des avantages des nuages publics et privés, et sont souvent utilisés par les organisations comme première étape de leur migration vers le nuage. Ils permettent à ces dernières de mettre en place des exigences plus rigoureuses en matière de sécurité dans leurs installations, tout en déployant des charges de travail qui nécessitent d'importantes ressources informatiques pour assurer le traitement, l'extensibilité et l'élasticité sur le nuage public.

Le modèle de nuage hybride se caractérise par une complexité accrue. Par exemple, les organisations doivent procéder à l'évaluation de sécurité de plusieurs FSI, ainsi que déterminer les fonctions de sécurité à utiliser pour chacun des nuages, la façon de gérer les ressources des différents FSI, l'emplacement de ces ressources et la façon d'interconnecter les environnements infonuagiques de manière sécurisée.

8.1.4 MODÈLE DE DÉPLOIEMENT EN NUAGE COMMUNAUTAIRE

Un nuage communautaire est mis en place aux fins d'utilisation exclusive par une communauté particulière de clients provenant d'organisations partageant des enjeux communs (p. ex. mission, exigences de sécurité, politiques et considérations liées à la conformité). Une ou plusieurs organisations de la communauté ou une tierce partie, ou une combinaison de ces intervenants, peuvent être propriétaire du nuage, le gérer et l'exploiter, et ce nuage peut être mis en place localement ou à distance. Les coûts sont répartis parmi moins d'utilisateurs qu'un nuage public (mais plus qu'un nuage privé), donc les utilisateurs ne bénéficient pas de toutes les économies possibles de l'infonuagique.

Bien qu'ils ne permettent pas de réaliser les mêmes économies que le modèle de déploiement en nuage public, les nuages communautaires peuvent fournir des économies d'échelle considérables, ainsi qu'une partie de la souplesse offerte par les nuages privés.

Les organisations qui envisagent de faire appel à un nuage communautaire devraient déterminer la façon dont la disponibilité et les interruptions de service seront gérées, et qui s'en chargera. Elles devraient également réfléchir aux implications que pourrait avoir la répartition de leurs données entre plusieurs organisations et, possiblement, dans des emplacements différents.

8.2 MODÈLES DE SERVICE INFONUAGIQUE

Le choix des modèles de déploiement en nuage et de service infonuagique doit être effectué en fonction de ce qui suit :

- la nature du service;
- le niveau de contrôle que l'organisation cliente veut conserver;
- le degré d'expertise et de maturité de l'organisation cliente dans le cadre de l'exploitation et de la maintenance des environnements des systèmes d'information fondés sur l'infonuagique.

Le NIST définit les trois modèles de services suivants :

- Le modèle **SaaS** permet au client d'utiliser les applications du fournisseur qui sont exécutées dans une infrastructure en nuage. Ces applications sont accessibles à partir de divers dispositifs clients par l'intermédiaire d'une interface client léger comme un navigateur Web (p. ex. services de courrier Web) ou d'une interface de programmation;
- Le modèle **PaaS** permet au client de déployer sur son infrastructure infonuagique des applications qu'il a acquises ou créées à l'aide de langages, de bibliothèques, de services et d'outils de programmation pris en charge par le fournisseur;
- Le modèle **IaaS** offre au client le traitement, le stockage, les réseaux ainsi que d'autres ressources informatiques fondamentales, grâce auxquels le client peut déployer et exécuter des logiciels arbitraires, dont des systèmes d'exploitation et des applications.

Dans le cas de ce dernier modèle, les responsabilités qui incombent aux clients du service infonuagique sont plus grandes que pour les modèles PaaS et SaaS. Par ailleurs, contrairement aux modèles PaaS et Saas pour lesquels la latitude est moins grande, le modèle IaaS offre aux organisations la latitude nécessaire pour adapter, mettre en œuvre et gérer leurs propres contrôles de sécurité[13].

[13] L'annexe de l'ITSP.50.103 fait mention des profils de contrôle de sécurité qui permettent d'allouer les contrôles de manière à préciser dans quelle mesure le FSI ou le client du service infonuagique est responsable des exigences de sécurité énoncées dans le profil de contrôle de sécurité sélectionné. On y traite également de l'attribution de contrôles par modèle de service.

9 RÉSUMÉ

Les clients de services infonuagiques doivent procéder à la catégorisation de la sécurité de leurs activités opérationnelles afin de faciliter la sélection du profil de contrôle de sécurité requis, ainsi que le choix des modèles de déploiement en nuage et de service infonuagique.

L'ITSP.50.103 aide les clients de services infonuagiques à comprendre les activités de catégorisation de la sécurité qu'ils devront mettre en œuvre s'ils ont recours à des services infonuagiques. Dans la présente, on recommande également des profils de contrôle de sécurité qui permettront de prendre en charge les domaines opérationnels dont la catégorie de sécurité est de niveau FAIBLE et MOYEN.

9.1 AIDE ET RENSEIGNEMENTS

Si votre organisation a besoin de conseils pour assurer la catégorisation de la sécurité de services infonuagiques et veut obtenir de plus amples renseignements, veuillez communiquer avec le Centre d'appel du Centre pour la cybersécurité.

Centre pour la cybersécurité Centre d'appel

contact@cyber.gc.ca

613-949-7048

10 CONTENU COMPLÉMENTAIRE

10.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
AAP	Architecture d'alignement des programmes
AMPS	Avis de mise en œuvre de la Politique sur la sécurité
ANS	Accord sur les niveaux de service
Centre pour la cybersécurité	Centre canadien pour la cybersécurité
CDS	Cycle de développement des systèmes
CST	Centre de la sécurité des télécommunications
FSI	Fournisseur de service infonuagique
GC	Gouvernement du Canada
GSTI	Gestion de la sécurité des technologies de l'information
IaaS	Infrastructure en tant que service (*Infrastructure as a Service*)
ITSP	Conseils en matière de sécurité des technologies de l'information pour les praticiens (*Information Technology Security Guidance for Practitioners*)
PaaS	Plateforme en tant que service (*Platform as a Service*)
RPP	Rapport sur les plans et les priorités
SaaS	Logiciel en tant que service (*Software as a Service*)
STI	Sécurité des technologies de l'information
TI	Technologies de l'information

10.2 GLOSSAIRE

Terme	Définition
Catégorisation de la sécurité	Processus permettant d'identifier les possibles préjudices liés à la compromission des processus opérationnels et des biens d'information connexes.
Comité d'évaluation	Équipe multidisciplinaire composée de représentants des secteurs responsables des opérations, des questions juridiques, de l'accès à l'information, de la sécurité et du respect de la vie privée. Le propriétaire opérationnel ou son délégué devrait également faire partie de cette équipe, de même que le responsable de l'autorisation (si cette tâche n'a pas été confiée au propriétaire opérationnel) et les représentants et analystes opérationnels de chaque programme ou secteur d'activités.
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril la confidentialité, l'intégrité ou la disponibilité de l'information en question.
Confidentialité	Fait d'être divulgué uniquement aux mandants autorisés.
Conseiller en sécurité	Personne ou équipe qui possède les connaissances fondamentales et l'expérience requise pour formuler des recommandations en matière de gestion des risques à l'agent d'autorisation de l'organisation.
Disponibilité	Fait d'être accessible et utilisable intégralement et en temps opportun.
Domaine opérationnel	Un domaine opérationnel est un environnement dans lequel une organisation mène des activités qui soutiennent des objectifs communs.
Fournisseur de service infonuagique	Fournisseur commercial de services infonuagiques qui souhaite offrir ses services à des clients. Un FSI peut détenir (ou non) une attestation pour ses services infonuagiques au début du processus de gestion des risques.
Incidence	Terme utilisé pour désigner à la fois un préjudice et une conséquence. On emploie fréquemment les termes répercussions sur les opérations et répercussions sur la mission dans ce sens.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Le concept d'intégrité s'applique également aux processus opérationnels, à la logique des logiciels d'application, au matériel et au personnel.
Intérêt national	Dommages qui concernent la sécurité et la stabilité sociopolitique et économique du Canada.
Intérêt non national	Dommages qui concernent la sûreté, la santé et le bien-être des personnes, ainsi que la situation financière et la réputation des citoyens et des organisations canadiennes.
Organisation cliente d'un service infonuagique	Organisation souhaitant faire appel à un FSI pour mettre en œuvre des services fondés sur l'infonuagique.
Préjudice	Dommage causé aux intérêts nationaux et non nationaux par les activités opérationnelles mises à leur service et qui résulte de la compromission de biens de TI desquels elles dépendent.
Profil de contrôle de la sécurité d'un domaine opérationnel	Le profil de contrôle de la sécurité d'un domaine opérationnel est associé à un domaine opérationnel en particulier plutôt qu'à l'ensemble d'une organisation.

10.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité. *ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
2	Centre canadien pour la cybersécurité. *Gestion des risques liés à la sécurité infonuagique* (ITSM.50.062) , mars 2019.
3	Secrétariat du Conseil du Trésor du Canada. *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada*, 25 juin 2018.
4	Secrétariat du Conseil du Trésor du Canada. *Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada*, non daté.
5	Secrétariat du Conseil du Trésor du Canada. *Avis de mise en œuvre de la Politique sur la sécurité (AMPS), Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage*, 1er novembre 2017.
6	Secrétariat du Conseil du Trésor du Canada. *Politique sur la gestion des technologies de l'information*, 31 mars 2018.
7	*La Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). S.C. 2000, c.5.
8	National Institute of Standards and Technology. *Guide for Mapping Types of Information and Information Systems to Security Categories* (publication spéciale 800-60, vol. 1, rév. 1), août 2008.
9	Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4.0, 2017.
10	National Institute of Standards and Technology. *The NIST Definition of Cloud Computing* (publication spéciale 800-145, septembre 2011.
11	Cloud Standards Customer Council, *Practical Guide to Hybrid Computing*, février 2016.
12	National Institute of Standards and Technology. *Cloud Computing Synopsis and Recommendations* (publication spéciale 800-146), mai 2012.

Annexe A Profil de contrôle de la sécurité infonuagique – FAIBLE

Pour de plus amples renseignements, prière de consulter l'*Annexe A – Recommandations du Centre pour la cybersécurité pour le profil de contrôle de la sécurité infonuagique FAIBLE*.

Annexe B Profil de contrôle de la sécurité infonuagique – MOYEN

Pour de plus amples renseignements, prière de consulter le fichier Excel, *Annexe B – Recommandations du Centre pour la cybersécurité pour le profil de contrôle de la sécurité infonuagique MOYEN*.

Annexe C Résumé des points à considérer à la sélection du modèle de déploiement en nuage[14]

	Public	Privé (sur site)	Hybride	Communautaire (sur site)
Emplacement	• Non visible au client du service infonuagique, à moins que le fournisseur n'ait mis en place (facultatif) des stratégies pour restreindre l'emplacement du nuage et que le client du service ait configuré son compte de manière à exiger des restrictions particulières pour cet emplacement.	• Les clients des services infonuagiques choisissent l'infrastructure physique qui hébergera le nuage privé et déterminent l'emplacement géographique possible des charges de travail.	• Les clients des services infonuagiques déterminent l'emplacement géographique des charges de travail à l'aide de stratégies visant à restreindre l'hébergement interne ou l'emplacement du FSI.	• Les charges de travail demeurent généralement en possession des organisations participantes (à moins d'être externalisées).
Investissement initial	• Faible	• Important à élevé[15]	• Investissement moindre puisque les charges de travail non essentielles à la réalisation de la mission sont hébergées dans des nuages publics offrant une extensibilité et une élasticité élevées.	• Important à élevé
Complexité	• Importante	• Peu élevée à importante	• Importante à élevée	• Les configurations associées à la gestion de l'identité et de l'accès effectuées par les organisations participantes peuvent être complexes.
Accord sur les niveaux de service (ANS)	• L'ANS par défaut précise les promesses limitées qui ont été faites aux clients des services infonuagiques et les solutions proposées. • Peu de place à la négociation.	• Plus de souplesse pour ce qui est de l'ANS et de la négociation des contrats. • Peut se limiter aux points négociés dans le contrat.	• Peut nécessiter la gestion de plusieurs contrats et ANS.	• Plus de souplesse pour ce qui est de l'ANS et de la négociation des contrats. • Peut se limiter aux points négociés dans le contrat. • Les clients des services infonuagiques devraient déterminer la façon dont la disponibilité et les interruptions de service seront gérées, et qui s'en chargera.

[14] National Institute of Standards and Technology. *Cloud Computing Synopsis and Recommendations* (publication spéciale 800-146) [12].

[15] Dans le cas du modèle de nuage privé externalisé, les ressources sont fournies par le fournisseur. Les coûts initiaux pour l'organisation cliente peuvent être faibles ou élevés, et inclure la négociation de l'ANS, les frais de connectivité du réseau, la conversion des applications pour l'environnement en nuage et la formation.

	Public	Privé (sur site)	Hybride	Communautaire (sur site)
Compétences en TI requises	• Les clients de services infonuagiques devront avoir les compétences en TI requises pour gérer les dispositifs des utilisateurs et devront également acquérir de nouvelles compétences en infonuagique.	• Les clients de services infonuagiques devront avoir les compétences en TI requises pour gérer les dispositifs des utilisateurs et devront également acquérir de nouvelles compétences en infonuagique. • Les organisations des fournisseurs devront acquérir les compétences nécessaires pour assurer la mise en œuvre et la gestion de l'infrastructure infonuagique.	• Les clients de services infonuagiques devront avoir les compétences en TI requises pour gérer les dispositifs des utilisateurs et devront également acquérir de nouvelles compétences en infonuagique pour des nuages multiples.	• Les clients de services infonuagiques devront avoir les compétences en TI requises pour gérer les dispositifs des utilisateurs et devront également acquérir de nouvelles compétences en infonuagique. • Les organisations des fournisseurs devront acquérir les compétences nécessaires pour assurer la mise en œuvre et la gestion de l'infrastructure infonuagique.
Risques liés à l'architecture mutualisée	• Une seule machine peut prendre en charge les charges de travail de plusieurs utilisateurs. Dans la pratique, cela signifie que la charge de travail d'un client peut corésider avec les charges de travail de concurrents ou d'adversaires.	• Les risques sont quelque peu atténués par la restriction du nombre d'attaquants possibles. • Tous les clients seraient typiquement membres de l'organisation cliente, ou des invités ou partenaires autorisés.	• Les clients de services infonuagiques peuvent héberger les charges de travail stratégiques dans leurs installations et les autres charges de travail dans d'autres modèles de déploiement en nuage de manière à réduire les coûts, et à tirer avantage de nouvelles capacités et d'une plus grande élasticité.	• Atténue certains des risques liés à l'architecture mutualisée en limitant le nombre d'attaquants possibles. • Le nuage englobe plusieurs organisations et peut ainsi assurer une meilleure limitation des attaquants potentiels qu'avec un nuage privé sur site.
Protection contre les menaces externes	• Les clients de services infonuagiques qui ont des exigences très strictes en matière de sécurité, d'opérations ou de gouvernance peuvent mettre en place des contrôles de compensation afin de combler les lacunes inhérentes aux solutions proposées par les FSI.	• Les clients de services infonuagiques ont le choix de mettre en place un périmètre rigoureux de sécurité pour protéger les ressources dans le nuage privé contre les menaces externes au même niveau de sécurité offert aux ressources qui ne sont pas en nuage[16].	• Les clients de services infonuagiques déploient typiquement des charges de travail en imposant des exigences de sécurité plus rigoureuses dans leurs installations. Ils ont donc l'option de mettre en œuvre un périmètre de sécurité rigoureux pour ces charges de travail.	• La protection contre les menaces externes dépend de la sécurité assurée pour tous les périmètres de sécurité des organisations participantes et de la robustesse des liens de communications.
Visibilité et contrôle	• Limité	• Élevé	• Élevé pour les charges de travail hébergées sur site	• Élevé

[16] La principale différence avec le nuage privé externalisé est que les techniques doivent être appliquées tant au périmètre du client qu'à celui du fournisseur, et que le lien des communications doit être protégé.

	Public	Privé (sur site)	Hybride	Communautaire (sur site)
Élasticité	• Généralement sans restriction en ce qui concerne l'emplacement ou la taille. • Avantages uniques en ce qui concerne l'élasticité ou l'illusion (pour les clients) d'une disponibilité illimitée des ressources.	• La capacité de traitement et de stockage établie est adaptée de manière à répondre aux charges de travail prévues et aux restrictions budgétaires.	• Les clients de services infonuagiques mettent typiquement en place des exigences plus rigoureuses en matière de sécurité dans leurs installations, tout en déployant des charges de travail qui nécessitent d'importantes ressources informatiques pour assurer le traitement, l'adaptabilité et l'élasticité sur le nuage public.	• La capacité de traitement et de stockage établie est adaptée de manière à répondre aux charges de travail prévues et aux restrictions budgétaires.