Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1601

(10/2015)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'informatique en nuage – Aperçu de la sécurité de l'informatique en nuage

## Cadre de sécurité applicable à l'informatique en nuage

Recommandation UIT-T X.1601

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ**

| | |
|---|---|
| RÉSEAUX PUBLICS DE DONNÉES | X.1–X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | X.200–X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | X.300–X.399 |
| SYSTÈMES DE MESSAGERIE | X.400–X.499 |
| ANNUAIRE | X.500–X.599 |
| RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES | X.600–X.699 |
| GESTION OSI | X.700–X.799 |
| SÉCURITÉ | X.800–X.849 |
| APPLICATIONS OSI | X.850–X.899 |
| TRAITEMENT RÉPARTI OUVERT | X.900–X.999 |
| SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX | |
| Aspects généraux de la sécurité | X.1000–X.1029 |
| Sécurité des réseaux | X.1030–X.1049 |
| Gestion de la sécurité | X.1050–X.1069 |
| Télébiométrie | X.1080–X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS | |
| Sécurité en multidiffusion | X.1100–X.1109 |
| Sécurité des réseaux domestiques | X.1110–X.1119 |
| Sécurité des télécommunications mobiles | X.1120–X.1139 |
| Sécurité de la toile | X.1140–X.1149 |
| Protocoles de sécurité | X.1150–X.1159 |
| Sécurité d'homologue à homologue | X.1160–X.1169 |
| Sécurité des identificateurs en réseau | X.1170–X.1179 |
| Sécurité de la télévision par réseau IP | X.1180–X.1199 |
| SÉCURITÉ DU CYBERESPACE | |
| Cybersécurité | X.1200–X.1229 |
| Lutte contre le pollupostage | X.1230–X.1249 |
| Gestion des identités | X.1250–X.1279 |
| APPLICATIONS ET SERVICES SÉCURISÉS | |
| Communications d'urgence | X.1300–X.1309 |
| Sécurité des réseaux de capteurs ubiquitaires | X.1310–X.1339 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | |
| Aperçu général de la cybersécurité | X.1500–X.1519 |
| Echange concernant les vulnérabilités/les états | X.1520–X.1539 |
| Echange concernant les événements/les incidents/l'heuristique | X.1540–X.1549 |
| Echange de politiques | X.1550–X.1559 |
| Heuristique et demande d'informations | X.1560–X.1569 |
| Identification et découverte | X.1570–X.1579 |
| Echange garanti | X.1580–X.1589 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | |
| **Aperçu de la sécurité de l'informatique en nuage** | **X.1600–X.1601** |
| Conception de la sécurité de l'informatique en nuage | X.1602–X.1639 |
| Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage | X.1640–X.1659 |
| Mise en oeuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

# Recommandation UIT-T X.1601

## Cadre de sécurité applicable à l'informatique en nuage


### Résumé

La Recommandation UIT-T X.1601 décrit le cadre de sécurité applicable à l'informatique en nuage. Elle présente une analyse des menaces et des problèmes de sécurité dans l'environnement de l'informatique en nuage et décrit les capacités de sécurité qui pourraient atténuer ces menaces et résoudre les problèmes de sécurité. On y trouve une méthode générale permettant de déterminer, parmi ces capacités de sécurité, celles qu'il faudra préciser pour atténuer les menaces et résoudre les problèmes de sécurité dans le cadre de l'informatique en nuage. L'Appendice I contient un tableau mettant en correspondance, pour une menace ou un problème donné, la ou les capacités de sécurité à mettre en oeuvre.



### Historique

| Edition | Recommandation | Approbation | Commission d'études | ID unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1601 | 24-01-2014 | 17 | 11.1002/1000/12036 |
| 2.0 | UIT-T X.1601 | 29-10-2015 | 17 | 11.1002/1000/12613 |

### Mots clés

Informatique en nuage, confidentialité, protection des données, capacités de sécurité, problèmes de sécurité, cadre de sécurité, menaces de sécurité.


* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

# Table des matières

# Recommandation UIT-T X.1601

## Cadre de sécurité applicable à l'informatique en nuage

### 1 Domaine d'application

La présente Recommandation analyse les menaces et les problèmes de sécurité dans l'environnement de l'informatique en nuage et décrit les capacités de sécurité qui pourraient atténuer ces menaces et résoudre les problèmes de sécurité. Elle présente une méthode générale permettant de déterminer, parmi ces capacités de sécurité, celles qu'il faudra préciser pour atténuer les menaces et résoudre les problèmes de sécurité dans le cadre de l'informatique en nuage.

### 2 Références

Aucune.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 authentification** [b-NIST-SP-800-53]: vérification de l'identité d'un utilisateur, d'un processus ou d'un dispositif souvent indispensable pour pouvoir accéder aux ressources d'un système d'information.

**3.1.2 capacité** [b-ISO/CEI 19440]: qualité permettant d'accomplir une activité donnée.

**3.1.3 informatique en nuage** [b-UIT-T Y.3500]: modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service.

NOTE – Comme exemples de ressources, on peut citer les serveurs, les systèmes d'exploitation, les réseaux, les logiciels, les applications et les équipements de stockage.

**3.1.4 service en nuage** [b-UIT-T Y.3500]: une ou plusieurs capacités offertes par l'intermédiaire de l'informatique en nuage (§ 3.1.3) demandées à l'aide d'une interface définie.

**3.1.5 client d'un service en nuage** [b-UIT-T Y.3500]: partie (§ 3.1.17) à une relation commerciale aux fins de l'utilisation de services en nuage (§ 3.1.4).

NOTE – Une relation commerciale n'implique pas nécessairement des accords financiers.

**3.1.6 partenaire de services en nuage** [b-UIT-T Y.3500]: partie (§ 3.1.17) fournissant un appui ou une aide aux activités d'un fournisseur de services en nuage (§ 3.1.7), d'un client de services en nuage (§ 3.1.5), ou des deux.

**3.1.7 fournisseur de services en nuage** [b-UIT-T Y.3500]: partie (§ 3.1.17) qui met à disposition des services en nuage (§ 3.1.4).

**3.1.8 utilisateur de services en nuage** [b-UIT-T Y.3500]: personne physique, ou entité agissant en son nom, associée à un client de services en nuage (§ 3.1.5) qui utilise des services en nuage (§ 3.1.4).

NOTE – Comme exemples de ces entités, on peut citer les dispositifs et applications.

**3.1.9 communications en tant que service (CaaS)** [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle la capacité fournie au client du service en nuage (§ 3.1.5) est une interaction et une collaboration en temps réel.

NOTE – La communication CaaS peut correspondre à la fourniture de capacités de plate-forme et de capacités d'application.

**3.1.10 nuage communautaire** [b-UIT-T Y.3500]: modèle de déploiement d'un nuage dans lequel les services en nuage (§ 3.1.4) prennent en charge exclusivement un ensemble défini de clients de services en nuage (§ 3.1.5) et sont utilisées en partage par ce même ensemble de clients, qui ont des exigences communes et une relation entre eux, les ressources étant contrôlées par au moins un membre de cet ensemble.

**3.1.11 personne responsable du contrôle des données** [b-key definition]: personne qui (seule, collectivement ou avec d'autres personnes) détermine à quelles fins et de quelle manière des données personnelles sont ou doivent être traitées.

**3.1.12 personne responsable du traitement des données** [b-key definition]: en ce qui concerne les données personnelles, toute personne (autre qu'un employé de la personne responsable du contrôle des données) qui traite les données au nom de la personne responsable du contrôle des données.

**3.1.13 hyperviseur** [b-NIST-SP-800-125]: élément de virtualisation qui gère les systèmes d'exploitation invités sur un serveur et contrôle le flux d'instructions entre ces systèmes d'exploitation et le matériel physique.

**3.1.14 infrastructure en tant que service (IaaS)** [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité de nuage fourni au client de services en nuage (§ 3.1.5) correspond à des capacités d'infrastructure.

NOTE – Le client de services en nuage (§ 3.1.5) ne gère pas ni ne contrôle les ressources physiques et virtuelles sous-jacentes, mais contrôle les systèmes d'exploitation, le stockage et les applications déployées qui utilisent les ressources physiques et virtuelles. Le client de services en nuage (§ 3.1.5) peut en outre avoir une capacité limitée de contrôler certains éléments du réseau (par exemple, pare-feux du serveur).

**3.1.15 multilocataires** [b-UIT-T Y.3500]: attribution de ressources physiques ou virtuelles selon laquelle plusieurs locataires (§ 3.1.26) ainsi que leurs calculs et leurs données sont isolés les uns des autres et inaccessibles entre eux.

**3.1.16 réseau en tant que service (NaaS)** [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle la capacité fournie au client de services en nuage (§ 3.1.5) correspond à des capacités de connectivité de transport et à des capacités de réseau connexes.

NOTE – Le réseau NaaS peut fournir l'un quelconque des trois types de capacités de nuage.

**3.1.17 partie** [b-ISO/CEI 27729]: personne physique ou morale, constituée ou non en société, ou groupe de l'une ou l'autre de ces personnes.

**3.1.18 information d'identification personnelle** [b-ISO/CEI 29100]: toute information qui a) peut être utilisée pour identifier la personne à laquelle elle se rapporte, ou b) est ou peut être directement ou indirectement liée à une personne.

**3.1.19 plate-forme en tant que service (PaaS)** [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité de nuage fourni au client du service en nuage (§ 3.1.5) correspond à des capacités de plate-forme.

**3.1.20 nuage privé** [b-UIT-T Y.3500]: modèle de déploiement du nuage où les services en nuage (§ 3.1.4) sont utilisés exclusivement par un seul client de services en nuage (§ 3.1.5) et où les ressources sont contrôlées par le client de services en nuage (§ 3.1.5).

**3.1.21 nuage public** [b-UIT-T Y.3500]: modèle de déploiement du nuage où les services en nuage (§ 3.1.4) peuvent être mis à la disposition de tout client de services en nuage (§ 3.1.5) et où les ressources sont contrôlées par le fournisseur de services en nuage (§ 3.1.7).

**3.1.22 domaine de sécurité** [b-UIT-T X.810]: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est assujetti à la politique de sécurité, pour les activités indiquées et la politique de sécurité est administrée par l'autorité de sécurité pour le domaine de sécurité.

**3.1.23 atteinte à la sécurité** [b-UIT-T E.409]: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

**3.1.24 accord de niveau de service (SLA)** [b-ISO/CEI 20000-1]: accord écrit entre le prestataire de service et le client qui identifie les services et les objectifs de service.

NOTE 1 – Un accord de niveau de service peut également être conclu entre le prestataire de service et un fournisseur, un groupe interne ou un client agissant en qualité de fournisseur.

NOTE 2 – Un accord de niveau de service peut être intégré dans un contrat ou dans un autre type d'accord écrit.

**3.1.25 logiciel en tant que service (SaaS)** [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité en nuage fourni au client de services en nuage (§ 3.1.5) correspond à des capacités d'application.

**3.1.26 locataire** [b-UIT-T Y.3500]: un ou plusieurs utilisateurs de services en nuage (§ 3.1.8) utilisant en partage l'accès à un ensemble de ressources physiques et virtuelles.

**3.1.27 menace** [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, susceptible de nuire à un système ou à une organisation.

**3.1.28 machine virtuelle (VM)** [b-NIST-SP-800-145]: reproduction efficace, isolée et logique d'une machine réelle.

**3.1.29 vulnérabilité** [b-NIST-SP-800-30]: faiblesse dans un système d'information, les procédures de sécurité système, les contrôles internes ou la mise en oeuvre, qui pourrait être exploitée par une source de menace.

### 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

**3.2.1 problème de sécurité**: "souci" de sécurité autre qu'une menace directe de sécurité découlant de la nature et de l'environnement d'exploitation des services de nuage, y compris les menaces "indirectes". Voir les § 7 et 8.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

BCP plan de continuité des activités (*business continuity plan*)

CaaS communication en tant que service (*communications as a service*)

CPU unité centrale de traitement (*central processing unit*)

CSC client de services en nuage (*cloud service customer)*

CSN partenaire de services en nuage (*cloud service partner*)

CSP fournisseur de services en nuage (*cloud service provider*)

CSU utilisateur de services en nuage (*cloud service user*)

DNS système des noms de domaine *(domain name system*)

IaaS infrastructure en tant que service *(infrastructure as a service*)

IAM gestion des identités et de l'accès (*identity and access management*)

IP protocole Internet (*IP Internet protocol*)

IT technologies de l'information (*information technology*)

NaaS réseau en tant que service (*network as a service*)

OS système d'exploitation (*operating system*)

PaaS plate-forme en tant que service (*platform as a service*)

PII information d'identification personnelle (*personally identifiable information*)

PKI infrastructure de clé publique (*public key infrastructure*)

SaaS logiciel en tant que service (*software as a service*)

SIM module d'identification de l'abonné (*subscriber identity module*)

SLA engagement de niveaux de services (*service level agreement*)

TIC technologies de l'information et de la communication

VM machine virtuelle (*virtual machine*)

## 5 Conventions

Aucune.

## 6 Présentation générale

L'informatique en nuage est un modèle permettant d'offrir un accès pratique, à la demande et via le réseau à un ensemble mutualisé de ressources configurables (par exemple réseaux, serveurs, mémoires, applications et services), qui peuvent être configurées et libérées rapidement moyennant un effort de gestion minime et une interaction minime avec le fournisseur de service. Les clients de services d'informatique en nuage peuvent utiliser ces ressources pour développer, héberger et exécuter des services et des applications à la demande et de manière souple sur n'importe quel dispositif, à tout moment et en tout lieu, dans l'environnement de l'informatique en nuage. Les services d'informatique en nuage sont en règle générale fournis par catégorie de services, par exemple infrastructure en tant que service (IaaS), plate-forme en tant que service (PaaS), réseau en tant que service (NaaS), parmi bien d'autres. Ces catégories de services, d'une part, permettent aux clients de services d'informatique en nuage de lancer ou de modifier leurs activités rapidement et facilement, sans mettre en place de nouvelles infrastructures et de nouveaux systèmes de technologies de l'information et de la communication (TIC) et, d'autre part, offrent la possibilité de fournir des ressources de manière élastique, en fonction des besoins. Par exemple, certains fournisseurs de services en nuage (CSP) peuvent fournir des ressources matérielles et logicielles sous forme abstraite pouvant être offertes en tant que services (par exemple, infrastructure IaaS ou réseau NaaS). D'autres fournisseurs CSP peuvent fournir des plates-formes (PaaS) ou des applications (SaaS) propres au nuage, qui permettront aux clients et aux partenaires de concevoir et de déployer rapidement de nouvelles applications pouvant être configurées et utilisées à distance.

L'adoption de l'informatique en nuage va de pair avec des menaces et des problèmes de sécurité et les exigences de sécurité varient considérablement selon les modèles de déploiement des services d'informatique en nuage et les catégories de services. Etant donné qu'elle a par nature une architecture répartie et multilocataires, que, dans la plupart des cas, l'accès se fait à distance et que chaque processus fait intervenir plusieurs entités, l'informatique en nuage est intrinsèquement plus exposée que d'autres modèles aux menaces de sécurité, qu'elles soient intérieures ou extérieures. L'application de processus et de mécanismes de sécurité classiques permet de limiter nombre de menaces de sécurité. La sécurité concerne et affecte de nombreux éléments d'un service d'informatique en nuage.

Par conséquent, la gestion de la sécurité des services d'informatique en nuage ainsi que des ressources associées est un aspect essentiel de l'informatique en nuage.

Avant d'adopter l'informatique en nuage pour son système TIC, un client de services d'informatique en nuage (CSC) potentiel devrait recenser les menaces de sécurité (voir le § 7) et les problèmes de sécurité (voir le § 8) auxquels il s'expose.

Sur la base de ces menaces et problèmes, un ensemble de capacités de sécurité de haut niveau (voir le § 9) est identifié. La présente Recommandation ne traite pas des exigences spécifiques concernant ces capacités, qui devront toutefois être identifiées pour les applications particulières des services d'informatique en nuage, à partir d'une évaluation des risques par rapport aux menaces et problèmes recensés.

Sur la base de l'évaluation des risques, un client CSC peut décider ou non d'adopter l'informatique en nuage et choisir des fournisseurs et une architecture de service en connaissance de cause. Il conviendrait de procéder à l'évaluation des risques susmentionnée en utilisant un cadre de gestion des risques de sécurité de l'information (par exemple, le cadre de gestion des risques défini dans la norme [b-ISO/CEI 27005]). Voir également le § 10 ci-dessous qui propose une méthode générale.

La présente Recommandation fait une distinction entre les menaces de sécurité et les problèmes de sécurité. Les menaces de sécurité sont liées à des attaques (actives et passives), ainsi qu'à des dysfonctionnements de l'environnement ou à des catastrophes, tandis que les problèmes de sécurité sont ceux qui découlent de la nature et de l'environnement d'exploitation des services en nuage. Lorsqu'ils ne sont pas traités comme il se doit, les problèmes de sécurité peuvent constituer une "porte d'entrée" pour les menaces.

Sur la base des menaces et des problèmes de sécurité recensés, on décrit les capacités de sécurité qui permettront d'atténuer les menaces de sécurité et de résoudre les problèmes de sécurité liés à l'informatique en nuage.

## 7 Menaces de sécurité visant l'informatique en nuage

Les menaces peuvent endommager des ressources comme l'information, les processus et les systèmes et, par conséquent, nuire aux organisations. Une menace peut être d'origine naturelle ou humaine, accidentelle ou intentionnelle. Elle peut venir de l'intérieur ou de l'extérieur de l'organisation. Une menace peut être accidentelle ou intentionnelle et active ou passive.

Les différentes menaces rencontrées dépendent avant tout du type de services en nuage retenu. Par exemple, dans le cas d'un nuage public, les menaces peuvent être dues à la répartition des responsabilités entre le client CSC et le fournisseur CSP: complexité de la répartition des responsabilités en ce qui concerne les données et les processus, cohérence et pertinence de la protection des données et protection de la confidentialité, etc. En revanche, dans le cas d'un nuage privé, les menaces sont plus simples à traiter, car le client CSC contrôle tous les locataires hébergés par le fournisseur CSP. Bien que certaines des menaces recensées dans la présente Recommandation fassent également l'objet de documents élaborés par le secteur (par exemple, la Recommandation UIT-T X.800), toutes concernent l'informatique en nuage. La réalité des différentes menaces dépendra du type de service considéré.

Le présent paragraphe décrit les différentes menaces de sécurité que l'on peut rencontrer dans l'environnement de l'informatique en nuage.

### 7.1 Menaces de sécurité visant les clients de services en nuage (CSC)

Les menaces présentées ci-après sont celles qui visent directement les clients CSC. Elles peuvent concerner les intérêts personnels ou professionnels, la confidentialité, la légalité ou la sécurité d'un client CSC. Les clients CSC ne sont pas tous concernés par toutes les menaces. Le risque variera en fonction de la nature du client CSC et du service d'informatique en nuage qu'il utilise. Par exemple,

un service en nuage utilisé pour le transcodage des fichiers vidéo commerciaux n'est soumis à aucune exigence en matière de protection des données d'identification personnelles (PII), mais devra respecter des exigences très strictes en ce qui concerne la protection des ressources numériques.

### 7.1.1 Perte et fuite de données

Etant donné que l'environnement des services en nuage a, en règle générale, une architecture multilocataires, la perte ou la fuite de données représente une grave menace pour le client CSC. L'absence de gestion appropriée des informations cryptographiques, comme les clés de chiffrement, les codes d'authentification et le privilège d'accès, pourrait entraîner des préjudices considérables, tels que la perte de données ou une fuite inattendue de données vers l'extérieur. Par exemple, l'insuffisance des contrôles d'authentification, d'autorisation et de vérification, la mauvaise utilisation des clés de chiffrement et/ou d'authentification, les défaillances opérationnelles, les problèmes de destruction des données, les questions de juridiction et de politique, la fiabilité des centres de données et le rétablissement après une catastrophe sont reconnus comme étant au nombre des principales sources de ce type de menaces et peuvent être associés aux problèmes décrits dans les § 8.1.2 "Perte de confiance", 8.1.3 "Perte de gouvernance" et 8.1.4 "Perte de confidentialité".

### 7.1.2 Accès non sécurisé aux services

Les justificatifs d'identité, y compris ceux des administrateurs CSC, sont particulièrement vulnérables face aux utilisateurs non autorisés dans l'environnement très réparti de l'informatique en nuage, étant donné qu'à l'inverse des télécommunications traditionnelles, il est souvent difficile de s'appuyer sur un emplacement (par exemple, une ligne fixe) ou sur la présence d'un élément matériel particulier (par exemple, un module d'identité de l'abonné mobile (SIM)) pour renforcer l'authentification de l'identité. Dans la mesure où la plupart des offres de services portent sur des services à distance, les connexions non protégées sont synonymes de vulnérabilités potentielles. Même lorsque les connexions sont protégées ou locales, d'autres méthodes d'attaque (hameçonnage, usurpation, ingénierie sociale, exploitation des failles logicielles, etc.) peuvent réussir. Si un attaquant parvient à accéder aux justificatifs d'identité des utilisateurs ou des administrateurs, il peut espionner les activités et les transactions, manipuler les données, renvoyer des informations falsifiées et rediriger les clients d'un client CSC vers des sites illégaux. Un même mot de passe est souvent utilisé pour plusieurs sites web et services, ce qui accroît l'ampleur de ces attaques, étant donné que le craquage d'un seul mot de passe rend vulnérables plusieurs services. Les solutions d'informatique en nuage font par ailleurs naître une menace nouvelle dans cet environnement. Les instances de compte ou de service du client CSC peuvent devenir, pour l'attaquant, un nouveau point de départ à partir duquel il peut utiliser la réputation et les ressources du client CSC pour lancer de nouvelles attaques.

### 7.1.3 Menaces internes

Lorsqu'une activité implique une intervention humaine, le risque est toujours présent que des personnes agissent au détriment de la sécurité du service. Les employés d'un client CSC qui communiquent les mots de passe "administrateur" ou qui, d'une manière ou d'une autre, ne protègent pas leurs justificatifs d'identité (par exemple, en les notant sur un post-it collé sur un écran), les utilisateurs négligents ou mal formés (ou les membres d'une famille dans le cas d'une configuration chez des particuliers) ou encore des actions malveillantes de la part d'employés aigris, représenteront toujours une menace importante.

## 7.2 Menaces de sécurité visant les fournisseurs de services en nuage (CSP)

Cette partie recense les menaces qui visent directement les fournisseurs CSP. Ces menaces pourraient nuire à la capacité des fournisseurs CSP de proposer des services, de mener des activités, de conserver des clients et d'éviter des problèmes sur le plan juridique ou réglementaire. Les menaces visant un fournisseur CSP donné dépendront également des services que celui-ci propose et des environnements dans lesquels il évolue.

### 7.2.1 Accès non autorisé aux fonctions d'administration

Tout service d'informatique en nuage comprendra des interfaces et des composants logiciels grâce auxquels le personnel du client CSC pourra administrer les aspects du service d'informatique en nuage qui relèvent du client CSC (ajout ou suppression de comptes employé, connexions aux serveurs du client CSC, modifications de la capacité du service, mise à jour des entrées du système de noms de domaine (DNS) et des sites web, etc.). Ces interfaces administratives peuvent devenir des cibles de choix pour les attaquants, qui se font passer pour des administrateurs du client CSC afin d'attaquer un fournisseur CSP. Etant donné que le personnel du client CSC doit pouvoir avoir accès à ces services d'informatique en nuage, la protection desdits services devient une préoccupation de premier plan pour la sécurité de l'informatique en nuage.

### 7.2.2 Menaces internes

Lorsqu'une activité implique une intervention humaine, le risque est toujours présent que des personnes fassent preuve de malveillance ou de négligence et ainsi fragilisent la sécurité du service.

Les employés d'un fournisseur CSC qui communiquent les mots de passe "administrateur" ou qui, d'une manière ou d'une autre, ne protègent pas leurs justificatifs d'identité (par exemple, en les notant sur un post-it collé sur un écran), les utilisateurs négligents ou mal formés ou encore des actions malveillantes de la part d'employés aigris représenteront toujours une menace importante pour n'importe quelle entreprise.

En particulier, les fournisseurs CSP doivent déterminer avec sérieux si leurs propres employés sont dignes de confiance. Aucune sélection des employés, aussi rigoureuse soit elle, ne permet d'éliminer totalement le risque qu'un intrus habile parvienne à se faire recruter dans un centre de données du fournisseur CSP. Cet intrus peut chercher à nuire au fournisseur CSP ou à s'introduire dans certains systèmes d'un client CSC pris en charge, en particulier si ce client est une entreprise de renom ou un organisme public.

## 8 Problèmes de sécurité posés par l'informatique en nuage

Les problèmes de sécurité vont au-delà des menaces de sécurité qui découlent de la nature et de l'environnement de fonctionnement des services en nuage, y compris les menaces "indirectes". On entend par menace indirecte une menace qui vise un seul participant d'un service en nuage, mais qui peut avoir des conséquences néfastes pour d'autres participants.

La présente Recommandation recense les problèmes qui, s'ils ne sont pas traités comme il se doit, peuvent constituer une "porte d'entrée" pour les menaces. Ces problèmes doivent être examinés lorsqu'on envisage d'avoir recours à des services d'informatique en nuage.

### 8.1 Problèmes de sécurité pour les clients de services en nuage (CSC)

Le présent paragraphe décrit les problèmes de sécurité associés aux problèmes liés à l'environnement ou aux menaces indirectes qui peuvent engendrer des menaces plus directes pour les intérêts du client CSC.

### 8.1.1 Répartition ambiguë des responsabilités

Les clients CSC consomment des ressources fournies dans le cadre de catégories de services différentes et selon des modèles de déploiement différents. Le système TIC construit autour du client dépend donc de ces services. Des contradictions conceptuelles et opérationnelles risquent d'apparaître lorsque les responsabilités ne sont pas clairement réparties entre les clients CSC et les fournisseurs CSP. Toute incohérence contractuelle concernant les services fournis pourrait se traduire par une anomalie ou des incidents. Par exemple, la question de savoir quelle entité contrôle les données et quelle entité les traite peut être floue au niveau international, même si la dimension internationale est minime et se limite à un tiers en dehors d'une région donnée, comme l'Union européenne.

En raison des contraintes légales et réglementaires, tout doute en la matière (par exemple, savoir qui du client CSC ou du fournisseur CSP contrôle ou traite les données) peut amener une ambigüité quant à la réglementation à appliquer. Si cette interprétation varie d'une juridiction à l'autre, un client CSC ou un fournisseur CSP pourrait se trouver soumis à des réglementations contradictoires pour un même service ou ensemble de données.

### 8.1.2 Perte de confiance

Il est parfois difficile pour un client CSC de reconnaître le niveau de confiance de leur fournisseur CSP, car le service d'informatique en nuage fonctionne comme une boîte noire. S'il n'existe aucun moyen d'obtenir et de partager le niveau de sécurité du fournisseur de manière formelle, les clients CSC ne disposent d'aucun moyen pour évaluer le niveau de mise en oeuvre de la sécurité atteint par le fournisseur. Le fait que le CSP ne partage pas suffisamment d'informations de sécurité pourrait devenir une menace de sécurité importante pour certains clients CSC lorsqu'ils utilisent les services d'informatique en nuage.

### 8.1.3 Perte de gouvernance

Pour un client CSC, le fait de transférer une partie de son propre système TIC vers une infrastructure d'informatique en nuage revient à concéder un contrôle partiel à un fournisseur CSP, ce qui pourrait représenter une menace importante pour les données du client CSC, notamment en ce qui concerne le rôle et l'attribution des privilèges au fournisseur. Si à cela s'ajoute un manque de transparence des pratiques du fournisseur de services d'informatique en nuage, il en résulte un risque de mauvaise configuration, ou même d'attaques malveillantes de l'intérieur.

Lorsqu'ils adoptent des services d'informatique en nuage, certains clients CSC éprouveront peut-être des préoccupations à l'idée de ne plus maîtriser leurs informations et leurs ressources hébergées par le fournisseur CSP, le stockage des données, la fiabilité des sauvegardes des données (problèmes de rétention des données), les contre-mesures permettant de mettre en oeuvre les plans de continuité d'activités (BCO) et d'assurer le rétablissement après une catastrophe, etc.

Par exemple:

- Un client CSC souhaite supprimer un fichier pour des raisons juridiques, mais le fournisseur CSP conserve une copie sans que le client CSC le sache.
- Un fournisseur CSP accorde des privilèges d'administrateur pour le client CSC, qui vont au-delà de ce que la politique du client CSC permet.
- Certains clients CSC craignent peut-être qu'un fournisseur CSP permette à des gouvernements étrangers d'accéder aux données, ce qui pourrait avoir une incidence sur le respect par les clients CSC des lois sur la confidentialité, par exemple aux directives de l'Union européennes relatives à la protection des données.

### 8.1.4 Perte de confidentialité

Lorsqu'un fournisseur CSP traite des informations confidentielles, il existe un risque de violation de la confidentialité, notamment de violation de la réglementation, des certificats ou de la législation applicables sur la protection des données. Il pourra s'agir de la fuite d'informations confidentielles ou du traitement d'informations d'identification personnelle (PII) à des fins pour lesquelles le client CSC et/ou le sujet des données n'a pas donné son autorisation.

### 8.1.5 Indisponibilité des services

La disponibilité n'est pas propre à l'environnement de l'informatique en nuage. Toutefois, étant donné qu'elle obéit au principe de conception orientée sur les services, la fourniture d'un service peut être perturbée lorsque les services d'informatique en nuage en amont ne sont pas totalement disponibles.

Par ailleurs, la dépendance dynamique de l'informatique en nuage multiplie les possibilités pour un attaquant. Par exemple, une attaque par déni de service sur un service en amont peut avoir des répercussions sur plusieurs services en aval du même système d'informatique en nuage.

### 8.1.6 Enfermement vis-à-vis du fournisseur de services d'informatique en nuage

Lorsqu'on dépend trop d'un seul fournisseur CSP, il peut être difficile de changer de fournisseur CSP. Ce cas de figure peut se présenter, par exemple, lorsqu'un fournisseur CSP utilise des fonctions et des formats qui ne sont pas normalisée et n'assure pas l'interopérabilité. Cette situation peut devenir une menace pour la sécurité si le fournisseur CSP "captif" ne parvient pas à résoudre les failles de sécurité connues, rendant ainsi le client CSC vulnérable, sans pour autant qu'il ait la possibilité de se tourner vers un autre fournisseur CSP.

### 8.1.7 Détournement de la propriété intellectuelle

Lorsque le fournisseur CSP exécute le logiciel ou stocke d'autres ressources d'un client CSC, il existe un risque que ces données soient divulguées à des tiers ou détournées à des fins non autorisées. Cette situation peut donner lieu à des atteintes au droit d'auteur et à la divulgation de secrets commerciaux.

### 8.1.8 Perte d'intégrité d'un logiciel

Lorsque le logiciel d'un client CSC est exécuté dans le système du fournisseur CSP, il est possible que ce logiciel soit modifié ou altéré lorsqu'il n'est plus sous le contrôle direct du client CSC, le logiciel se comportant alors de manière anormale. Même si le client CSC n'a aucune responsabilité concernant ce risque, sa réputation et, par conséquent, ses activités peuvent en pâtir.

## 8.2 Problèmes de sécurité pour les fournisseurs de services en nuage (CSP)

Le présent paragraphe décrit les problèmes de sécurité associés aux problèmes liés à l'environnement ou aux menaces indirectes qui peuvent engendrer des menaces plus directes pour les intérêts du fournisseur CSP.

### 8.2.1 Répartition ambiguë des responsabilités

Différents rôles (fournisseur CSP, client CSC et partenaire CSN) peuvent être définis dans un système d'informatique en nuage. Une définition ambiguë des responsabilités pour des questions comme la propriété des données, le contrôle de l'accès ou la maintenance de l'infrastructure peut avoir une incidence sur les activités ou donner lieu à des poursuites (en particulier en cas de présence d'un tiers ou lorsque le CSP est également un client CSC ou un partenaire CSN). Ce risque augmente lorsque le fournisseur CSP exploite et/ou propose des services sur plusieurs juridictions où il se peut que les contrats et les accords soient rédigés dans différentes langues et assujettis à des cadres juridiques différents. Voir également le § 8.2.4 "Conflit juridictionnel".

### 8.2.2 Environnement partagé

L'informatique en nuage permet de réduire considérablement les coûts moyennant la mutualisation à très grande échelle de très nombreuses ressources. Cette situation fragilise de nombreuses interfaces potentiellement vulnérables. Par exemple, lorsque plusieurs clients CSC consomment simultanément des services fournis par le même nuage, un client CSC pourrait accéder sans autorisation aux machines virtuelles, au trafic réseau, aux données effectives/résiduelles, etc, d'autres locataires. Tout accès non autorisé ou à des fins malveillantes aux ressources d'un autre client CSC pourrait compromettre l'intégrité, la disponibilité et la confidentialité.

Par exemple, plusieurs machines virtuelles hébergées sur un même serveur physique partagent à la fois l'unité centrale de traitement (CPU) et les ressources de mémoire qui sont virtualisées par l'hyperviseur. Il peut par exemple y avoir une défaillance des mécanismes d'isolation de l'hyperviseur, qui permettrait d'accéder sans autorisation à la mémoire ou au stockage d'autres machines virtuelles.

### 8.2.3 Incohérence ou conflit entre les mécanismes de protection

L'infrastructure de l'informatique en nuage ayant une architecture décentralisée, ses mécanismes de protection peuvent présenter des incohérences entres les différents modules de sécurité répartis. Par exemple, il se peut qu'un accès refusé par un module de sécurité soit autorisé par un autre. Cette incohérence peut poser des problèmes à un utilisateur autorisé et être exploitée par un attaquant, ce qui compromettra la confidentialité, l'intégrité et la disponibilité.

### 8.2.4 Conflit juridictionnel

Les données stockées dans le nuage peuvent être transférées d'un centre de données à un autre, voire changer de pays. En fonction du pays dans lequel elles sont hébergées, les données seront soumises à des législations différentes. Par exemple, certaines juridictions, comme l'Union européenne, imposent une protection très stricte des informations d'identification personnelles (PII), lesquelles ne peuvent normalement pas être traitées dans des lieux qui n'offrent pas un niveau suffisant de protection garantie. Autre exemple, certaines juridictions pourront considérer que la communication en tant que service (CaaS) est un service d'information non réglementé, alors que pour d'autres, elle sera traitée comme un service téléphonique réglementé. Ce conflit juridictionnel peut être source de complications sur le plan juridique et avoir des incidences sur la sécurité, par exemple les règles régissant l'interception licite des communications par les autorités chargées de l'application des lois, ce qui risque d'influer sur les décisions en matière de cryptographie.

### 8.2.5 Risques liés à l'évolution

L'un des avantages de l'informatique en nuage est qu'elle permet de différer certains choix de la phase de conception du système à la phase d'exécution. Ainsi, il se peut que certains éléments logiciels dépendants composant un système ne soient choisis et mis en oeuvre qu'une fois exécutée la fonction pour laquelle ils sont requis. Or, les méthodes conventionnelles d'évaluation des risques ne peuvent plus être appliquées à ce type de systèmes dont l'évolution est dynamique. De nouvelles vulnérabilités peuvent en effet apparaître dans un système tout au long de sa durée de vie du fait des modifications apportées à ses éléments logiciels, alors que ce système avait fait l'objet d'une évaluation de sécurité positive au moment de sa conception.

### 8.2.6 Migration et intégration médiocres

La migration vers le nuage suppose souvent le transfert de gros volumes de données et des modifications de configuration majeures (par exemple, adressage du réseau). La migration d'une partie d'un système TIC vers un fournisseur CSP extérieur pourrait nécessiter de revoir en profondeur la conception du système (par exemple, politiques de réseau et de sécurité). Une intégration médiocre due à l'incompatibilité des interfaces ou à l'application incohérente des politiques pourrait avoir des incidences fonctionnelles et non fonctionnelles. Par exemple, des machines virtuelles qui fonctionnent derrière un pare-feu dans un centre de données privé sont accidentellement exposées à l'Internet ouvert dans le nuage du fournisseur CSP.

### 8.2.7 Discontinuité de l'activité

L'informatique en nuage consiste à attribuer des ressources et à les fournir sous forme de services. L'écosystème de l'informatique en nuage dans sa globalité est composé de nombreux éléments interdépendants. Tout dysfonctionnement de l'un quelconque de ces éléments (par exemple, coupure d'alimentation électrique, déni de service ou retard) risque de nuire à la disponibilité des services d'informatique en nuage (voir le § 8.1.5 "Indisponibilité des services") et entraîner par la suite une discontinuité de l'activité.

### 8.2.8 Enfermement vis-à-vis d'un partenaire de services en nuage

La plate-forme du fournisseur CSP est composée d'éléments logiciels et matériels provenant de différents fabricants. Certains de ces éléments peuvent comprendre des fonctionnalités ou des extensions propriétaires utiles pour les fournisseurs CSP. Toutefois, le fait de dépendre de ces fonctionnalités propriétaires restreint la capacité du fournisseur CSP de changer de fabricants.

L'enfermement est un problème commercial, mais ne constitue pas une menace de sécurité à proprement parler. Dans certains cas, il peut toutefois finir par poser des problèmes sur le plan de la sécurité. Par exemple, la faillite d'un partenaire CSN fournissant un élément essentiel peut signifier qu'aucun nouveau correctif de sécurité ne sera plus disponible. Si une vulnérabilité apparaît dans l'élément en question, il peut être très difficile ou coûteux d'éliminer le risque correspondant.

### 8.2.9 Vulnérabilité de la chaîne d'approvisionnement

Un fournisseur CSP est fragilisé si le matériel ou le logiciel fourni à la plate-forme par l'intermédiaire de sa chaîne d'approvisionnement menace la sécurité du client CSC ou du fournisseur CSP, par exemple dans le cas de l'introduction accidentelle ou intentionnelle d'un logiciel malveillant ou de failles pouvant être exploitées.

Il peut s'agir, par exemple, de la fourniture d'un logiciel défaillant par le partenaire CSN. Ce problème de sécurité se pose lorsque le logiciel fourni par un partenaire CSN est exécuté dans un système du fournisseur CSP, par exemple l'interface client, le système d'exploitation (OS) invité d'une machine virtuelle (VM), des applications, des éléments de plate-forme ou un logiciel d'audit/de suivi (par exemple, si le partenaire fournit un service d'audit).

Autre exemple, un fournisseur CSP exécute un logiciel fourni par un partenaire; le fournisseur CSP est fragilisé si le partenaire n'arrive pas à fournir rapidement les mises à jour de sécurité requises.

### 8.2.10 Dépendance entre les logiciels

Lorsqu'une vulnérabilité est détectée, il n'est pas toujours possible d'appliquer immédiatement les mises à jour car celles-ci interrompraient l'exécution d'autres éléments logiciels (alors que sans cela, ces éléments ne nécessiteraient pas de mise à jour). Cela est d'autant plus vrai s'il existe une relation de dépendance entre des éléments fournis par un ou plusieurs partenaires CSN et non par le fournisseur CSP lui-même.

## 8.3 Problèmes de sécurité pour les partenaires de services en nuage (CSN)

Le présent paragraphe porte sur les problèmes qui touchent directement les partenaires CSN. Ces problèmes peuvent nuire à la capacité d'un partenaire CSN de mener des activités, d'être payé, de protéger ses actifs de propriété intellectuelle et d'éviter des problèmes sur le plan juridique ou réglementaire. Les problèmes de sécurité pour un partenaire CSN donné dépendront de ses activités et des environnements dans lesquels il évolue (par exemple, développement, intégration, audit, etc.).

### 8.3.1 Répartition ambiguë des responsabilités

Lorsque le service exécute des logiciels fournis par des fournisseurs CSP et des partenaires CSN, le client CSC ne saura peut-être pas à qui incombe la responsabilité d'atténuer et de traiter les incidents de sécurité. Il peut être très difficile d'établir quelle est l'entité responsable sur la base d'une analyse technique. Le fournisseur CSP et le ou les partenaires CSN pourraient par conséquent se renvoyer mutuellement la faute, ce qui pourrait entraîner de nouvelles failles de sécurité si l'origine du problème n'est pas identifiée.

### 8.3.2 Détournement de la propriété intellectuelle

Lorsqu'un partenaire fournit des logiciels ou d'autres ressources au fournisseur CSP pour qu'il les exécute, le risque pour la sécurité est que ces données soient divulguées à des tiers ou détournées à des fins non autorisées. Cette situation peut donner lieu à des atteintes au droit d'auteur et à la divulgation de secrets commerciaux.

### 8.3.3 Perte d'intégrité d'un logiciel

Lorsque le logiciel d'un partenaire est exécuté dans le système du fournisseur CSP, il se peut que ce logiciel soit modifié ou altéré lorsqu'il n'est plus sous le contrôle direct du partenaire CSN, le logiciel se comportant alors de manière anormale. Même si le partenaire CSN n'a aucune responsabilité concernant ce risque, sa réputation et, par conséquent, ses activités peuvent en pâtir.

## 9 Capacités de sécurité de l'informatique en nuage

La présente Recommandation décrit ci-après des capacités de sécurité qui permettront de remédier aux menaces et aux problèmes de sécurité identifiés pour l'informatique en nuage. Les paramètres de ces capacités de sécurité pourront être précisés dans les conventions de niveaux de services (SLA), par exemple, le délai d'intervention en cas d'incident.

### 9.1 Modèle de confiance

Tout système dans lequel plusieurs fournisseurs coopèrent pour fournir un service fiable nécessite un modèle de confiance commun.

Etant donné qu'il a par nature une architecture très répartie et fait intervenir de multiples parties prenantes, l'environnement de l'informatique en nuage devra comprendre un modèle de confiance général. Ce modèle de confiance permettra de créer des îlots et/ou des fédérations d'entités de confiance, de telle sorte que des éléments distincts du système pourront authentifier l'identité et les droits autorisés d'autres entités et éléments. Chaque îlot ou fédération de confiance reposera sur une ou plusieurs autorités de confiance (par exemple, une autorité délivrant des certificats d'infrastructure de clé publique (PKI)).

Il existe aujourd'hui un grand nombre de modèles de confiance pouvant être utilisés pour l'informatique en nuage ou d'autres types d'architecture. Le modèle de confiance précis à adopter ne relève pas de la présente Recommandation.

### 9.2 Gestion des identités et de l'accès (IAM), authentification, autorisation et audit des transactions

Plusieurs administrateurs et utilisateurs interviennent dans les services d'informatique en nuage. De plus, il est possible d'accéder à ces services et de les utiliser depuis l'intérieur (fournisseurs CSP) ou depuis l'extérieur (clients CSC). Il est donc nécessaire de gérer les identités, non seulement pour protéger ces identités, mais aussi pour faciliter les processus de gestion de l'accès, d'authentification, d'autorisation et d'audit des transactions dans l'infrastructure dynamique et ouverte qui caractérise l'informatique en nuage.

La gestion IAM a besoin d'un ou plusieurs modèles de confiance (§ 9.1) communs pour authentifier les identités; les développeurs, les hyperviseurs et d'autres éléments du système ont eux aussi besoin de ces modèles de confiance pour authentifier les éléments du système comme les modules logiciels, les applications ou les ensembles de données téléchargés.

La gestion IAM contribue à la confidentialité, à l'intégrité et à la disponibilité des services et des ressources et devient à ce titre incontournable dans l'informatique en nuage.

En outre, la gestion IAM peut permettre de mettre en oeuvre l'authentification unique et la fédération d'identités pour les nuages qui utilisent des mécanismes d'authentification différents ou qui sont répartis dans des domaines de sécurité différents.

L'audit des transactions protège contre la répudiation, permet une analyse sur le plan légal après une atteinte à la sécurité et dissuade les attaques (qu'elles viennent de l'intérieur ou de l'extérieur). L'audit des transactions est plus qu'un simple enregistrement, puisqu'il comprend une surveillance active pour repérer les activités suspectes.

### 9.3 Sécurité physique

Il est nécessaire d'assurer la sécurité physique. L'accès aux locaux hébergeant les équipements du fournisseur CSP est limité aux personnes autorisées, qui, de plus, ne pourront accéder qu'aux espaces directement nécessaires pour leur travail; ce point fait partie du processus de gestion IAM. Toutefois, le niveau de sécurité physique dépendra de la valeur des données et du nombre de clients pour lesquels l'accès est autorisé.

### 9.4 Sécurité des interfaces

Cette capacité sécurise, d'une part, les interfaces ouvertes aux clients CSC et/ou à d'autres fournisseurs CSP sous-traitants par l'intermédiaire desquels différents types de services d'informatique en nuage sont fournis et, d'autre part, les communications fondées sur ces interfaces. Les mécanismes disponibles pour assurer la sécurité des interfaces sont notamment les suivants: authentification unilatérale/mutuelle, total de contrôle d'intégrité, chiffrement de bout en bout, signature numérique, etc.

### 9.5 Sécurité de la virtualisation informatique

Par sécurité de virtualisation informatique, on entend la sécurité de l'environnement de virtualisation informatique dans son ensemble. Elle protège l'hyperviseur contre les attaques, ainsi que la plate-forme du serveur contre les menaces venant de l'environnement de virtualisation informatique, et sécurise les machines virtuelles tout au long de leur cycle de vie. En particulier, cette capacité permet d'isoler les machines virtuelles et de protéger les images de machines virtuelles ainsi que les instances de machines virtuelles suspendues pendant la durée du stockage et au cours des transferts.

Pour le fournisseur CSP, l'hyperviseur offre souvent une protection pour les machines virtuelles hébergées, par exemple en fournissant un traitement anti-virus et anti-spam à l'intérieur des hyperviseurs, de telle manière que les machines virtuelles n'ont pas à mettre en oeuvre ces fonctions chacune de leur côté. L'hyperviseur sera normalement configuré avec l'ensemble minimum de services. En règle générale, les interfaces et interfaces de programmation d'application (API) superflues seront fermées et les éléments de service inutiles désactivés.

Les machines virtuelles concernées par cette capacité sont celles créées par un client CSC dans le cadre d'un logiciel SaaS, ainsi que toute machine virtuelle créée par un logiciel SaaS et une plate-forme PaaS. En règle générale, les machines virtuelles seront bien isolées les unes des autres lorsqu'elles partagent des mémoires, une unité centrale de traitement (CPU) et des capacités de stockage. Elles auront normalement des capacités de sécurité intrinsèques et une connaissance des politiques (par exemple, dans le système d'exploitation invité).

### 9.6 Sécurité du réseau

Dans l'environnement de l'informatique en nuage, la sécurité du réseau permet d'isoler à la fois le réseau physique et le réseau virtuel et de sécuriser les communications entre tous les participants. Elle permet de procéder à la partition des domaines de sécurité du réseau, de contrôler l'accès aux frontières du réseau (par exemple, avec un pare-feu), de détecter et d'empêcher les intrusions, d'assurer la séparation du trafic dans le réseau en fonction des politiques de sécurité et de protéger le réseau contre les attaques dans les environnements de réseaux virtuels ou physiques.

### 9.7 Isolation et protection des données et protection de la confidentialité

Cette capacité permet de résoudre des problèmes généraux de protection des données, qui ont souvent des incidences juridiques.

- Isolation des données

Dans le contexte de l'informatique en nuage, un locataire ne peut pas accéder à des données appartenant à un autre locataire, même lorsque les données sont cryptées, sauf autorisation explicite. L'isolation des données peut être logique ou physique, selon la granularité d'isolation requise et le modèle de déploiement des logiciels et des équipements d'informatique en nuage utilisés.

NOTE 1 – Dans le cas de l'informatique en nuage, l'isolation se fait au niveau du locataire. Un client CSC donné peut avoir plusieurs locataires dans le nuage, par exemple pour séparer ses différentes filiales, divisions ou unités organisationnelles.

- Protection des données

La protection des données garantit que les données du client CSC et les données dérivées détenues dans un environnement d'informatique en nuage sont protégées comme il se doit, afin que seules les personnes ou entités autorisées par le client CSC (ou conformément à la législation applicable) puissent avoir accès à ces données ou les modifier. Cette protection peut associer plusieurs méthodes: listes de contrôle d'accès, vérification de l'intégrité, correction des erreurs/récupération des données, chiffrement et autres mécanismes appropriés.

Lorsqu'un fournisseur CSP assure le chiffrement des mémoires pour les clients CSC, cette fonction peut correspondre à un chiffrement du côté du client (par exemple, dans une application CSP) ou du côté du serveur.

- Protection de la confidentialité

Les informations privées peuvent être des informations d'identification personnelles ou des données d'entreprise confidentielles. La collecte, l'utilisation, le transfert, le traitement, le stockage et la destruction d'informations privées peuvent être soumises à la réglementation ou à la législation sur la confidentialité. Cette restriction s'applique à la fois aux fournisseurs CSP et à leurs clients CSC. Par exemple, un client CSC doit pouvoir à tout moment détruire une table de données contenant des informations privées, même si le fournisseur CSP ne connaît pas le contenu de cette table. Les fournisseurs CSP devront peut-être par ailleurs prendre en charge le traitement, par exemple en faisant une recherche dans les données du client CSC sous leur forme transformée ou cryptée.

La protection de la confidentialité concerne également les informations privées qui peuvent être observées dans le cadre des activités du client CSC ou déduites de celles-ci, comme les tendances commerciales, les relations et les communications avec d'autres parties, les niveaux et modèles d'activité, etc.

La protection de la confidentialité doit également permettre de garantir que toutes les informations privées (données observées ou déduites) sont utilisées uniquement aux fins convenues entre un client CSC et le fournisseur CSP.

Une évaluation des risques pour les informations privées (appelée "évaluation des risques liés à la confidentialité") peut aider un fournisseur CSP à identifier les risques précis d'atteinte à la confidentialité associés à une opération envisagée. Le fournisseur CSP devrait identifier et mettre en oeuvre des capacités afin de remédier aux risques concernant la confidentialité mis en évidence dans le cadre de l'évaluation des risques et traiter les informations privées.

NOTE 2 – Dans certaines juridictions, les personnes physiques (c'est-à-dire des utilisateurs humains) sont considérées séparément de leurs employeurs à des fins de confidentialité. Dans ce cas, la confidentialité de l'utilisateur de services en nuage (CSU) sera protégée comme il se doit, de même que celle du client CSC et du locataire de services en nuage.

### 9.8 Coordination de la sécurité

Etant donné que différents services d'informatique en nuage supposent différentes mises en oeuvre de contrôle de sécurité, cette capacité de sécurité coordonne des mécanismes de sécurité hétérogènes pour éviter les conflits en matière de protection.

Les parties jouant différents rôles dans l'écosystème de l'informatique en nuage (par exemple, fournisseur CSP, client CSC ou partenaire CSN) ont des niveaux différents de contrôle des ressources et des services physiques ou virtuels, notamment en ce qui concerne le contrôle de la sécurité.

Pour chaque partie, il y aura divers mécanismes de sécurité, comme l'isolation du superviseur, la gestion IAM, la protection de réseau, etc.

L'une des finalités de l'informatique en nuage est de permettre l'association de ces différentes parties pour concevoir, construire, déployer et exploiter collectivement différentes ressources physiques et virtualisées. Par conséquent, un fournisseur CSP doit pouvoir coordonner les différents mécanismes de sécurité des différentes parties. La coordination de la sécurité dépend de l'interopérabilité et de l'harmonisation des divers mécanismes de sécurité.

### 9.9 Sécurité opérationnelle

Cette capacité assure une protection de sécurité pour le fonctionnement et la maintenance au quotidien des services et de l'infrastructure d'informatique en nuage.

Cette capacité de sécurité fonctionnelle:

- définit des ensemble de politiques et d'activités de sécurité comme la gestion de la configuration, la mise à jour des correctifs, l'évaluation de la sécurité, la réaction aux incidents (voir également le § 9.10 "Gestion des incidents") et s'assure que ces mesures de sécurité sont correctement mises en oeuvre en vue de respecter les obligations prévues dans la législation applicable et dans les contrats en vigueur, y compris dans toute convention SLA relative à la sécurité;
- surveille les mesures de sécurité du fournisseur CSP et leur efficacité et transmet aux clients CSC affectés et aux tiers effectuant les audits (agissant en qualité de partenaires CSN) les rapports pertinents, qui peuvent permettre au client CSC de déterminer si le fournisseur CSP respecte les engagements qu'il a pris en matière de sécurité dans le cadre de la convention SLA.

Si les mesures de sécurité appliquées par le fournisseur CSP ou leur efficacité évoluent, tous les fournisseurs et clients de services en nuage en aval en seront informés.

Ces rapports et alertes permettent aux clients CSC autorisés de consulter les incidents, les informations d'audit et les données de configuration se rapportant à leurs services d'informatique en nuage.

### 9.10 Gestion des incidents

La gestion des incidents consiste à surveiller les incidents, à les prévoir, à déclencher une alerte et à intervenir. Afin de savoir si le service d'informatique en nuage fonctionne comme prévu dans l'ensemble de l'infrastructure, une surveillance continue est nécessaire (par exemple, surveillance de la qualité de fonctionnement en temps réel de la plate-forme virtualisée et de la machine virtualisée). Les systèmes peuvent ainsi rendre compte de l'état de la sécurité des services, identifier les anomalies et avertir immédiatement en cas de surcharge du système de sécurité, d'atteinte à la sécurité, de discontinuité du service, etc. Lorsqu'un incident de sécurité se produit, le problème est identifié et l'incident est rapidement réglé, que ce soit de manière automatique ou grâce à l'intervention d'un administrateur humain. Les incidents résolus sont enregistrés et analysés afin de dégager d'éventuels schémas sous-jacents qui peuvent ensuite être traités préventivement.

### 9.11 Rétablissement après une catastrophe

Le rétablissement après une catastrophe est la capacité de faire face à des catastrophes de grande ampleur, de revenir à un état sécurisé et de reprendre un fonctionnement normal aussi rapidement que possible. Cette capacité assure la continuité du service fourni avec une interruption minimum.

### 9.12 Evaluation et audit de la sécurité des services

Cette capacité permet d'évaluer la sécurité des services d'informatique en nuage. Grâce à elle, un tiers habilité vérifie qu'un service d'informatique en nuage respecte les exigences de sécurité applicables. L'évaluation de la sécurité ou l'audit de sécurité pourrait être réalisé par le client CSC, le fournisseur CSP ou un tiers (partenaire CSN), tandis qu'un tiers habilité (partenaire CSN) pourrait effectuer la certification de sécurité.

Des critères de sécurité adaptés sont appliqués pour que le client CSC et le fournisseur CSP aient la même compréhension du niveau de sécurité.

Pour chaque fournisseur CSP et chacun de ses services, on pourra indiquer le niveau de sécurité en ce qui concerne les contrôles de sécurité appliqués par le CSP et leur efficacité. Grâce aux niveaux de sécurité annoncés par le fournisseur CSP et ses services, il sera plus facile de comparer les différents fournisseurs CSP et services d'informatique en nuage et de faire un choix en fonction des besoins. On pourra faire appel à des tiers de confiance indépendants pour fournir des évaluations fiables, indépendantes et impartiales du niveau de sécurité.

Afin d'éviter qu'un fournisseur CSP réalise un audit de sécurité pour chaque client CSC, on réutilisera selon qu'il convient les résultats d'audits de services communs. Pour un fournisseur CSP qui fournit un large éventail de services d'informatique en nuage, les audits de sécurité pourront être réalisés pour chaque service. Le fournisseur CSP pourra fournir les résultats de l'audit correspondant de tout ou partie des services d'informatique en nuage à un client CSC autorisé (par exemple, un client potentiel) et à d'autres fournisseurs CSP et partenaires CSN (par exemple, tiers chargés d'audit).

Dans le cas d'une chaîne de services d'informatique en nuage, les résultats de l'audit de sécurité d'un fournisseur de service en aval seront intégrés aux résultats des audits de sécurité pertinents des fournisseurs de services en amont.

### 9.13 Interopérabilité, portabilité et réversibilité

Grâce à cette capacité, des éléments hétérogènes (interopérabilité) peuvent coexister et coopérer, les clients CSC peuvent changer de fournisseur CSP si nécessaire (portabilité) ou abandonner l'environnement de l'informatique en nuage pour leur système TIC pour revenir à une infrastructure autre que l'informatique en nuage (réversibilité). Cette réversibilité permettra également le "droit à l'oubli" si la législation ou la réglementation locale l'exige.

NOTE 1 – Cette capacité est responsable uniquement de l'interopérabilité et de la portabilité des fonctions de sécurité de l'informatique en nuage, et non des formats utilisés pour les données, les métadonnées et les messages, qui relèvent d'autres fonctions des plates-formes d'informatique en nuage. Par exemple, cette capacité peut fournir le chiffrement pendant la transition, la gestion des clés et les informations d'identité, afin que les données et d'autres contenus puissent être transférés d'un système de chiffrement à un autre sans que le ou les systèmes et données en transit soient pour autant exposés.

NOTE 2 – Le "droit à l'oubli" n'est pas encore clairement défini et peut, dans certains cas, être limité par des prescriptions réglementaires prévoyant la conservation de certaines données pendant une période minimale, comme les relevés d'appels ou les informations de connexion. Par conséquent, il sera peut-être également nécessaire de conserver les clés de sécurité correspondantes ou d'autres informations de sécurité pendant la même période.

### 9.14 Sécurité de la chaîne d'approvisionnement

Les fournisseurs CSP font appel à plusieurs fabricants pour mettre en place leurs services. Certains d'entre eux appartiennent au secteur de l'informatique en nuage (par exemple, partenaires CSN), tandis que d'autres seront des équipementiers ou des fournisseurs de services de technologies de l'information traditionnels (par exemple, fabricants de matériel n'ayant pas de lien direct avec l'informatique en nuage). Cette capacité permet d'établir une relation de confiance entre le fournisseur CSP et tous les participants à la chaîne d'approvisionnement grâce à des activités de sécurité. Ces activités de sécurité consistent, d'une part, à recenser et à rassembler des informations sur les composants et les services achetés par le fournisseur CSP et utilisés pour fournir des services d'informatique en nuage et, d'autre part, à appliquer les politiques de sécurité dans la chaîne d'approvisionnement.

Les activités de sécurité types pour la chaîne d'approvisionnement d'un fournisseur CSP peuvent par exemple être les suivantes:

- confirmation des informations générales sur les participants à la chaîne d'approvisionnement;
- validation du matériel, des logiciels et des services utilisés par le fournisseur CSP;
- inspection du matériel et des logiciels achetés par le fournisseur CSP en vue de s'assurer qu'ils n'ont pas été altérés pendant le transit;
- fourniture de mécanismes permettant de vérifier la provenance des logiciels utilisés pour les services en nuage, par exemple, le code fourni par un partenaire CSN. Le cas échéant, les partenaires CSN et les fournisseurs CSP qui les hébergent mettent un place une procédure pour vérifier l'intégrité du composant logiciel du partenaire CSN afin de s'assurer qu'il est exactement tel que fourni, n'a pas été modifié et que son intégrité n'a pas été mise en danger. Certains partenaires CSN pourront demander des moyens pour vérifier ce point directement par eux-mêmes.

Cette capacité est mise en oeuvre de manière ininterrompue afin de couvrir les évolutions constantes et les mises à jour des systèmes.

## 10 Méthode générale

L'élaboration d'un cadre de sécurité applicable à l'informatique en nuage suppose de bien comprendre les menaces et les problèmes (voir les § 7 et 8) qui sont associés au service en nuage choisi, ainsi que les exigences commerciales, technologiques et réglementaires à prendre en considération pour identifier les contrôles, les politiques et les procédures de sécurité qui seront nécessaires pour un service en nuage donné. Les capacités permettant de faire face et de remédier à ces menaces et problèmes, décrites dans la partie 9, sont ensuite utilisées pour élaborer les contrôles, les politiques et les procédures de sécurité pour le service d'informatique en nuage choisi. La présente Recommandation porte sur les points suivants: quels sont les besoins de sécurité pour l'environnement de l'informatique en nuage; quelles menaces et quels problèmes de l'environnement informatique traditionnel sont également présents dans l'environnement de l'informatique en nuage; et quelles normes et bonnes pratiques définies par le secteur privé conviendrait-il d'appliquer en plus de la présente Recommandation?

Il faudrait appliquer la méthode décrite ci-après pour créer le cadre qui permettra d'identifier les contrôles, les politiques et les procédures de sécurité qui seront nécessaires pour un service d'informatique en nuage donné. Il n'est pas possible de proposer un cadre normatif unique applicable à tous les services d'informatique en nuage, étant donné que les modèles commerciaux, les services proposés et les choix de mise en oeuvre sont très différents d'un service à l'autre:

- Etape 1: Utiliser les §§ 7 et 8 pour identifier les menaces de sécurité et les répercussions sur le plan de la sécurité des problèmes associés au service d'informatique en nuage considéré.

- Etape 2: Utiliser le § 9 pour identifier, sur la base des menaces et des problèmes identifiés, les capacités de sécurité de haut niveau requises, qui pourraient permettre d'atténuer les menaces de sécurité et de résoudre les problèmes de sécurité.
- Etape 3: Déduire les contrôles, les politiques et les procédures de sécurité qui pourraient fournir les moyens de sécurité nécessaires sur la base des capacités de sécurité identifiées.

NOTE – Le client CSC et le fournisseur CSP devront définir, en utilisant les normes qui conviennent, un ensemble d'exigences appropriées en ce qui concerne les capacités de sécurité. Pour ce faire, ils devront se fonder sur l'évaluation des risques.

Il conviendrait d'examiner chaque menace ou problème pour identifier les menaces et problèmes de sécurité qui concernent le service en nuage considéré. L'une des solutions pourrait tout simplement consister à élaborer un tableau avec un "O" en regard de la menace ou du problème.

Pour illustrer cette solution, prenons par exemple le cas d'un fournisseur CSP qui assure le stockage des fichiers pour des particuliers et souhaiterait, d'une part, comprendre les principales menaces et les principaux problèmes de sécurité auxquels les utilisateurs sont exposés et, d'autre part, analyser principales menaces et les principaux problèmes de sécurité qu'il doit résoudre. Le Tableau 1 illustre cette approche.

**Tableau 1 – Exemple pour la première étape de l'analyse du cadre de sécurité dans le cas où le stockage des fichiers est fourni en tant que service**

| Domaine d'analyse | Menace ou problème particulier | Concerne ce service? |
|---|---|---|
| **§ 7.1 Menaces de sécurité visant les clients de services en nuage (CSC)** | § 7.1.1 Perte et fuite de données | O |
| | § 7.1.2 Accès non sécurisé aux services | O |
| | § 7.1.3 Menaces internes | |
| **§ 7.2 Menaces de sécurité visant les fournisseurs de services en nuage (CSP)** | § 7.2.1 Accès non autorisé aux fonctions d'administration | O |
| | § 7.2.2 Menaces internes | O |
| **§ 8.1 Problèmes de sécurité pour les clients de services en nuage (CSC)** | § 8.1.1 Répartition ambiguë des responsabilités | O |
| | § 8.1.2 Perte de confiance | O |
| | § 8.1.3 Perte de gouvernance | O |
| | § 8.1.4 Perte de confidentialité | O |
| | § 8.1.5 Indisponibilité des services | O |
| | § 8.1.6 Enfermement vis-à-vis du fournisseur de services en nuage | O |
| | § 8.1.7 Détournement de la propriété intellectuelle | |
| | § 8.1.8 Perte d'intégrité d'un logiciel | |
| **§ 8.2 Problèmes de sécurité pour les fournisseurs de services en nuage (CSP)** | § 8.2.1 Répartition ambiguë des responsabilités | O |
| | § 8.2.2 Environnement partagé | O |
| | § 8.2.3 Incohérence ou conflit entre les mécanismes de protection | O |
| | § 8.2.4 Conflit juridictionnel | O |

**Tableau 1 – Exemple pour la première étape de l'analyse du cadre de sécurité dans le cas où le stockage des fichiers est fourni en tant que service**

| Domaine d'analyse | Menace ou problème particulier | Concerne ce service? |
|---|---|---|
| | § 8.2.5 Risques liés à l'évolution | |
| | § 8.2.6 Migration et intégration médiocres | O |
| | § 8.2.7 Discontinuité de l'activité | O |
| | § 8.2.8 Enfermement vis-à-vis d'un partenaire de services en nuage | |
| | § 8.2.9 Vulnérabilité de la chaîne d'approvisionnement | O |
| | § 8.2.10 Dépendance entre les logiciels | |
| **§ 8.3 Problèmes de sécurité pour les partenaires de services en nuage (CSN)** | § 8.3.1 Répartition ambiguë des responsabilités | |
| | § 8.3.2 Détournement de la propriété intellectuelle | |
| | § 8.3.3 Perte d'intégrité d'un logiciel | |

Une fois que les menaces et les problèmes de sécurité ont été recensés, il est possible d'identifier les capacités de sécurité qui pourraient permettre d'atténuer ces menaces et de résoudre ces problèmes. On trouvera dans le Tableau I.1 un exemple de mise en correspondance des menaces et problèmes de sécurité liés à l'informatique en nuage et des capacités de sécurité. La lettre "O" dans la case à l'intersection d'une colonne et d'une ligne du tableau indique que la menace ou le problème de sécurité concerné peut être résolu grâce à la capacité de sécurité correspondante. Ce tableau montre, pour toutes les menaces et tous les problèmes de sécurité, la capacité de sécurité correspondante.

Une fois que les capacités requises ont été identifiées, les contrôles, les politiques et les procédures de sécurité peuvent être définis en fonction des besoins. On trouvera dans les § 12 ("Operations security") et 16 ("Information security incident management") de la norme [b-ISO/CEI 27002] des exemples de contrôles pouvant être utilisés, qui sont élaborés sur la base des capacités recensées dans les § 9.9 et 9.10 respectivement.

La chaîne d'approvisionnement d'un service en nuage peut comprendre plusieurs fournisseurs CSP. Les entreprises qui composent cette chaîne peuvent consulter les normes de l'UIT ou du secteur privé relatives à la sécurité de la chaîne d'approvisionnement (par exemple, la norme [b-ISO/CEI 28000]. Chaque fournisseur CSP devra délimiter clairement ses responsabilités dans la chaîne du service d'informatique en nuage et définir ses contrôles, politiques et procédures de sécurité sur la base des capacités de sécurité déduites de cette méthode en trois étapes. Pour assurer de manière cohérente la sécurité des clients CSC, le fournisseur CSP situé en amont devra peut-être négocier avec ses fournisseurs CSP en aval ces capacités de sécurité sur la base de ses responsabilités en matière de sécurité. Au besoin, les clients CSC devraient eux aussi suivre cette procédure en trois étapes.

En outre, la procédure en trois étapes décrite ci-dessus devrait être mise en oeuvre régulièrement ou selon les besoins (par exemple, en cas de grave atteinte à la sécurité ou lorsqu'un fournisseur CSP change de fournisseur CSP en amont).

# Appendice I

## Mise en correspondance des menaces et problèmes de sécurité de l'informatique en nuage et des capacités de sécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Le Tableau I.1 met en correspondance les menaces et problèmes de sécurité liés à l'informatique en nuage et de possibles capacités de sécurité.

La lettre "O" dans la case à l'intersection d'une colonne et d'une ligne du tableau indique que la menace ou le problème de sécurité concerné peut être résolu grâce à la capacité de sécurité correspondante.

**Tableau I.1 – Correspondance entre les menaces et problèmes de sécurité de l'informatique en nuage et les capacités de sécurité**

| | | | **§ 9 Capacités de sécurité de l'informatique en nuage** | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **§ 9.1 Modèle de confiance** | **§ 9.2 Gestion de l'identité et de l'accès (IAM), authentifi-cation, autorisation et audit des transactions** | **§ 9.3 Sécurité physique** | **§ 9.4 Sécurité des interfaces** | **§ 9.5 Sécurité de la virtualisation informatique** | **§ 9.6 Sécurité du réseau** | **§ 9.7 Isolation et protection des données et protection de la confidentia-lité** | **§ 9.8 Coordination de la sécurité** | **§ 9.9 Sécurité opération-nelle** | **§ 9.10 Gestion des incidents** | **§ 9.11 Rétablis-sement après une catastro-phe** | **§ 9.12 Evaluation et audit de la sécurité des services** | **§ 9.13 Interopérabilité, portabilité et réversibilité** | **§ 9.14 Sécurité de la chaîne d'approvi-sionnement** |
| § 7 Mena-ces de sécurité visant l'infor-matique en nuage | § 7.1 Menaces de sécurité visant les clients de services en nuage (CSC) | § 7.1.1 Perte et fuite de données | O | O | O | | | | O | | | | O | | | |
| | | § 7.1.2 Accès non sécurisé aux services | O | O | | O | O | O | | | | | | | | |
| | | § 7.1.3 Menaces internes | | O | O | | | | | | | | | O | | |

## Tableau I.1 – Correspondance entre les menaces et problèmes de sécurité de l'informatique en nuage et les capacités de sécurité

| | | | § 9 Capacités de sécurité de l'informatique en nuage | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **§ 9.1 Modèle de confiance** | **§ 9.2 Gestion de l'identité et de l'accès (IAM), authentifi-cation, autorisation et audit des transactions** | **§ 9.3 Sécurité physique** | **§ 9.4 Sécurité des interfaces** | **§ 9.5 Sécurité de la virtualisation informatique** | **§ 9.6 Sécurité du réseau** | **§ 9.7 Isolation et protection des données et protection de la confidentia-lité** | **§ 9.8 Coordina-tion de la sécurité** | **§ 9.9 Sécurité opération-nelle** | **§ 9.10 Gestion des incidents** | **§ 9.11 Rétablis-sement après une catastro-phe** | **§ 9.12 Evaluation et audit de la sécurité des services** | **§ 9.13 Interopérabilité, portabilité et réversibilité** | **§ 9.14 Sécurité de la chaîne d'approvi-sionnement** |
| | § 7.2 Menaces de sécurité visant les fournis-seurs de services en nuage (CSP) | § 7.2.1 Accès non autorisé aux fonctions d'admi-nistration | O | O | O | O | | | | | | | | | | |
| | | § 7.2.2 Menaces internes | | O | O | | | | | | | | | O | | |
| § 8 Problè-mes de sécurité posés par l'infor-matique en nuage | § 8.1 Problè-mes de sécurité pour les clients de services en nuage (CSC) | § 8.1.1 Réparti-tion ambiguë des responsa-bilités | | O | | | | | | | O | | | | | |
| | | § 8.1.2 Perte de confiance | O | | | | | | | | | | | O | | |
| | | § 8.1.3 Perte de gouver-nance | | O | O | | | | O | | O | O | O | O | | |
| | | § 8.1.4 Perte de confiden-tialité | | O | | | | | O | | | | | O | | |

## Tableau I.1 – Correspondance entre les menaces et problèmes de sécurité de l'informatique en nuage et les capacités de sécurité

| | | | § 9 Capacités de sécurité de l'informatique en nuage | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **§ 9.1 Modèle de confiance** | **§ 9.2 Gestion de l'identité et de l'accès (IAM), authentification, autorisation et audit des transactions** | **§ 9.3 Sécurité physique** | **§ 9.4 Sécurité des interfaces** | **§ 9.5 Sécurité de la virtualisation informatique** | **§ 9.6 Sécurité du réseau** | **§ 9.7 Isolation et protection des données et protection de la confidentialité** | **§ 9.8 Coordination de la sécurité** | **§ 9.9 Sécurité opérationnelle** | **§ 9.10 Gestion des incidents** | **§ 9.11 Rétablissement après une catastrophe** | **§ 9.12 Evaluation et audit de la sécurité des services** | **§ 9.13 Interopérabilité, portabilité et réversibilité** | **§ 9.14 Sécurité de la chaîne d'approvisionnement** |
| § 8 Problèmes de sécurité posés par l'informatique en nuage | § 8.1 Problèmes de sécurité pour les clients de services en nuage (CSC) | § 8.1.5 Indisponibilité des services | | | | | | | | O | O | O | O | | | O |
| | | § 8.1.6 Enfermement vis-à-vis du fournisseur de services en nuage | | | | | | | | | | | | | O | |
| | | § 8.1.7 Détournement de la propriété intellectuelle | | O | O | | | | O | | O | | | | | |
| | | § 8.1.8 Perte d'intégrité d'un logiciel | | O | | | O | | O | | | | | | | |

## Tableau I.1 – Correspondance entre les menaces et problèmes de sécurité de l'informatique en nuage et les capacités de sécurité

| | | | § 9 Capacités de sécurité de l'informatique en nuage | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **§ 9.1 Modèle de confiance** | **§ 9.2 Gestion de l'identité et de l'accès (IAM), authentifi-cation, autorisation et audit des transactions** | **§ 9.3 Sécurité physique** | **§ 9.4 Sécurité des interfaces** | **§ 9.5 Sécurité de la virtualisation informatique** | **§ 9.6 Sécurité du réseau** | **§ 9.7 Isolation et protection des données et protection de la confidentia-lité** | **§ 9.8 Coordina-tion de la sécurité** | **§ 9.9 Sécurité opération-nelle** | **§ 9.10 Gestion des incidents** | **§ 9.11 Rétablis-sement après une catastro-phe** | **§ 9.12 Evaluation et audit de la sécurité des services** | **§ 9.13 Interopérabilité, portabilité et réversibilité** | **§ 9.14 Sécurité de la chaîne d'approvi-sionnement** |
| § 8 Problè-mes de sécurité posés par l'infor-matique en nuage | § 8.2 Problè-mes de sécurité pour les fournis-seurs de services en nuage (CSP) | § 8.2.1 Répartition ambiguë des respon-sabilités | | O | | | | | | | O | | | | | |
| | | § 8.2.2 Environ-nement partagé | | | | | O | O | O | | | | | | | |
| | | § 8.2.3 Incohé-rence ou conflit entre les mécanis-mes de protection | | | | | | | | O | | | | | O | |
| | | § 8.2.4 Conflit juridic-tionnel | | | | | | | O | | O | | | | | |
| | | § 8.2.5 Risques liés à l'évolu-tion | | | | | | | | | O | | | | O | O |
| | | § 8.2.6 Migration et intégra-tion médiocres | | | | O | O | O | O | O | O | | | | | |

## Tableau I.1 – Correspondance entre les menaces et problèmes de sécurité de l'informatique en nuage et les capacités de sécurité

| | | | § 9 Capacités de sécurité de l'informatique en nuage | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **§ 9.1 Modèle de confiance** | **§ 9.2 Gestion de l'identité et de l'accès (IAM), authentifi-cation, autorisation et audit des transactions** | **§ 9.3 Sécurité physique** | **§ 9.4 Sécurité des interfaces** | **§ 9.5 Sécurité de la virtualisation informatique** | **§ 9.6 Sécurité du réseau** | **§ 9.7 Isolation et protection des données et protection de la confidentia-lité** | **§ 9.8 Coordina-tion de la sécurité** | **§ 9.9 Sécurité opération-nelle** | **§ 9.10 Gestion des incidents** | **§ 9.11 Rétablis-sement après une catastro-phe** | **§ 9.12 Evaluation et audit de la sécurité des services** | **§ 9.13 Interopérabilité, portabilité et réversibilité** | **§ 9.14 Sécurité de la chaîne d'approvi-sionnement** |
| § 8 Problè-mes de sécurité posés par l'infor-matique en nuage | § 8.2 Problè-mes de sécurité pour les fournis-seurs de services en nuage (CSP) | § 8.2.7 Disconti-nuité de l'activité | | | | | | | | | | O | O | | | |
| | | § 8.2.8 Enfer-mement vis-à-vis d'un partenaire de services en nuage | | | | | | | | | | | | | | O |
| | | § 8.2.9 Vulnéra-bilité de la chaîne d'appro-vision-nement | | | | | | | | | | | | | | O |
| | | § 8.2.10 Dépen-dance entre les logiciels | | | | | | | | | | | | | | O |

## Tableau I.1 – Correspondance entre les menaces et problèmes de sécurité de l'informatique en nuage et les capacités de sécurité

| | | | § 9 Capacités de sécurité de l'informatique en nuage | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **§ 9.1 Modèle de confiance** | **§ 9.2 Gestion de l'identité et de l'accès (IAM), authentifi-cation, autorisation et audit des transactions** | **§ 9.3 Sécurité physique** | **§ 9.4 Sécurité des interfaces** | **§ 9.5 Sécurité de la virtualisation informatique** | **§ 9.6 Sécurité du réseau** | **§ 9.7 Isolation et protection des données et protection de la confidentia-lité** | **§ 9.8 Coordina-tion de la sécurité** | **§ 9.9 Sécurité opération-nelle** | **§ 9.10 Gestion des incidents** | **§ 9.11 Rétablis-sement après une catastro-phe** | **§ 9.12 Evaluation et audit de la sécurité des services** | **§ 9.13 Interopérabilité, portabilité et réversibilité** | **§ 9.14 Sécurité de la chaîne d'approvi-sionnement** |
| | § 8.3 Problè-mes de sécurité pour les partenai-res de services en nuage (CSN) | § 8.3.1 Réparti-tion ambiguë des responsa-bilités | | O | | | | | | | O | | | | | |
| | | § 8.3.2 Détour-nement de la propriété intellec-tuelle | | O | O | | | | O | | O | | | | | |
| | | § 8.3.3 Perte d'intégrité d'un logiciel | | O | | | O | | O | | | | | | | |

# Bibliographie


[b-UIT-T E.409] Recommandation UIT-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*.

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*.

[b-UIT -T Y.3500] Recommandation UIT -T Y.3500 (2014) | ISO/CEI 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire*.

[b-UIT -T Y.3502] Recommandation UIT-T Y.3502 (2014) | ISO/ CEI 17789:2014, *Technologies de l'information – Informatique en nuage – Architecture de référence*.

[b-ISO/CEI 19440] ISO/CEI 19440:2007, *Entreprise intégrée – Constructions pour la modélisation d'entreprise*.

[b-ISO/CEI 20000-1] ISO/CEI 20000-1:2011, *Technologies de l'information – Gestion des services – Partie 1: Exigences du système de management des services*.

[b-ISO/CEI 27000] ISO/CEI 27000:2012, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/CEI 27002] ISO/CEI 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*.

[b-ISO/CEI 27005] ISO/CEI 27005:2011, *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.

[b- ISO/ CEI 27729] ISO/ CEI 27729:2012, *Information et documentation – Code international normalisé des noms (ISNI)*.

[b-ISO/CEI 28000] ISO/CEI 28000:2007, *Spécifications relatives aux systèmes de management de la sûreté de la chaîne d'approvisionnement*.

[b-ISO/CEI 29100] ISO/CEI 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre privé*.

[b-NIST-SP-800-30] Publication spéciale du NIST 800-30 (2012), *Guide pour l'évaluation des risques*.

[b-NIST-SP-800-53] Publication spéciale du NIST 800-53 Rev.3 (2009), *Contrôles de sécurité recommandés pour les systèmes et organismes d'informations fédéraux*.

[b-NIST-SP-800-125] Publication spéciale du NIST 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] Publication spéciale du NIST 800-145 (2011), *The NIST Definition of Cloud Computing*.

[b-CSA Matrix] CSA (2013), *Cloud Controls Matrix, Cloud Security Alliance*.

[b-key definition] Key definitions of the Data Protection Act, Information Commissioner's Office <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>

## SÉRIES DES RECOMMANDATIONS UIT-T

| | |
|---|---|
| Série A | Organisation du travail de l'UIT-T |
| Série D | Principes généraux de tarification |
| Série E | Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains |
| Série F | Services de télécommunication non téléphoniques |
| Série G | Systèmes et supports de transmission, systèmes et réseaux numériques |
| Série H | Systèmes audiovisuels et multimédias |
| Série I | Réseau numérique à intégration de services |
| Série J | Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias |
| Série K | Protection contre les perturbations |
| Série L | Construction, installation et protection des câbles et autres éléments des installations extérieures |
| Série M | Gestion des télécommunications y compris le RGT et maintenance des réseaux |
| Série N | Maintenance: circuits internationaux de transmission radiophonique et télévisuelle |
| Série O | Spécifications des appareils de mesure |
| Série P | Terminaux et méthodes d'évaluation subjectives et objectives |
| Série Q | Commutation et signalisation |
| Série R | Transmission télégraphique |
| Série S | Equipements terminaux de télégraphie |
| Série T | Terminaux des services télématiques |
| Série U | Commutation télégraphique |
| Série V | Communications de données sur le réseau téléphonique |
| **Série X** | **Réseaux de données, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération |
| Série Z | Langages et aspects généraux logiciels des systèmes de télécommunication |

Imprimé en Suisse
Genève, 2016