Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Gérer les risques liés aux données du gouvernement du Canada dans le contexte des services infonuagiques

SÉRIE GESTIONNAIRES

TLP:WHITE

Canada

Avant-propos

La publication *Gérer les risques liés aux données du gouvernement du Canada dans le contexte des services infonuagiques* (ITSM.50.109) est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre pour la cybersécurité.

Date d'entrée en vigueur

Le présent document entre en vigueur le 3 août 2022.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	3 août 2022

D97-4/50-109-2022F-PDF
978-0-660-44635-6

Vue d'ensemble

Le présent document formule des conseils visant à aider les ministères et organismes du gouvernement du Canada (GC) à gérer les risques liés aux données du GC lorsqu'ils ont recours à des services infonuagiques, en particulier les modèles de déploiement en nuage public.

Ce document définit les données du GC et démontre la manière dont un sous-ensemble de ces données peut correspondre à la terminologie d'un fournisseur de services infonuagiques (FSI) et dont la plateforme du FSI peut accéder à ces données et les traiter à diverses fins. Il importe que les ministères du GC comprennent les données du GC et en quoi consiste ce sous-ensemble de données dans le cadre des services qu'ils obtiennent. Ils devraient bien comprendre les niveaux de préjudice associés aux données sensibles et les risques liés aux activités à l'échelle du ministère. Les ministères seront en mesure d'appliquer les principes de gestion des risques à leurs données et de prendre des décisions axées sur le risque lorsqu'ils ont font appel à des services en nuage public pour répondre à des exigences liées à la mission.

Le présent document fait référence à une publication du National Institute of Standards and Technology (NIST) intitulée *Special Publication 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices* [1][1].

[1] Les numéros entre crochets renvoient à des ressources figurant à la section Contenu complémentaire du présent document.

Table des matières

Liste des tableaux

1 Introduction

Le présent document offre de l'information sur la gestion des risques liés aux données du gouvernement du Canada dans le contexte du recours aux services infonuagiques. Il importe de tenir compte de la gestion des risques lorsqu'une organisation qui avait l'habitude de gérer ses propres données en interne décide de faire appel à des services infonuagiques externes pour gérer ses données.

Lorsqu'elles ont recours à des FSI pour gérer de l'information, les organisations devraient considérer les risques internes habituels ainsi que les nouvelles menaces externes. Le présent document offre aux organisations des conseils sur les différents types d'information qu'il convient d'évaluer avant et durant l'utilisation de services de FSI pour déterminer les risques liés au stockage et au traitement de cette information en externe.

1.1 Types d'information à prendre en considération

Avant le virage vers les services infonuagiques, les organisations exploitaient leurs propres infrastructures de technologie de l'information (TI) à l'aide de membres du personnel possédant l'habilitation de sécurité nécessaire en fonction des exigences de sécurité organisationnelles. Le personnel achetait l'équipement de TI requis, l'installait dans le centre de données, puis en assurait la maintenance et la gestion pour répondre aux besoins opérationnels et soutenir les activités liées à la mission. Les organisations appliquaient des contrôles à l'information et aux biens d'information. Il est loin d'être simple de déterminer tous les types d'information qui se trouvent dans un environnement de TI conventionnel. En voici quelques exemples :

- données liées à la mission et données utilisateur qui résident dans les applications organisationnelles;
- données de configuration qui permettent aux applications de fonctionner comme prévu;
- métadonnées d'applications utilisées par le personnel pour exploiter et maintenir les applications.

Des données sont également liées à l'infrastructure, qui comprend les points terminaux, les appliances, les serveurs et les composants réseau et divers types de systèmes d'exploitation et de micrologiciels. Il s'agit des données qui permettent de décrire non seulement ce que font les composants de l'infrastructure, mais aussi les comportements de ces composants et la mesure dans laquelle ils fonctionnent bien.

On peut considérer l'information contenue dans un système de TI sous divers angles, comme le domaine opérationnel, l'architecture, le Web, les couches de base de données et la réseautique. Chacun comporte des objectifs précis.

Toutes ces données sont importantes. Elles représentent l'information contenue dans l'infrastructure de TI d'une organisation et fournissent de l'information sur l'environnement. Si les données sont menacées, des risques guettent la confidentialité, l'intégrité et la disponibilité des activités essentielles d'une organisation qui appuient l'atteinte d'objectifs liés à la mission. Il pourrait être impossible de mener les activités liées à la mission ou de bien les réaliser, ce qui risque de nuire à la capacité de l'organisation de fournir des produits et services. Les organisations devraient tenir compte de ces données et évaluer la sensibilité de celles-ci en fonction des principes de la sécurité opérationnelle (OPSEC pour *Operational Security*). De nombreuses organisations comprennent l'importance de ces données et les répercussions d'un accès non autorisé à celles-ci. Elles reconnaissent qu'elles doivent tenir compte de ces données dans le contexte de la gestion des

risques et mettre en œuvre les politiques, les normes, les procédures et les lignes directrices nécessaires pour prévenir l'accès non autorisé à l'infrastructure et protéger l'information.

Cet environnement de TI local représente bien les éléments sur lesquels une évaluation complète des données du GC devrait porter. Ces données du GC peuvent se classer dans trois catégories :

1. les données liées à la mission et aux objectifs de votre organisation et qui appuient ces éléments;
2. les données qui décrivent l'infrastructure de TI de soutien;
3. les données qui permettent à votre organisation d'exploiter ses infrastructures de TI et qui soutiennent le fonctionnement continu de ces infrastructures à l'appui de l'atteinte des objectifs organisationnels.

Les données créées et utilisées par les utilisateurs pour soutenir et atteindre les objectifs organisationnels correspondent aux données liées à la mission que les utilisateurs peuvent voir et traiter et auxquelles ils peuvent accéder au quotidien. Pour illustrer cette catégorie de données, la publication SP 800-60, vol. 2, rév. 1 [1] du NIST a dressé une liste exhaustive des types d'information qui couvriraient de nombreux aspects d'une organisation fonctionnelle et qu'on pourrait considérer comme divers types de données opérationnelles créées par des utilisateurs au sein de l'organisation à l'appui des activités liées à la mission.

Les deux autres grandes catégories de données liées à l'infrastructure de TI peuvent également être mieux représentées au moyen des types d'information définis dans la publication SP 800-60, vol. 2, rév. 1 [1] du NIST. Le tableau ci-dessous décrit les types d'information associés à une infrastructure de TI.

Tableau 1 : Types d'information liés à la gestion de l'information et des technologies

Type d'information	Définition de la publication 800-60 du NIST
Développement des systèmes	Le développement des systèmes soutient toutes les activités liées à la conception et au développement d'applications logicielles en interne.
Gestion du cycle de vie ou des changements	La gestion du cycle de vie ou des changements comporte les processus qui facilitent l'évolution, la composition et la transition en douceur de l'effectif, ainsi que la mise en œuvre de changements aux ressources organisationnelles comme les biens, les méthodologies, les systèmes ou les procédures.
Maintenance des systèmes	La maintenance des systèmes soutient toutes les activités liées à la maintenance d'applications logicielles conçues en interne.
Maintenance de l'infrastructure des TI	La maintenance de l'infrastructure des TI comporte la planification, la conception, la mise en œuvre et la maintenance d'une infrastructure des TI visant à soutenir efficacement les besoins automatisés (c'est-à-dire les systèmes d'exploitation. les logiciels d'application, les plateformes, les réseaux, les serveurs, les imprimantes, etc.). La maintenance de l'infrastructure des TI s'étend également à l'information sur la configuration des systèmes d'information et sur l'application des stratégies de sécurité. Cette information comprend les fichiers de mots de passe, les règles d'accès réseau, les fichiers de mise en œuvre, les paramètres des commutateurs, les paramètres de configuration du matériel et des logiciels, et toute documentation susceptible d'avoir une incidence sur l'accès aux données, aux programmes et aux processus du système d'information.
Sécurité des systèmes d'information	La sécurité des systèmes d'information concerne toutes les fonctions visant à sécuriser les données et systèmes fédéraux au moyen de la création et de la définition de stratégies, de procédures et de contrôles de sécurité s'appliquant à des services comme l'identification, l'authentification et la non-répudiation.
Gestion de l'information (GI)	La GI comporte la coordination de la collecte, du stockage, de la diffusion et de l'élimination de l'information, ainsi que la gestion des politiques, des lignes directrices et des normes liées à la GI.
Surveillance des systèmes et des réseaux	La surveillance des systèmes et des réseaux soutient toutes les activités liées à la surveillance en temps réel des systèmes et des réseaux pour en assurer la performance optimale. La surveillance des systèmes et des réseaux repose sur des outils et l'observation dans le but de déterminer la performance et l'état des systèmes d'information, et elle est étroitement liée à d'autres sous-fonctions de la gestion des TI. Il convient de définir le type d'information lié à la surveillance des systèmes et des réseaux au sens large, de manière à inclure l'information sur le réseau (comme la performance, la santé et l'état) et le soutien des opérations de sécurité (comme la surveillance des intrusions, les audits, etc.) de l'organisation.

2 Données du GC correspondant à la terminologie des fournisseurs de services infonuagiques

Comme les organisations choisissent de plus en plus de passer à des environnements en nuage et de tirer profit des avantages qu'offrent les services infonuagiques, elles doivent bien comprendre en quoi consistent les données du GC et réévaluer leurs données dans le contexte de l'infonuagique. Les types d'information définis dans le tableau ci-dessus donnent des renseignements sur les configurations et les composants associés à un environnement de TI particulier – ce qu'ils font et la manière dont ils fonctionnent, et l'efficacité de l'exploitation de l'infrastructure des TI – dans le cadre desquels les vulnérabilités et les points forts peuvent être relevés ou découverts. Dans un environnement en nuage, pour chaque type d'information, certaines données ne relèvent plus entièrement du contrôle de l'organisation. Les organisations peuvent néanmoins accéder à ces données, les traiter et les manipuler, mais les fournisseurs de services peuvent également le faire aux fins de l'exploitation et de la maintenance de la performance des services et de la sécurité de leurs plateformes. Il importe que les organisations comprennent la manière dont les fournisseurs de services décrivent cette information dans le but de tenir des discussions objectives et de prendre des décisions éclairées axées sur le risque.

2.1 Données utilisateur ou données du client

Les données liées à la mission ou les données opérationnelles correspondent aux données que les utilisateurs d'une organisation ont soit créées, soit téléversées dans les applications de la mission et qu'ils doivent traiter à l'appui des opérations de la mission. Dans l'environnement en nuage, il s'agit de l'information que les utilisateurs créent et enregistrent dans les services infonuagiques achetés. Le FSI désigne généralement cette information sous les termes « données utilisateur » ou « données du client ». Les fournisseurs établissent des politiques exhaustives sur la sécurité et la confidentialité des données en conformité avec les diverses lois dans plusieurs territoires afin d'assurer la protection de ce type de données sur le plan de la sécurité et de la confidentialité. Par exemple, la publication *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111) [2] établit les suites de chiffrement à utiliser pour chiffrer les données, alors que la *Loi sur la protection des renseignements personnels* (LPRP) et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) régissent la collecte, l'utilisation et la divulgation des renseignements personnels. Certaines provinces ont également adopté leurs propres lois sur le respect de la vie privée.

Même si des règles strictes régissent l'accès des fournisseurs aux données utilisateur et le traitement de ces données par ces fournisseurs, les organisations devraient toujours faire preuve de prudence quant à leurs données utilisateur et opérationnelles et s'assurer de comprendre les circonstances dans lesquelles leurs données pourraient transiter et être stockées dans différents territoires. Les organisations devraient alors se demander si les mesures de protection mises en place par les fournisseurs de services sont suffisantes. Par exemple, les fournisseurs devront possiblement traiter des copies de données utilisateur ou y accéder pour assurer la performance des services et aider les clients à régler des problèmes précis. Dans ces cas, les données utilisateur ne doivent contenir aucun renseignement personnel qui permettrait d'identifier une personne.

2.2 Données comportant de l'information sur l'infrastructure des TI

L'évaluation des répercussions d'une compromission de données comportant de l'information sur l'infrastructure des TI est plus complexe que celle visant des données utilisateur. Cette question n'est généralement pas soulevée lors des discussions sur les types de données organisationnelles. Lorsque des organisations discutent des données dans le contexte du nuage public, il est presque certain que ces discussions finiront par porter sur les données utilisateur. Cette situation s'explique par l'un ou l'autre des facteurs suivants :

1. Les données sur l'infrastructure des TI ne sont pas aussi visibles que les données utilisateur en ce qui concerne la contribution directe aux activités liées à la mission;
2. L'organisation met moins l'accent sur la propriété des données sur l'infrastructure des TI dans le nuage public du FSI en raison d'un manque de contrôle et de sensibilisation.

Chaque organisation doit comprendre son point de vue sur la question des types de données et la relation avec son FSI. Les organisations doivent tenir compte de tous les types de données, comme lorsqu'elles gèrent les données dans leur environnement de TI local. Les organisations qui utilisent des services infonuagiques devraient considérer les éléments suivants, entre autres :

- Déterminer les responsabilités des fournisseurs et des clients dans le modèle de services infonuagiques;
- Comprendre la nécessité d'exercer ses responsabilités pour sécuriser ses données et l'environnement infonuagique, et gérer les risques connexes;
- Communiquer avec le FSI au sujet de son modèle de service pour déterminer quelle partie est considérée comme le propriétaire des données et qui a accès aux données;
- Discuter avec le FSI du type de données d'analyse traitées et à qui appartient le service d'analyse qui traite les données.

Au moment de mettre en place leur environnement infonuagique, certaines organisations pourraient compter des centaines ou des milliers de charges de travail (c'est-à-dire un environnement complexe), alors que d'autres pourraient choisir de déployer seulement quelques applications. Les infrastructures infonuagiques qui soutiennent ces environnements se ressemblent, et elles devraient toutes comporter des services réseau, informatiques, de stockage et de gestion fiables et configurés de manière sécurisée. Ce qui distingue les environnements infonuagiques des organisations, c'est la manière dont chacune crée et configure les services pour qu'ils se comportent et fonctionnent d'une façon propre à la mission. Il existe plusieurs types de données, notamment différents types de configurations, l'information sur la surveillance de la performance et de la sécurité, ainsi que l'information sur le contrôle de l'accès, qui pourraient faire la lumière sur l'infrastructure des TI d'un système du gouvernement. Cette information, de même que les services configurés, constitue les éléments essentiels d'un environnement infonuagique fonctionnel dans le cadre duquel l'organisation est propriétaire des données et gère elle-même le traitement et l'analyse de l'information, ainsi que l'accès à cette dernière. Cette information et ces services configurés fournissent aux organisations un environnement infonuagique fonctionnel. En plus d'être propriétaires des données et de l'information, elles y accèdent, les traite et les analyse. Toutefois, dans le contexte des services de nuage public, les fournisseurs de services infonuagiques sont également en mesure d'accéder à certaines de ces données et de les gérer.

Dans plusieurs cas, les FSI doivent avoir accès aux données qui contiennent l'information sur les environnements infonuagiques des organisations pour remplir leurs obligations en vertu des accords sur les niveaux de service. Par exemple, les FSI sont appelés à gérer la performance et la personnalisation des services, la sécurité de leurs plateformes et les services offerts. Il est essentiel de bien comprendre la terminologie employée par les FSI pour désigner les données et l'information de l'organisation dans l'infrastructure infonuagique. Les organisations seront ainsi en mesure de tenir des discussions efficaces avec les fournisseurs afin de faire valoir les considérations nécessaires en matière de sécurité, dans le but de veiller à ce que les données soient sécurisées et protégées contre toute modification ou tout accès non autorisés. Par exemple, le forfait de données d'un service pourrait se trouver dans un territoire qui respecte les exigences du client sur les plans de la conformité et des politiques, alors que le plan de gestion du service réside dans un autre territoire. Si cette situation est préoccupante, il importe que l'organisation sache quelles données ou quel sous-ensemble de données fournissent les données sur l'infrastructure auxquelles le plan de gestion aurait accès et quelles autres activités de traitement pourraient être effectuées. L'organisation et les FSI devraient tenir un dialogue collaboratif. Il est utile de reconnaître la terminologie employée par les fournisseurs qui pourrait correspondre aux données de l'organisation. Le tableau 2 en donne quelques exemples.

Tableau 2 : Données du GC correspondant à la terminologie des services infonuagiques

Type de données	Définition
Données du client et données utilisateur	Données fournies par le client au FSI, y compris les fichiers texte, audio ou vidéo, les images et les logiciels. Il s'agit notamment des données que les clients téléversent aux fins de stockage ou de traitement et les applications que les clients téléversent aux fins de distribution.
Métadonnées d'objet	Données générées durant l'exécution du service. Il peut s'agir d'information fournie par le client ou au nom du client et qui sert à identifier ou à configurer les ressources du service (c'est-à-dire les logiciels et les systèmes). En voici quelques exemples : noms et paramètres techniques des comptes de stockage, machines virtuelles, bases de données et ensembles de données (comme les tableaux, les titres de colonnes, les étiquettes et les chemins d'accès aux documents). Les métadonnées peuvent être transmises dans l'ensemble de l'infrastructure du FSI pour faciliter les opérations et le dépannage.
Métadonnées générées par les services	Données générées et déduites par un fournisseur de services dans le cadre de l'exploitation d'un service infonuagique. Le fournisseur de services regroupe ce type de données pour assurer la performance et la sécurité.
Données de diagnostic	Données de télémesure et données obtenues depuis les applications que les clients installent localement et utilisent pour se connecter aux services infonuagiques.
Métadonnées de contrôle de l'accès	Données utilisées pour gérer l'accès à d'autres types de données ou de fonctions au sein des services.

3 Catégorisation de la sécurité des données

En sachant que les types de données qu'utilisent les FSI peuvent comporter de l'information sensible, les organisations doivent effectuer des analyses fondées sur la gestion des risques afin de déterminer les préjudices possibles liés aux données et de prendre des décisions éclairées en fonction du risque.

La catégorisation de la sécurité constitue l'une des étapes essentielles de l'approche de gestion des risques liés à la sécurité infonuagique, conformément à l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique* [3]. Par catégorisation de la sécurité, on entend le processus permettant d'identifier le possible préjudice qu'une compromission pourrait entraîner pour les processus opérationnels, les activités opérationnelles et l'information connexe. Pour catégoriser les activités et les processus opérationnels, il faut d'abord déterminer les préjudices qui découleraient d'une compromission et le niveau de ces préjudices.

La publication du NIST [1] propose une catégorisation de la sécurité de base pour les types d'information liés à l'infrastructure des TI. Le tableau 3 tient compte des recommandations du NIST et établit des liens entre les types d'information du GC et les types de données définis dans la terminologie de l'infonuagique. Ce tableau porte sur la catégorisation de la sécurité de base recommandée pour les types de données dans le contexte de la catégorie PROTÉGÉ B, intégrité moyenne, disponibilité moyenne (PBMM).

Tableau 3 : Catégorisation de la sécurité pour un domaine du GC d'usage général (profil PBMM)

Type d'information	Type de données du FSI connexe	Catégorisation de la sécurité		
		Confidentialité	Intégrité	Disponibilité
Information relative à la mission	Données du client	Moyen	Moyen	Moyen
Information sur le développement des systèmes	Données du client	Faible	Moyen	Faible
Information sur la gestion du cycle de vie et des changements	Données du client	Faible	Moyen	Faible
Information sur la maintenance des systèmes	Données générées par les services	Faible	Moyen	Faible
Information liée à la maintenance de l'infrastructure des TI	Métadonnées d'objet Métadonnées de contrôle de l'accès	Moyen	Moyen	Moyen
Information sur la sécurité des systèmes d'information	Données du client	Moyen	Moyen	Moyen
Information liée à la gestion de l'information	Métadonnées d'objet	Faible	Moyen	Faible

Information liée à la surveillance de systèmes et de réseaux	Données générées par les services Métadonnées d'objet Données de diagnostic	Moyen	Moyen	Moyen

Il convient de considérer les niveaux de préjudice établis dans le tableau comme le niveau de base ou le niveau de préjudice minimum dans le contexte du profil PBMM. On recommande fortement aux organisations de prendre en considération leurs activités opérationnelles et le niveau de sensibilité et de criticité de leur mission. Les résultats de leurs évaluations pourraient établir des niveaux de préjudice plus élevés pour certains types de données en ce qui concerne la confidentialité, l'intégrité et la disponibilité des objectifs de sécurité et il conviendra d'en tenir compte dans l'approche de gestion des risques liés à l'infonuagique [3].

Il faudrait également prendre en considération les situations où les données ou des sous-ensembles de données sont stockés ou traités, ou les deux, à l'extérieur du Canada. Les données correspondant aux types mentionnés ci-dessus pourraient être transférées à d'autres territoires aux fins de stockage ou de traitement, selon l'architecture de la plateforme du FSI. Les FSI qui mènent leurs activités dans d'autres territoires sont assujettis aux lois locales et doivent les respecter. Cette situation risque d'avoir des répercussions sur l'intégrité et la disponibilité des données liées aux activités relatives à la mission de l'organisation. L'information qui réside dans d'autres territoires pourrait être assujettie à des lois étrangères, ce qui risque d'entraîner la divulgation de données du GC.

4 Sommaire

Bien que les types de données liés à la mission soient importants, les organisations ne doivent pas négliger l'importance des types de données qui fournissent de l'information sur leur environnement de TI. Ces importants types de données sont protégés lorsque les opérations sont effectuées sur site. Il faut prévoir des considérations relatives à la sécurité plus rigoureuses pour les types de données liés à l'infrastructure des TI lors du passage à un environnement commercial en nuage public. Les organisations devraient consulter les FSI pour comprendre les nuances terminologiques possibles, à quels termes correspondent leurs données et où les données se trouveront dans l'infrastructure du FSI, puis évaluer les niveaux de préjudice des données en procédant à une analyse de la catégorisation de la sécurité [3]. Cette analyse devrait s'inscrire dans le processus de gestion des risques pour veiller à ce que des décisions éclairées et fondées sur le risque soient prises en tenant compte de tous les types de données.

5 Contenu complémentaire

5.1 Liste des acronymes et des sigles

Acronyme ou sigle	Définition
CST	Centre de la sécurité des télécommunications
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
GI	Gestion de l'' information
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
OPSEC	Sécurité opérationnelle
PBMM	PROTÉGÉ B, intégrité moyenne, disponibilité moyenne
STI	Sécurité des technologies de l'information
TI	Technologies de l'information

5.2 Glossaire

Terme	Définition
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Autorisation	Droits d'accès accordés à un utilisateur, à un programme ou à un processus.
Chiffrement	Transformation de données d'un format vers un autre pour cacher leur contenu et empêcher un accès non autorisé.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Contrôle d'accès	Attestation confirmant que seul un accès autorisé est donné aux biens (tant physiques qu'électroniques). Pour les biens physiques, des contrôles d'accès peuvent être nécessaires pour les installations ou les zones d'accès limité (par exemple, le contrôle des visiteurs et du matériel aux points d'entrée, l'accompagnement des visiteurs). Pour les biens de TI, des contrôles d'accès peuvent être nécessaires pour les réseaux, les systèmes et l'information (par exemple, limiter l'accès à certains systèmes à des utilisateurs, limiter les privilèges du compte).
Contrôle de sécurité opérationnel	Contrôle de sécurité qui est principalement mis en œuvre et exécuté par des personnes, mais habituellement fondé sur l'utilisation de la technologie (comme un logiciel de soutien).
Fournisseur de services infonuagiques	Tout fournisseur commercial qui offre des services infonuagiques afin d'assurer, sur demande, la disponibilité aux ressources des systèmes informatiques.
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. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.

Terme	Définition
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs et à l'information de TI.
Niveau de préjudice	Gravité d'un préjudice en fonction de cinq niveaux : très faible, faible, moyen, élevé, très élevé.
Niveau de risque	Dans le contexte de la cybersécurité, la probabilité qu'un auteur de menace se serve d'une vulnérabilité pour accéder aux biens et l'incidence de la menace.
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.

5.3 Références

Numéro	Référence
1	*Special Publication 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories:* du National Institute of Standards and Technology (NIST), août 2008 (en anglais seulement).
2	*Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITPS.40.111)*, août 2016.
3	*Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)*, mars 2019.