Développement de scénarios d'analyse de risques en matière de protection des renseignements personnels (PRP) intégrés à la méthodologie Méhari

Bernard Dionne, CISSP-ISSMP
Chef de projet

25 août 2006

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

Québec

Ministère
du Conseil exécutif
Québec

Mise en garde

Le contenu du présent document a fait l'objet d'une mise à jour (préliminaire), compte tenu de l'adoption le 13 juin 2006 du projet de loi n^{o} 86 modifiant la loi sur l'accès. Les références au texte de loi seront révisées de nouveau, lorsque la version officielle de la loi sur l'accès sera rendue publique.

N'hésitez pas, par ailleurs, à communiquer toute information nous permettant de corriger et d'améliorer le présent document. Pour ce faire, vous pouvez rejoindre M. Bernard Dionne, du Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information (SRIDAI) à l'adresse suivante : bernard.dionne@mce.gouv.qc.ca

Version électronique

Le présent document peut être téléchargé dans sa version électronique dans la section « Accès à l'information » du site Internet du SRIDAI (http://www.institutions-democratiques.gouv.qc.ca).

La base de connaissance Méhari comportant l'ajout des éléments PRP est disponible sur le site du SRIDAI. On peut aussi se la procurer lors de l'acquisition du logiciel Risicare, à la suite d'une entente prise avec le ministère des Services gouvernementaux (MSG).

Groupe de travail ministériel

Le présent document a été rédigé par un groupe de travail formé de membres du personnel de différents ministères et organismes gouvernementaux québécois suivants.

GROUPE DE TRAVAIL MINISTÉRIEL	
Ministère et organisme gouvernemental	**Membre**
Ministère de l'Éducation	Sylvie Blouin
Ministère des Relations avec les citoyens et de l'Immigration / Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information (SRIDAI)	Denyse Roussel Bernard Dionne
Ministère du Développement économique et régional et de la Recherche	André Huard
Régie des rentes du Québec	Danielle Corriveau
Revenu Québec	Luc Tremblay
Secrétariat du Conseil du trésor	Pierre Sasseville

Les travaux de ce groupe de travail ont été effectués entre septembre et décembre 2004, à un rythme d'une rencontre aux deux semaines.

De façon à valider l'outil d'analyse de risques PRP adapté à Méhari, deux ministères ont accepté de participer à un projet pilote au cours de l'année 2005 : le ministère du Revenu du Québec et le ministère de l'Éducation, du Loisir et du Sport.

À la suite de l'adoption du projet de loi n^{o} 86 modifiant la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et d'autres dispositions législatives, des travaux ont été effectués en mars et avril 2006 par le personnel du SRIDAI pour mettre à jour le document.

Nous tenons à remercier les membres du groupe de travail ministériel, les membres des équipes chargés d'effectuer les tests dans les deux ministères mentionnés ci-dessus, le personnel du SRIDAI et toutes les personnes qui, de près ou de loin, ont contribué à la production de ce document.

Table des matières

1. Contexte

Les ministères et les organismes du gouvernement du Québec mettent en place des systèmes d'information et d'informatique afin d'améliorer non seulement la gestion de leurs programmes, mais aussi la qualité de la prestation ou de la livraison des services qu'ils offrent aux citoyens. À cette fin, de nombreux systèmes et services peuvent être reliés, par exemple, dans un mode de prestation électronique.

La collecte, l'utilisation, la communication, la conservation, la destruction de renseignements personnels au sein des ministères et des organismes publics peuvent avoir des répercussions négatives sur la protection des renseignements, ce qui comporte de grands risques.

Rappelons que les ministères et les organismes publics sont assujettis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et que cette loi a un caractère prépondérant.

En conséquence, la probabilité que les risques d'atteinte à la protection des renseignements personnels se réalisent doit être considérée sérieusement, puisqu'ils se présentent dans presque toutes les situations de la vie quotidienne. De fait, tous les secteurs d'activité privés ou publics sont exposés à de tels risques.

Les ministères et les organismes publics doivent donc insister pour que de nouvelles pratiques en matière de gestion du risque soient intégrées à leurs activités, afin de lever toute incertitude de manière stratégique, de tirer profit des occasions offertes, de fournir de l'information et de favoriser la participation des différents acteurs. Ainsi, la prise de décisions éclairées s'en trouvera améliorée, ce qui ne peut que garantir et renforcer la protection des renseignements personnels.

Il est donc primordial que les ministères et les organismes publics puissent compter sur une méthode d'analyse des risques pour éviter l'improvisation et pour canaliser les mesures préventives à mettre en œuvre dans ce domaine.

Or, nous avons constaté qu'il n'existait encore aucun outil d'analyse des risques liés à la protection des renseignements personnels adapté au contexte de la législation québécoise. Toutefois, en matière de sécurité des systèmes d'information, les ministères et organismes peuvent déjà compter sur plusieurs méthodes d'analyse de risques, dont une recommandée par le Ministère des services gouvernementaux : la méthode Méhari.

Afin de répondre au grand besoin des ministères et organismes publics de disposer d'une méthode d'analyse des risques pour évaluer les répercussions possibles d'une nouvelle technologie ou d'un nouveau système d'information sur la protection des renseignements personnels et d'élaborer un plan d'action, le choix a été fait d'intégrer les éléments PRP les plus pertinents en la matière à la méthode Méhari.

L’objet du présent document est d’offrir une méthode commune d’analyse des risques en matière de protection des renseignements personnels élaborée par les membres du groupe de travail.

C’est le ministre responsable des affaires intergouvernementales canadiennes, de la francophonie canadienne, de l’accord sur le commerce intérieur, de la réforme des institutions démocratiques et de l’accès à l’information qui a le mandat de conseiller le gouvernement en matière d’accès aux documents et de protection des renseignements personnels. Le Secrétariat à la réforme des institutions démocratiques et de l’accès à l’information (SRIDAI) est chargé tant quand à lui de soutenir les actions du ministre dans ce domaine.

2. Portée du document

Le présent document est destiné à tous les ministères et organismes publics assujettis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et, d'une façon subsidiaire, aux entreprises québécoises soumis à la *Loi sur la protection des renseignements personnels dans le secteur privé*. Il vise donc toutes les personnes qui, au sein de ces organisations, se préoccupent de la gestion des risques en la matière.

Les éléments qu'il comporte se limitent aux services et aux scénarios à incorporer ou à prendre en considération dans la méthode Méhari et le logiciel RISICARE qui en fait partie. Précisons d'emblée qu'il est préférable de connaître la méthode Méhari pour avoir une bonne compréhension de ce qui suit.

Bien que les scénarios de risques proposés dans ce document recouvrent le cycle de vie d'un renseignement personnel ainsi que les obligations légales s'y rapportant, d'autres risques liés à la protection de ce type de renseignement peuvent ne pas avoir été pris en considération. Il n'en demeure pas moins qu'ils pourraient, au besoin, être incorporés dans les versions à venir.

3. Définitions usuelles

Cadre de gestion
Ensemble des moyens mis en œuvre pour soutenir la prise de décision en vue de l'atteinte des objectifs visés.

Directive
Prescription qui émane d'une autorité administrative et qui détermine la ligne de conduite à adopter, l'orientation à suivre ou la façon de procéder.

Incident
Tout événement qui va à l'encontre d'une politique ou d'une directive.

Norme
Spécification technique d'un produit, d'un procédé.

Plan
Ensemble structuré d'objectifs que se fixe une organisation, ainsi que des moyens qu'elle se donne pour les atteindre.

Politique
Ensemble de principes généraux adoptés par une organisation pour l'exercice de ses activités.

Procédé
Méthode employée pour produire un effet déterminé ou parvenir à un certain résultat.

Procédure
Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.

Programme
Suite ordonnée d'actions qu'une organisation se propose d'accomplir, en vue d'atteindre les objectifs qu'elle s'est fixés dans un plan.

Source – *Grand dictionnaire terminologique de l'Office québécois de la langue française.*

Note **–** L'expression « informations visées par les dispositions légales en matière de PRP », utilisée dans ce document, inclut aussi de l'information confidentielle autre que de nature personnelle.

4. Organisation du document

Le présent document est divisé en sections et sous-sections.

Section Concepts à la base de la méthodologie Méhari

Bien que ce document s'adresse à des personnes qui ont déjà une bonne connaissance de la méthode Méhari, la présente section fournit l'occasion à celles qui sont moins averties de faire un rapide survol des différents concepts préconisés. Pour en savoir plus, il est recommandé de consulter le *Guide d'utilisation de la méthode Méhari et de l'outil Risicare*, publié par le ministère des Services gouvernementaux (MSG), le *Manuel d'utilisation du logiciel Risicare* de même que les documents concernant la méthode Méhari sur le site Web du Club de la sécurité informatique français (CLUSIF).

Sous-section Définition des types de mesures Méhari

Les différentes mesures prises en considération dans la méthode Méhari sont définies dans cette sous-section.

Sous-section Pondération des questions et des scénarios de risques Méhari

Cette sous-section traite de la façon dont les éléments de pondération de la méthodologie Méhari ont été appliqués aux sous-services de sécurité et aux scénarios de risques.

Sous-section Scénarios de risques Méhari

Cette sous-section présente non seulement les nouveaux scénarios de risques développés pour étendre le champ d'application de la méthode Méhari à la protection des renseignements personnels, mais aussi ceux qui en font déjà partie.

Section Audit des nouveaux services

La définition des nouveaux services de protection des renseignements personnels est fournie dans cette section, de même qu'une liste de questions pour en vérifier l'existence.

Section Audit des services existants

Tous les services qui existent déjà dans les bases de connaissances proposées par le MSG et qui peuvent s'appliquer dans le contexte des scénarios de protection des renseignements personnels sont énumérés dans cette section. Une liste de questions y est également fournie pour en vérifier l'existence.

Vous noterez que nous avons fait ici un copier/coller, sans modification ou correction. Comme cette partie est tirée des travaux du CLUSIF, nous avons soumis à cet organisme une révision linguistique afin de corriger et d'améliorer le texte.

Section Scénarios de risques

Cette section comprend les scénarios de risques en matière de protection des renseignements personnels, les mesures à appliquer pour éviter que des risques surviennent et pour en atténuer, le cas échant, les répercussions négatives, ainsi que la formule de calcul du niveau de gravité de chaque scénario.

Annexe A – Tableau des liens existant entre les mesures de protection des renseignements personnels, le modèle de bonnes pratiques en la matière et les articles de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*

Dans le tableau qui constitue cette annexe, sont établis les liens qui existent entre les mesures de protection proposées dans le présent document, les éléments de pratiques énumérés dans l'ouvrage intitulé *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics* qu'a publié le ministère des Relations avec les citoyens et de l'Immigration ainsi que la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la loi sur le cadre juridique des technologies de l'information. Vous trouverez ces deux documents à la section « Accès à l'information » du site Internet du SRIDAI (http://www.institutions-democratiques.gouv.qc.ca).

Notez que le document concernant le Modèle de pratiques a été conçu afin d'aider les ministères et les organismes publics à mettre en application, dans leurs projets de développement, des principes et des obligations légales en matière de protection de renseignements personnels. Toutefois, il a été élaboré avant le projet de loi n^{o} 86 et n'a pas été mis à jour depuis lors.

5. Concepts à la base de la méthodologie Méhari

L'approche analytique de la méthode Méhari repose essentiellement sur l'utilisation d'un questionnaire d'analyse en vue d'évaluer l'existence et l'efficacité des mesures de sécurité, ou « services de sécurité » selon la terminologie de Méhari. Elle permet de réduire la probabilité qu'un scénario de risques se réalise ou ait des répercussions négatives. En d'autres termes, il s'agit d'une méthode d'évaluation systématique des mesures de sécurité en place.

Un scénario est un événement, ayant une origine et une cause, qui entraîne des répercussions négatives sur la protection des renseignements personnels. À titre d'exemple, citons la divulgation, par un membre du personnel d'un ministère ou d'un organisme public, de renseignements personnels à des personnes non autorisées.

La gravité des risques inhérents à chaque scénario est calculée à l'aide du logiciel Risicare, qui comporte une échelle de 0 à 4. Cet outil établit une distinction entre les trois catégories de risques qui suivent :

– les risques tolérables (niveau 0, 1 ou 2);
– les risques inadmissibles (niveau 3);
– les risques insupportables (niveau 4).

L'évaluation quantitative de la gravité des risques pour un scénario donné est faite en fonction de deux paramètres : l'impact (terme propre à la méthode Méhari) et la potentialité.

<u>L'impact</u>

L'impact est une évaluation globale de l'ensemble des conséquences d'un scénario de risques précis.

La métrique standard de l'impact est une cotation sur l'échelle à niveaux (de 1 à 4) décrite ci-dessous.

Niveau 1 – Impact insignifiant sur le ministère ou l'organisme public
Niveau 2 – Impact significatif, c'est-à-dire qu'il cause du tort au ministère ou à l'organisme public
Niveau 3 – Impact très grave, mais qui ne menace ni la mission ni les activités du ministère ou de l'organisme public
Niveau 4 – Impact extrêmement grave, c'est-à-dire qu'il menace le ministère ou l'organisme public ou l'une de ses activités

<u>La potentialité</u>

La potentialité est une estimation de la possibilité qu'un scénario de risques précis se réalise.

La métrique de la potentialité est une cotation sur une échelle à 4 niveaux (de 1 à 4), plus un niveau de potentialité 0 pour indiquer que le scénario de risques ne s'applique pas au ministère ou à l'organisme public ou qu'il est sans objet. La signification des différents niveaux est donnée ci-après.

Niveau 0 – Non envisageable ou non envisagé
Niveau 1 – Très improbable, c'est-à-dire qu'il ne se présentera probablement jamais
Niveau 2 – Possible, mais plutôt improbable
Niveau 3 – Probable, c'est-à-dire qu'il devrait se présenter un jour
Niveau 4 – Très probable, c'est-à-dire qu'il se présentera sûrement à court terme

Les six types de mesures de sécurité que comprend la méthode Méhari sont définis dans ce document avec des exemples à l'appui. Il s'agit des mesures d'exposition ou structurelles, des mesures de dissuasion ou dissuasives, des mesures de prévention, des mesures de protection, des mesures de récupération et des mesures palliatives.

Le questionnaire sert à évaluer l'existence et l'efficacité de chaque mesure de sécurité selon une certaine gradation de son niveau de maturité (en place, diffusée, mise à jour, vérifiée, etc.

Ainsi, pour un même scénario, il existe généralement plusieurs mesures de sécurité de différents types en vue de réduire sa probabilité de réalisation ou son impact. Pour ce qui est d'une même mesure de sécurité, des questions peuvent être posées afin d'évaluer sa qualité et son niveau d'efficacité. Les mesures de sécurité font l'objet d'une pondération, car elles n'ont pas toutes la même importance et le même impact sur la réduction des risques.

L'existence ou l'absence de mesures de sécurité, ainsi que l'évaluation de leur « qualité », c'est-à-dire de leur efficacité et de leur pertinence pour un scénario donné, se traduit en indicateurs, appelés status. Au nombre de six, ces indicateurs servent à évaluer l'impact des mesures de sécurité sur l'un des facteurs de risques du scénario. Les status sont donc calculés selon le type de mesure de sécurité : EXPO (mesure d'exposition ou structurelle); DISS (mesure de dissuasion ou dissuasive); PREV (mesure de prévention); PROT (mesure de protection); PALL (mesure palliative); RECUP (mesure de récupération). Ils sont ensuite consolidés en status RI (réduction d'impact) et status P (potentialité).

La conduite d'un projet d'implantation d'un système d'information est basée sur la connaissance de son cycle de vie. Les phases de la vie d'un tel système sont les suivantes : l'analyse des besoins, la conception préliminaire, la conception détaillée, le développement, la mise en œuvre, la vie utile, le suivi, la maintenance, la fin de la vie utile et la mise au rebut.

Des évaluations de risques peuvent être effectuées à chaque phase du cycle de vie d'un système d'information, de façon à ce que la collecte, l'utilisation, la communication, la conservation et la destruction de renseignements personnels se fassent dans le respect des dispositions légales et des bonnes pratiques établies en matière de sécurité.

La réalisation d'une étude Méhari implique la participation de trois types d'acteurs au sein de tout ministère et organisme public.

- Les membres de la direction, parce qu'ils assument les responsabilités liées au domaine stratégique, à la conception de la politique générale, à la définition des objectifs prioritaires, c'est-à-dire ceux qui correspondent à l'appréciation des risques les plus redoutables, et à la proposition de solutions à retenir ou à éviter absolument.

- Les experts et les techniciens en informatique, en sécurité des systèmes d'information, en protection des renseignements personnels et en vérification interne, parce qu'ils possèdent une vaste connaissance des systèmes existants, de leurs caractéristiques et de la nature des informations détenues. Ils sont donc en mesure de prévoir les risques, d'évaluer leur portée, de suggérer des solutions et de les appliquer pour les éliminer ou, à défaut, pour les réduire.

Les utilisateurs de tous les niveaux de la hiérarchie, parce qu'ils sont les seuls à même d'évaluer les conséquences des sinistres sur leurs propres activités et de signaler les contraintes des mesures de protection proposées. Il importe donc de leur offrir la possibilité de valider les mesures de sécurité à mettre en œuvre, à défaut de les faire participer à la prise de décisions.

La conduite de l'implantation d'un système d'information est confiée à un chef de projet. Selon l'importance de ce dernier, le chef doit pouvoir compter sur une équipe de personnes qui connaissent bien le domaine étudié et les applications du système d'information; cette équipe constitue le noyau dur du projet. L'ensemble forme le groupe d'analyse, ou comité de projet, qui, au besoin, peut faire appel à des experts. Comme dans la réalisation de tout bon projet, ce groupe relève d'un comité de direction.

À titre indicatif, les deux groupes, ou l'un d'eux, pourraient être composés, en plus du chef de projet, du responsable de la sécurité des systèmes d'information ou son équivalent, d'un représentant du responsable de la protection des renseignements personnels, d'un représentant de la vérification interne, d'un représentant de la Direction de l'informatique ou son équivalent, d'un représentant du détenteur de chaque système d'information analysé, d'un représentant des utilisateurs de chaque système d'information analysé, d'un représentant des ressources matérielles ou son équivalent (pour les questions relatives aux édifices) et d'un représentant des affaires juridiques.

6. Définition des types de mesures Méhari

Comme leur nom l'indique, les mesures structurelles agissent sur la structure même du ministère ou de l'organisme public pour éviter qu'elle subisse certaines agressions de nature humaine ou autre, et pour en limiter la gravité, le cas échéant.

Exemples

Sensibilisation du personnel

Programmes de formation

Les **mesures de dissuasion** empêchent des agressions de nature humaine, puisqu'elles permettent de persuader les personnes qui veulent les mettre à exécution d'y renoncer.

Exemples

Surveillance des réseaux

Enregistrement des anomalies

Les **mesures de prévention** ont pour objet d'empêcher une menace d'atteindre des ressources.

Exemples

Contrôle de la mise en production

Contrôle de la confidentialité des échanges et des communications

Chiffrement des données

Gestion des autorisations d'accès et des privilèges

Les **mesures de protection** n'évitent pas les détériorations possibles, mais elles en limitent l'ampleur. Elles réduisent les conséquences directes d'une menace.

Exemples

Investigation sur des anomalies

Scellement des données sensibles

Gestion des autorisations d'accès et des privilèges

Les **mesures palliatives** limitent les conséquences de possibles détériorations. Elles réduisent les conséquences indirectes d'une menace.

Exemples

Plan de continuité des services (PCS)

Plan de relève des utilisateurs (PRU)

Les **mesures de récupération** visent à récupérer une partie du préjudice subi en faisant endosser des pertes par des tiers (assurances, dommages et intérêts consécutifs à des actions en justice). En somme, elles limitent les pertes financières.

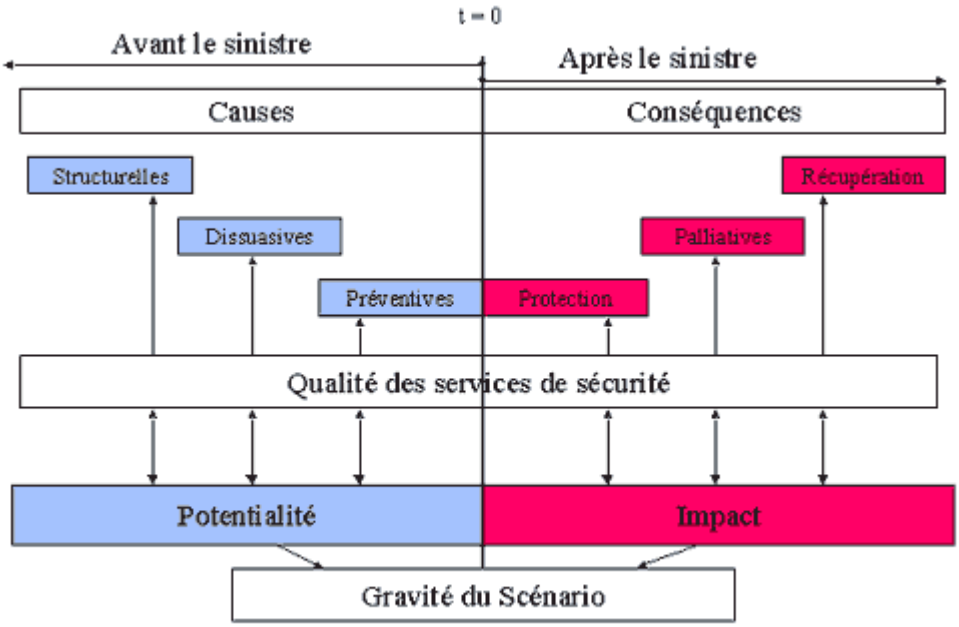
Exemples

Assurances de biens matériels

Gestion des assurances

Recours légaux

Synoptique des mesures de sécurité selon Méhari



Synoptique des mesures de sécurité selon MEHARI

7. Pondération des questions et des scénarios de risques Méhari

L'efficacité, ou le résultat de l'audit, d'un sous-service de sécurité est calculée en compilant la valeur attribuée à chaque question et en tenant compte des MIN et des MAX.

Pondération

2 Valeur minimale attribuée à une question selon la méthodologie Méhari.

4 Valeur attribuée à une question jugée plus importante pour l'atteinte de l'efficacité du sous-service de sécurité.

MAX Valeur MAXIMALE attribuée au sous-service de sécurité lors du calcul de l'audit, si la réponse à la question est NON.

MIN Valeur MINIMALE attribuée au sous-service de sécurité lors du calcul de l'audit, si la réponse à la question est OUI.

Pondération des scénarios

La gravité des scénarios est calculée à partir de l'effet conjugué de l'efficacité de chacun des sous-services de sécurité pris en considération pour diminuer la potentialité ou atténuer les impacts.

MAX La formule MAX est utilisée pour mettre en relation deux mesures ou plus jugées équivalentes.

MIN La formule MIN est utilisée pour mettre en relation deux mesures ou plus jugées complémentaires.

8. Scénarios de risques Méhari

La méthode Méhari comporte plusieurs scénarios de risques ou de menaces. Les scénarios sont analysés en fonction de la disponibilité, de l'intégrité et de la confidentialité des actifs informationnels ou des systèmes d'information du ministère ou de l'organisme public. Or, ces trois concepts sont étroitement liés à la notion de sécurité de l'information. Bien qu'il s'avère que, sous bien des aspects, la sécurité de l'information et la protection des renseignements personnels sont reliées et se recoupent souvent, ces deux notions ne sont pas synonymes.

À preuve, un certain nombre de scénarios de risques Méhari (voir l'annexe B) relèvent autant de la sécurité que de la protection des renseignements personnels, soit :

- l'altération de données;
- la manipulation de données;
- la divulgation de données;
- le détournement de fichiers de données;
- la perte de fichiers;
- les poursuites judiciaires concernant la réglementation des données personnelles, qui est renommée « réglementation concernant les renseignements personnels » dans ce document.

D'autres aspects de la protection des renseignements personnels ne s'y trouvent pas, comme une collecte non justifiée, une communication illégale ou une utilisation illicite.

En conséquence, considérant que la protection des renseignements personnels se traduit concrètement par le respect des principes et des règles législatives relativement à :

- la collecte de renseignements personnels;
- leur accessibilité par le personnel visé;
- leur accessibilité par la personne visée;
- leur rectification;
- leur utilisation à l'interne (traitement);
- leur communication;
- leur détention et leur conservation;
- leur archivage et leur destruction.

Considérant le fait que les scénarios de risques actuels Méhari ne recouvrent pas totalement ces aspects de la protection des renseignements personnels,

le groupe de travail ministériel propose huit nouveaux scénarios de risques :

- la collecte non nécessaire;
- la communication non autorisée;

- l’utilisation illicite de renseignements personnels;
- l’accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire);
- l’accès par une personne non autorisée (habilitation non reconnue);
- la détention au-delà de la limite prévue au calendrier de conservation;
- la non-destruction d’un renseignement personnel dont l'objet est accompli;
- le refus d'une demande d'accès ou d'une demande de rectification concernant un renseignement personnel.

Ces huit nouveaux scénarios de risques sont classés sous la rubrique Méhari « Non-conformité à la législation et à la réglementation – Réglementation des renseignements personnels ».

Comme la définition de chaque scénario de risques Méhari est basée sur un modèle qui tient compte de la présence et de l’efficacité des types de mesures susceptibles d’en diminuer la potentialité ou les impacts, les mesures de protection à ajouter (nouveaux services) ou à prendre en considération (services existants) pour calculer la gravité de chacun de ces nouveaux scénarios sont présentées par la suite.

9. Audit des nouveaux services

Champ	Service	Sous-service	Question		Pondération	MAX	MIN
1			**Domaine de l'organisation de la sécurité**				
	01E		**PRP– Organisation de la gestion de la PRP**				
		01E01	**Politique relative à la PRP**				
			01E01-01	Existe-t-il une politique en matière de PRP ou la politique de sécurité existante comporte-t-elle des volets propres à la PRP?	4,0	2,0	
			01E01-02	Cette politique a-t-elle été approuvée par les instances dirigeantes?	2,0		
			01E01-03	Cette politique a-t-elle été transmise à tous les membres du personnel?	4,0		
			01E01-04	Cette politique contient-elle des mesures conforment à celles édictées à cette fin par règlement du gouvernement?	4,0		
			01E01-05	Cette politique prévoit-elle des sanctions en cas de défaut ou de non-conformité?	2,0		
			01E01-06	Un responsable ou un répondant en matière de PRP a-t-il été nommé?	4,0		
			01E01-07	Le responsable ou le répondant en matière de PRP est-il connu de tous les membres du personnel?	2,0		
			01E01-08	Cette politique indique-t-elle que la PRP doit être prise en considération dans le développement des projets liés aux technologies de l'information?	2,0		
			01E01-09	Cette politique (ou le cadre de gestion) établit-elle clairement les responsabilités des différents intervenants : responsable de la PRP (RPRP), responsable de la sécurité de l’information gouvernementale, vérificateur interne, etc.?	4,0	2,0	
			01E01-10	Cette politique recouvre-t-elle l'ensemble des obligations légales en matière de PRP, dont celles qui ont trait à la collecte de tels renseignements, à leur accès, à leur communication, à leur utilisation, à leur conservation et à leur destruction?	4,0		

Champ Service Sous-service	Question	Pondération	MAX	MIN
01E01-11	Un comité relevant des instances dirigeantes est-il chargé d'élaborer les orientations en matière de PRP et d'étudier périodiquement les problématiques qui y sont liées, et est-il composé notamment du RPRP et de représentants de la direction, de la sécurité, de l'audit, de l'informatique, des affaires juridiques, de la gestion documentaire et des utilisateurs?	2,0		
01E01-12	Cette politique est-elle révisée au moins tous les cinq ans?	2,0		
01E01-13	L'application de cette politique fait-elle périodiquement l'objet d'un audit?	2,0		

01E02 PRP – Programme de formation et de sensibilisation à la PRP

01E02-01	Existe-t-il un programme de formation ou de sensibilisation en matière de PRP?	4,0	2,0	
01E02-02	Ce programme a-t-il été approuvé par le responsable ou le répondant en matière de PRP?	2,0		
01E02-03	Ce programme est-il offert aux personnes qui traitent des informations visées par les dispositions légales en matière de PRP?	4,0		
01E02-04	Ce programme est-il adapté aux tâches accomplies?	2,0		
01E02-05	Ce programme tient-il compte des problématiques en matière de PRP propres à l'utilisation des systèmes informatiques et de télécommunication?	2,0		
01E02-06	Ce programme inclut-il une formation ou une sensibilisation aux conséquences possibles de non-respect des dispositions légales en matière de PRP?	2,0		
01E02-07	Le niveau de connaissance des membres du personnel en matière de PRP est-il évalué périodiquement à l'aide de sondages ou autrement?	2,0		
01E02-08	L’existence de ce programme est-elle rappelée périodiquement aux membres du personnel par le moyen de l'affichage, de communiqués, etc.?	4,0		
01E02-09	Ce programme est-il révisé au moins tous les cinq ans?	2,0		
01E02-10	L'application de ce programme fait-elle l'objet d'un audit périodique?	2,0		

Champ Service Sous-service	Question		Pondération	MAX	MIN
01E03	**PRP – Procédure préalable à la collecte**				
01E03-01	Existe-t-il une norme de documentation au regard des renseignements personnels à recueillir?		2,0		
01E03-02	Cette norme a-t-elle été approuvée par les instances dirigeantes?		2,0		
01E03-03	Cette norme a-t-elle été transmise aux personnes chargées de faire la collecte de renseignements personnels, y compris celles qui veillent au développement de système?		2,0		
01E03-04	Est-il prévu de fournir, dans la documentation, les raisons justifiant la collecte des informations visées par les dispositions légales de PRP?		4,0		
01E03-05	Le ministère ou l'organisme public a-t-il établi des critères afin de juger de la nécessité de recueillir des renseignements personnels pour exercer ses attributions, pour accomplir sa mission ou pour mettre en œuvre un programme qu'il gère?		4,0	2,0	2,0
01E03-06	Cette norme prévoit-elle la diffusion de documentation sur les sources d'obtention des renseignements personnels?		20		
01E03-07	Cette norme est-elle révisée au moins tous les cinq ans?		2,0		
01E03-08	L'application de cette norme fait-elle l'objet d'un audit périodique?		2,0		

Champ Service	Sous-service	Question	Pondération	MAX	MIN
	01E04	**PRP – Procédures de collecte des informations visées par les dispositions légales en matière de PRP**			
		01E04-01 Existe-t-il des procédures particulières quant à la collecte des informations visées par les dispositions légales en matière de PRP?	4,0	2,0	
		01E04-02 Ces procédures ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E04-03 Ces procédures ont-elles été transmises aux personnes visées, y compris celles qui veillent au développement de système?	4,0		
		01E04-04 Ces procédures comportent-elles des instructions quant à l'information à donner, au moment de la collecte, aux personnes qui fournissent des renseignements personnels, quant à la façon dont celles-ci doivent utiliser cette information, quant aux droits d'accès et de rectification, etc.?	2,0		
		01E04-05 Ces procédures comportent-elles des instructions quant aux mesures de sécurité propres à assurer raisonnablement la protection des renseignements personnels collectés, compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support?	4,0	2,0	
		01E04-06 Ces procédures comportent-elles des instructions, dans les cas où il y a collecte de renseignements personnels nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune, notamment celle visant l'établissement d'une entente écrite devant être transmise à l'autorité compétente (Commission d'accès à l'information (CAI)?	4,0		
		01E04-07 Ces procédures comportent-elles des instructions concernant la collecte de renseignements personnels déjà recueillis auprès d'une personne ou d'une entreprise, notamment celle visant d'en informer préalablement l'autorité compétente (CAI)?	2,0		
		01E04-08 Ces procédures font-elles l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E04-09 L'application de ces procédures fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E05	**PRP – Inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP**				
		01E05-01	Existe-t-il une procédure en vue de mettre à jour l'inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP recueillis?	4,0	2,0	
		01E05-02	Cette procédure a-t-elle été approuvée par les instances dirigeantes?	2,0		
		01E05-03	Cette procédure a-t-elle été transmise aux personnes chargées de l'appliquer?	2,0		
		01E05-04	Cette directive décrit-elle les éléments de données devant faire partie de l'inventaire?	4,0		
		01E05-05	Cette procédure définit-elle les responsabilités au regard de la mise à jour de l'inventaire des fichiers?	2,0		
		01E05-06	Cette procédure prévoit-elle les mécanismes pour rendre cet inventaire accessible?	4,0		
		01E05-07	Toute création d'une banque de caractéristiques ou de mesures biométriques est-elle préalablement divulguée à l'autorité compétente (CAI)?	4,0		
		01E05-08	Cette procédure fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E05-09	L'application de cette procédure fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E06		**PRP – Procédures de communication des informations visées par les dispositions légales en matière de PRP**			
		01E06-01	Existe-t-il des procédures concernant la communication des informations visées par les dispositions légales en matière de PRP?	4,0	2,0	
		01E06-02	Ces procédures ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E06-03	Ces procédures ont-elles été transmises aux membres du personnel?	2,0		
		01E06-04	Ces procédures précisent-elles les règles de communication à suivre quant aux types de renseignements, aux destinataires de la communication, aux conditions d'exception, au processus d'autorisation de la communication, etc.?	4,0		
		01E06-05	Ces procédures comportent-elles des instructions quant aux mesures de sécurité propres à assurer la protection des renseignements personnels communiqués qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support?	4,0	2,0	
		01E06-06	Ces procédures précisent-elles que le destinataire doit faire l'objet d'une habilitation, c'est-à-dire d’une vérification de son droit d’obtenir l'information?	4,0		
		01E06-07	Ces procédures précisent-elles qui est autorisé à accorder la permission de communiquer des informations visées par les dispositions légales en matière de PRP?	4,0		
		01E06-08	Dans les cas où la communication de renseignements personnels se fait à l’extérieur du Québec, s’est-on assuré que ceux-ci bénéficieront d’une protection équivalant à celle prévue aux lois québécoises en matière de PRP?	4,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
		01E06-09	Ces procédures précisent-elles par qui, pour quels événements et comment les communications doivent être consignées dans un registre tenu conformément aux dispositions légales en matière de PRP?	2,0		
		01E06-10	Ces procédures font-elles l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E06-11	L'application de ces procédures fait-elle périodiquement l'objet d'un audit?	2,0		
		01E06-12	Lorsqu'elle est requise par une disposition légale, la communication de renseignements personnels sans consentement préalable de la personne concernée fait-elle l'objet d'une entente écrite comportant les instructions prescrites?	4,0		
		01E06-13	Cette entente écrite est-elle soumise à l'avis à l'autorité compétente (CAI) ou, si la communication est prévue expressément par la loi, l'entente est-elle transmise à l'autorité compétente (CAI)?	4,0		
		01E06-14	L'application des ententes fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question	Pondération	MAX	MIN
	01E07	**PRP – Consentement à la communication**			
		01E07-01 Existe-t-il des normes en vue d'évaluer la validité d'un consentement?	2,0		
		01E07-02 Ces normes ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E07-03 Ces normes ont-elles été transmises aux membres du personnel?	2,0		
		01E07-04 Ces normes font-elles l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E07-05 L'application de ces normes fait-elle l'objet d'un audit périodique?	2,0		
		01E07-06 Les libellés de consentement conçus pour l'usage du ministère ou de l'organisme public de même que les modalités selon lesquelles ils seront obtenus sont-ils approuvés préalablement par une personne indépendante qui s'y connaît en matière de PRP, telle que le responsable en la matière ou son répondant?	2,0		
	01E08	**PRP – Authentification de l'identité des personnes autorisées à prendre connaissance d'un renseignement personnel**			
		01E08-01 Existe-t-il des procédures assurant que l'authentification de l'identité des personnes ayant qualité pour agir au nom d'autrui, par exemple, au nom d'une personne inapte, est faite?	2,0		
		01E08-02 Ces procédures ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E08-03 Ces procédures ont-elles été transmises aux membres du personnel?	2,0		
		01E08-04 Ces procédures font-elles l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E08-05 L'application de ces procédures fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question	Pondération	MAX	MIN
	01E09	**PRP – Utilisation des renseignements anonymes**			
	01E09-01	Existe-t-il une procédure, notamment en ce qui concerne les activités d'évaluation de services, de tableaux de bord et d'autres activités de gestion stratégique, afin de déterminer et de mettre en œuvre les conditions à satisfaire pour que les résultats de l'utilisation des renseignements personnels soient présentés de façon anonyme?	4,0	2,0	
	01E09-02	Cette procédure a-t-elle été approuvée par les instances dirigeantes?	2,0		
	01E09-03	Cette procédure a-t-elle été transmise aux membres du personnel?	2,0		
	01F09-04	Cette procédure fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
	01E09-05	L'application de cette procédure fait l'objet d'un audit périodique?	2,0		
	01E10	**PRP – Qualité des renseignements personnels utilisés**			
	01E10-01	Existe-t-il des procédures en vue de contrôler et de vérifier la qualité des renseignements personnels recueillis ou utilisés (exactitude, fiabilité, complet et à jour)?	4,0	2,0	
	01E10-02	Ces procédures ont-elles été approuvées par les instances dirigeantes?	2,0		
	01E10-03	Ces procédures ont-elles été transmises aux membres du personnel?	2,0		
	01E10-04	Ces procédures font-elles l'objet d'une révision au moins tous les cinq ans?	2,0		
	01E10-05	L'application de ces procédures fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E11	**PRP – Utilisation des renseignements personnels aux bonnes fins**				
		01E11-01	Les fins pour lesquelles l'utilisation des renseignements personnels est permise sont-elles documentées?	4,0	2,0	
		01E11-02	Ces fins ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E11-03	La documentation concernant ces fins a-t-elle été transmise aux membres du personnel?	2,0		
		01E11-04	Cette documentation est-elle révisée au moins tous les cinq ans?	2,0		
		01E11-05	Existe-t-il des instructions quant aux mesures de sécurité propres à assurer la protection des renseignements personnels lors de leur utilisation qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support?	4,0	2,0	
		01E11-06	Existe-t-il des instructions quant à l'utilisation de renseignements personnels à d'autres fins que celles pour lesquelles ils ont été recueillis, notamment celle de l'inscription dans un registre?	4.0		
		01E11-07	A-t-on mis en place des moyens pour restreindre l'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels aux finalités pour lesquelles ils ont été collectés?	4,0		
		01E11-08	Existe-t-il une directive concernant l'utilisation des renseignements personnels à des fins de sondage, de recherche à l'interne ou encore de renseignements qui sont communiqués à des tiers dans le cadre d'autorisation de recherche, après avis favorable de l'autorité compétente (CAI)?	2,0		
		01E11-09	Cette directive a-t-elle été approuvée par les instances dirigeantes?	2,0		
		01E11-10	Cette directive est-elle révisée au moins tous les cinq ans?	2,0		
		01E11-11	L'application de cette directive fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E12	**PRP – Procédure relative à l'accès aux renseignements personnels et à leur rectification**				
		01E12-01	Existe-il une politique ou une directive qui favorise l'exercice du droit d'accès aux renseignements personnels et du droit de les rectifier?	2,0		
		01E12-02	Cette politique ou cette directive a-t-elle été approuvée par les instances dirigeantes?	2,0		
		01E12-03	Cette politique ou cette directive a-t-elle été transmise aux membres du personnel?	2,0		
		01E12-04	Cette politique ou cette directive précise-t-elle les rôles et les responsabilités des intervenants quant au traitement des demandes?	4,0	2,0	
		01E12-05	Cette politique prévoie-t-elle des mesures d'accommodement raisonnables, lorsque le requérant est une personne handicapée?	4,0		
		01E12-06	Cette politique ou cette directive fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E12-07	Cette politique ou cette directive fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E13	**PRP – Exigences relatives à l’engagement du personnel**				
		01E13-01	Les attentes du ministère ou de l’organisme public en matière de PRP sont-elles intégrées dans le processus d'engagement du personnel (responsabilités, connaissances, attitudes et aptitudes)?	4,0		
		01E13-02	Ces attentes ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E13-03	Ces attentes ont-elles été exposées à tous les nouveaux employés et chacun comprend-il l'importance de ses obligations?	4,0		
		01E13-04	Le processus d'engagement prévoit-il l'habilitation du personnel pour s'assurer de leur intégrité et de leur engagement en matière de PPR avant leur entrée en fonction?	2,0		
		01E13-05	Les attentes en matière de PRP exposées lors de l'engagement du personnel sont-elles renouvelées au moins tous les cinq ans?	2,0		
		01E13-06	Le processus d'engagement du personnel fait-il l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E14	**PRP – Exigences relatives au personnel en emploi**				
		01E14-01	Les attentes du ministère ou de l’organisme public en matière de PRP sont-elles intégrées dans le processus de gestion de rendement du personnel (responsabilités, connaissances, attitudes et aptitudes)?	4,0		
		01E14-02	Ces attentes ont-elles été approuvées par les instances dirigeantes?	2,0		
		01E14-03	Ces attentes ont-elles été rappelées périodiquement aux membres du personnel?	2,0		
		01E14-04	Les obligations en matière de PRP sont-elles périodiquement rappelées aux membres du personnel et chacun comprend-il l'importance de ses responsabilités au regard de la PRP?	2,0		
		01E14-05	Lorsqu'elles sont applicables, des sanctions sont-elles prévues en ce qui concerne le non-respect des obligations en matière de PRP et le non-respect des règles déontologiques qui ne découlent pas de l’engagement personnel des employés?	4,0		
		01E14-06	Ces attentes sont-elles mises à jour au moins tous les cinq ans?	2,0		
		01E14-07	Le processus de gestion du rendement en ce qui concerne les attentes en matière de PRP fait-il l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
	01E15	**PRP – Gestion des relations avec les fournisseurs**				
		01E15-01	Le processus de gestion des contrats de services comprend-il des exigences en matière de PRP?	4,0		
		01E15-02	Un modèle de contrat de services nécessitant la communication de renseignements personnels a-t-il été conçu de façon à contenir des clauses sur l'engagement du fournisseur, de son personnel et de ses sous-traitants à la confidentialité et sur leurs obligations au regard de la protection des renseignements personnels qui leur seront communiqués?	4,0	2,0	
		01E15-03	Ce processus prévoit-il une étape d'authentification des contrats qui nécessitent la communication de renseignements personnels?	2,0		
		01E15-04	Ce processus prévoit-il l'inscription des contrats qui nécessitent la communication de renseignements personnels dans un registre de communication?	2,0		
		01E15-05	Ce processus prévoit-il des procédures d'habilitation pour s'assurer de la probité des contractuels avant leur entrée en fonction?	2,0		
		01E15-06	Le modèle de contrat comporte-t-il des clauses permettant d'informer un fournisseur, à qui on confie un document technologique pour qu'il en assure la garde, quant à la protection que requiert ce document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance?	4,0		
		01E15-07	Le modèle de contrat comporte-t-il des clauses qui obligent le fournisseur à garantir que toute communication à l'extérieur du Québec de renseignements personnels qui lui sont confiés par l'organisme bénéficiera d'une protection équivalent à celle prévue aux lois québécoises en matière de PRP?	4,0		
		01E15-08	Ce processus, y compris, le cas échéant, le modèle de contrat de services, a-t-il été approuvé par le responsable ou le répondant en matière de PRP?	2,0		
		01E15-09	Ce processus, y compris, le cas échéant, le modèle de contrat de services, a-t-il été transmis aux responsables de l'élaboration de tels contrats?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
		01E15-10	Ce processus, y compris, le cas échéant, le modèle de contrat de services, fait-il l'objet d'une révision au moins tous les cinq ans?	2,0		
		01E15-11	Ce processus fait-il l'objet d'un audit périodique?	2,0		
7		**Domaine de la sécurité des systèmes et de leur architecture**				
07A		**Contrôle d'accès aux systèmes et aux applications**				
	07A05	**PRP – Contrôle d'accès aux renseignements personnels**				
		07A05-01	Existe-t-il une procédure qui autorise l'accès aux renseignements personnels uniquement lorsque des personnes exercent leurs fonctions ou remplissent leurs mandats respectifs?	4,0	2,0	
		07A05-02	Cette procédure a-t-elle été approuvée par les instances dirigeantes?	2,0		
		07A05-03	Cette procédure a-t-elle été transmise aux membres du personnel?	2,0		
		07A05-04	Cette procédure prévoit-elle que seuls les employés désignés dans l'inventaire de fichiers auront accès aux renseignements personnels?	2,0		
		07A05-05	Cette procédure prévoit-elle que les contrôles d'accès seront conçus de façon à ce que tout ce qui a trait à la création, à la modification, à la consultation ou à la destruction de renseignements personnels puisse être retracé, au moins d'après la date et l'identité de la personne (journalisation des accès)?	2,0		
		07A05-06	Cette procédure prévoit-elle l'analyse périodique des différents journaux générés par les contrôles d'accès (recherche et analyse d'incidents)?	2,0		
		07A05-07	Cette procédure fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
		07A05-08	L'application de cette procédure fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
8			**Domaine de la production informatique**			
08C			**Gestion des supports informatiques de données et de programmes**			
	08C07		**PRP – Contrôle de la diffusion des supports (imprimé, disquette, CD, etc.) contenant des informations visées par les dispositions légales en matière de PRP**			
		08C07-01	Existe-t-il une procédure particulière en vue de reproduire et de diffuser des renseignements personnels (prise de copie sur disquette ou CD-ROM, remise en main propre sous enveloppe cachetée, etc.)?	4,0	2,0	
		08C07-02	Cette procédure a-t-elle été approuvée par les instances dirigeantes?	2,0		
		08C07-03	Cette procédure a-t-elle été transmise aux membres du personnel?	2,0		
		08C07-04	Cette procédure prévoit-elle que la reproduction des supports contenant des renseignements personnels devra être faite en présence d'une personne habilitée, donc sous sa surveillance?	2,0		
		08C07-05	Est-il indiqué dans cette procédure que la possibilité de reproduire des supports contenant des informations classées confidentielles qui sont visées par les dispositions légales en matière de PRP est restreinte aux personnes qui en ont besoin pour exécuter leur travail?	4,0	2,0	
		08C07-06	Cette procédure fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
		08C07-07	L'application de cette procédure fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question	Pondération	MAX	MIN
	08C08	**PRP – Processus de conservation, d'archivage et de destruction des informations visées par les dispositions légales en matière de PRP**			
		08C08-01 Les procédures d'archivage en vigueur tiennent-elles compte du fait que les différents supports peuvent comporter des documents visés par les dispositions légales en matière de PRP?	4,0	2,0	
		08C08-02 Une directive concernant la conservation, l'archivage et la destruction des renseignements personnels a-t-elle été mise en place?	4,0		
		08C08-03 Cette directive a-t-elle été approuvée par les instances dirigeantes?	2,0		
		08C08-04 Cette directive a-t-elle été transmise aux membres du personnel?	2,0		
		08C08-05 Cette directive tient-elle compte de tous les supports sur lesquels les renseignements personnels peuvent être emmagasinés?	4,0		
		08C08-06 Cette directive comporte-elle des instructions quant aux mesures de sécurité propres à assurer la protection des renseignements personnels conservés, archivés et détruits qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support?	4,0	2,0	
		08C08-07 Existe-t-il un calendrier de conservation des documents qui détermine les délais de conservation des fichiers contenant des informations visées par les dispositions légales en matière de PRP en fonction du cycle de vie de ces derniers (actifs, semi-actifs et inactifs)?	4,0		
		08C08-08 Lorsque le mandat de destruction de renseignements personnels est confié à une firme externe, le contrat alors conclu comporte-t-il des clauses de confidentialité et de sécurité liées aux renseignements qui doivent être détruits ainsi que des pénalités en cas de non-respect de ces clauses?	4,0		
		08C08-09 Cette directive tient-elle compte des obligations concernant la destruction des renseignements personnels recueillis au nom du ministère ou de l'organisme public et détenus par ses mandataires?	4.0		
		08C08-10 Une personne est-elle chargée d'assurer la mise en application du calendrier de conservation ainsi que des procédures d'archivage et de destruction des renseignements personnels jugés non nécessaires?	4,0	2,0	

Champ Service	Sous-service	Question		Pondération	MAX	MIN
		08C08-11	Cette directive ou tout autre directive prévoit-elle que pour qu'un document source puisse être détruit et remplacé par le document qui résulte du transfert sur un autre support, le transfert doit être documenté en précisant les éléments suivants : le format d'origine du document dont l'information fait l'objet du transfert, le procédé de transfert utilisé ainsi que des garanties qu'il est censé offrir, selon les indications fournies avec le produit, quant à la préservation de l'intégrité, tant du document devant être transféré, s'il n'est pas détruit, que du document résultant du transfert?	4,0		
		08C08-12	La documentation résultant d'un transfert de format est-elle conservée durant tout le cycle de vie du document résultant du transfert?	4,0		
		08C08-13	Avant la destruction d'un document source, s'est-on préoccupé de sa valeur archivistique, historique ou patrimoniale eu égard aux critères élaborés par règlement?	4,0		
		08C08-14	Cette directive fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
		08C08-15	L'application de cette directive fait-elle l'objet d'un audit périodique?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
08E		**Gestion et traitement des incidents**				
	08E04	**PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP**				
		08E04-01	Existe-t-il une procédure concernant la gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP (accès non autorisé, utilisation illégale, communication non sécurisée, etc.)?	4,0	2,0	
		08E04-02	Cette procédure a-elle été approuvée par les instances dirigeantes?	2,0		
		08E04-03	Cette procédure a-elle été transmise aux membres du personnel?	2,0		
		08E04-04	Cette procédure oblige-t-elle les membres du personnel à assurer le suivi de tout incident lié aux informations visées par les dispositions légales en matière de PRP et à faire rapport aux instances dirigeantes?	2,0		
		08E04-05	Le responsable en matière de PRP (ou la direction) est-il systématiquement informé de tous les incidents visés par des dispositions légales en matière de PRP?	4,0		
		08E04-06	Cette procédure oblige-t-elle les membres du personnel à consigner dans un registre chaque incident lié aux informations visées par les dispositions légales en matière de PRP?	2,0		
		08E04-07	Cette procédure indique-t-elle que le contenu du registre doit faire l'objet d'un examen périodique en vue de vérifier les éléments répétitifs?	2,0		
		08E04-08	Cette procédure fait-elle l'objet d'une révision au moins tous les cinq ans?	2,0		
		08E04-09	L'application de cette procédure fait-elle l'objet d'un audit périodique?	2,0		
		08E04-10	Les incidents font-ils l'objet d'une analyse globale périodique afin de réviser les politiques et les procédures ou la formation du personnel?	2,0		

Champ Service	Sous-service	Question		Pondération	MAX	MIN
10			**Domaine de la sécurité des projets et des développements applicatifs**			
10C			**PRP – Gestion de la PRP dans les projets liés aux technologies de l'information**			
	10C01		**Prise en considération des exigences en matière de PRP dans le développement et la gestion de projets**			
		10C01-01	Le plan maître du projet de développement du système d'information incorpore-t-il les exigences légales en matière de PRP?	4,0		
		10C01-02	Toutes les activités effectuées en matière de PRP sont-elles intégrées à la planification détaillée du projet?	2,0		
		10C01-03	L'évaluation des risques liés à la PRP doit-elle être soumise aux instances dirigeantes avant l'approbation du projet?	4,0	2,0	
		10C01-04	Les rôles et les responsabilités des membres de l'équipe de projet en matière de PRP ont-ils été déterminés?	2,0		
		10C01-05	Les ressources humaines, matérielles et financières requises pour réaliser les biens livrables en matière de PRP ont-elles été allouées?	2,0		
		10C01-06	Le processus de priorisation des projets tient-il compte des risques liés à la PRP?	2,0		
		10C01-07	Les processus de développement de système d'information en vigueur intègrent-ils toutes les exigences légales en matière de PRP?	4,0		2,0
		10C01-08	Les procédures de développement de système d'information en vigueur dans l'organisme obligent-elles à faire une évaluation préalable des risques des projets de développement en matière de PRP?	4,0		
		10C01-09	Les personnes chargées du développement de système d'information reçoivent-elles une formation appropriée sur les principes et les obligations légales en matière de PRP?	2,0		
		10C01-10	L'application des règles en matière de PRP dans le développement de système d'information fait-elle l'objet d'un audit périodique?	2,0		

10. Audit des services existants

Service et Sous-Service	Question

1 Domaine organisation

01B Référentiel de sécurité

01B01 Devoirs et responsabilités du personnel et du management

01B01-01	Les devoirs et responsabilités du personnel quant à l'utilisation, la conservation et l'archivage des informations et à la protection du secret sont-ils précisés dans une note ou document mis à la disposition du management?
01B01-02	Les devoirs et responsabilités du personnel quant à l'utilisation et la protection des biens et ressources de l'entreprise sont-ils précisés dans une note ou document mis à la disposition du management?
01B01-03	Ces notes précisent-elles ce qui est toléré et les limites à ne pas dépasser (usage des biens de l'entreprise à des fins personnelles, par exemple)?
01B01-04	Ces notes précisent-elles la conduite à tenir en cas de dépassement ou d'abus?
01B01-05	Les devoirs et responsabilités du management dans le domaine de la protection de l'information et des ressources de l'entreprise sont-ils précisés dans une note ou document communiqué à l'ensemble des managers?
01B01-06	L'authenticité des notes publiées (ou de la Charte) relative aux devoirs et responsabilités du personnel est-elle contrôlée?
01B01-07	Existe-t-il une revue régulière de la charte des devoirs et responsabilités du personnel (ou des notes correspondantes)?

Service et Sous-Service **Question**

01C Gestion des ressources humaines

01C01 Engagement du personnel, clauses contractuelles

01C01-01	Une note précisant les devoirs et responsabilités du personnel a-t-elle été diffusée à l'ensemble des collaborateurs (y compris les intérimaires, stagiaires, etc.) de telle sorte qu'ils ne puissent nier en avoir eu connaissance?
01C01-02	Existe-t-il, dans les contrats d'embauche ou dans le règlement intérieur, une clause précisant l'obligation de respecter l'ensemble des règles de sécurité en vigueur?
01C01-03	Une note précisant les obligations légales, réglementaires ou contractuelles a-t-elle été diffusée à l'ensemble des collaborateurs?
01C01-04	Les devoirs et responsabilités imposés au personnel sont-ils imposés contractuellement (par le biais de conditions générales ou de clauses spécifiques) à tout prestataire intervenant au profit de l'entreprise et pouvant, de ce fait, avoir accès ou favoriser l'accès à des informations ou à des ressources sensibles?
01C01-05	Impose-t-on contractuellement à toute société prestataire pouvant avoir accès ou favoriser l'accès à des informations ou à des ressources sensibles, que ses collaborateurs signent un engagement personnel de respect des clauses de sécurité spécifiées?
01C01-06	Existe-t-il une procédure de contrôle de l'authenticité et de la pertinence des règles de sécurité diffusées à l'ensemble du personnel?

Service et Sous-Service **Question**

01C04 Sensibilisation et formation à la sécurité

01C04-01	Existe-t-il un programme de sensibilisation du personnel aux risques d'accident, d'erreur et de malveillance relatifs au traitement de l'information?
01C04-02	Ce programme de sensibilisation touche-t-il l'ensemble du personnel et est-il réactivé régulièrement?
01C04-03	Existe-t-il un programme de formation du personnel aux règles et mesures générales de protection de l'information?
01C04-04	Ces règles et mesures générales couvrent-elles l'ensemble des domaines concernés (documents, micro-informatique, accès aux systèmes et applications, téléphone et fax, comportements en réunion ou à l'extérieur, etc.)?
01C04-05	Ces règles et mesures générales sont-elles facilement accessibles au personnel en cas de besoin (intranet par exemple) et a-t-on communiqué sur cette possibilité?
01C04-06	Le personnel ayant des responsabilités dans le domaine de la sécurité reçoit-il une formation particulière adaptée?
01C04-07	Existe-t-il un tableau de bord de la mise en œuvre effective des actions de sensibilisation et de formation?
01C04-08	Existe-t-il un suivi du niveau de satisfaction et d'adhésion du personnel aux actions de sensibilisation et de formation à la sécurité des systèmes d'information?

Service et Sous-Service	Question

01D Assurances

01D02 Assurance de dommages immatériels

01D02-01	Les systèmes d'information sont-ils couverts par un contrat d'assurance couvrant les dommages immatériels (malveillance, utilisation non autorisée des systèmes d'information, pertes accidentelles de données ou de programmes, déni de service, etc.)?
01D02-02	Ce contrat couvre-t-il l'ensemble des systèmes informatiques (systèmes internes, intranet, extranet, sites Web, etc.)?
01D02-03	Ce contrat couvre-t-il toutes les causes usuelles de ce type de sinistre : accidents (pannes, bogues, etc.), erreurs humaines (erreurs de manipulation, erreurs de programmation, etc.), malveillances (fraudes, intrusions, déni de service, y compris par le personnel de l'entreprise ou préposé à son opération ou entretien)?
01D02-04	Ce contrat assure-t-il tous les frais (réels) d'investigation et de recherche des causes et des conséquences du sinistre?
01D02-05	Ce contrat assure-t-il tous les frais (réels) de réinitialisation des systèmes d'information touchés par le sinistre (frais de redémarrage et de test après redémarrage, frais de reconstitution des données, etc.)?
01D02-06	Ce contrat couvre-t-il tous les frais supplémentaires d'exploitation et de fonctionnement (prise en charge des frais et dépenses qui continuent à courir, des frais exposés pour éviter ou limiter l'arrêt de l'activité)?
01D02-07	Ce contrat couvre-t-il tous les frais supplémentaires engagés par l'entreprise pour rétablir son image auprès de ses clients ou partenaires?
01D02-08	Ce contrat couvre-t-il globalement la perte d'exploitation engendrée par le sinistre?
01D02-09	Le choix des garanties en matière informatique (exclusions, franchises, etc.) est-il le résultat d'une étude spécifique conduite en commun avec la Direction Informatique et remise à jour régulièrement?
01D02-10	Les niveaux des garanties et des franchises permettent-ils de garantir la survie de l'entreprise en cas de sinistre?
01D02-11	Les niveaux des garanties et des franchises permettent-ils de garantir qu'un sinistre pourrait être supporté sans conséquences graves pour l'entreprise?

Service et Sous-Service	Question

4 Domaine du réseau étendu (intersites)

04B Contrôle des connexions sur le réseau étendu

04B01 Profils de sécurité des entités connectées au réseau étendu

04B01-01	A-t-on défini un ensemble de règles pour qu'une entité puisse être connectée au réseau étendu considéré comme un espace de confiance?
04B01-02	Ces règles couvrent-elles l'organisation nécessaire au sein de chaque entité connectée et la nomination de responsables de la sécurité de divers domaines (sécurité physique, sécurité des systèmes d'information, etc.)?
04B01-03	Ces règles définissent-elles les mesures de sécurité physique devant protéger les équipements de réseau et le câblage?
04B01-04	Ces règles définissent-elles les mesures de sécurité logique devant protéger les équipements de réseau et les équipements de sécurité?
04B01-05	Ces règles précisent-elles les filtrages à assurer pour les accès entrants aussi bien que pour les accès sortants?
04B01-06	Ces règles précisent-elles les contrôles à effectuer sur les configurations des équipements de réseau et sur les configurations des postes utilisateurs?
04B01-07	Ces règles définissent-elles les mesures nécessaires pour la gestion des anomalies et incidents et les rapports obligatoires vers une entité centrale?
04B01-08	Existe-t-il une procédure de gestion des demandes d'autorisation de rattachement au réseau étendu émanant des entités, et une structure en charge de l'analyse de ces demandes, de l'audit de l'application des règles, et de la suppression des droits spécifiques quand le besoin a disparu ou quand les conditions exigées ne sont plus remplies?
04B01-09	Procède-t-on régulièrement à un audit des conditions requises et de l'application des règles, dans chaque entité autorisée à faire partie du réseau étendu?

Service et Sous-Service	Question

04B02 Authentification de l’entité accédante lors des accès entrants depuis le réseau étendu

04B02-01	Y a-t-il un mécanisme d'authentification et de contrôle d'accès de l'entité appelante avant tout accès au réseau local depuis le réseau étendu?
04B02-02	Le processus d'authentification est-il un processus reconnu comme «°fort »? Un simple mot de passe sera toujours un point faible notable. Les seuls processus qui soient reconnus comme forts, c'est-à-dire observables sans divulguer d'information et pratiquement inviolables sont basés sur des algorithmes cryptologiques.
04B02-03	La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supports de l'authentification (clés secrètes ou publiques, etc.), ainsi que leur transmission entre des systèmes de référence et les équipements de sécurité, font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité? Dans le cas d'authentification faisant appel à des procédés cryptologiques, les mécanismes de modification, de stockage et de transmission des éléments de base (des clés publiques, en particulier) doit présenter des garanties de solidité au même titre que le protocole d'authentification.
04B02-04	Les procédures de gestion des clés révoquées garantissent-elles que les systèmes de contrôle prennent en compte ces révocations en temps réel et testent systématiquement que les clés ne sont pas révoquées?
04B02-05	Les processus qui assurent l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.

Service et Sous-Service	Question

04B03 Authentification de l’entité accédée lors des accès sortants vers d’autres entités par le réseau étendu

04B03-01	Y a-t-il un mécanisme d'authentification et de contrôle d'accès de l'entité appelée avant tout accès sortant depuis le réseau interne par le réseau étendu?
04B03-02	Le processus d'authentification est-il un processus reconnu comme « fort »?
04B03-03	La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supports de l'authentification (mots de passe, clés publiques, etc.), ainsi que leur transmission entre des systèmes de référence et les équipements de sécurité, font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité? Dans le cas d'authentification faisant appel à des procédés cryptologiques, les mécanismes de modification, de stockage et de transmission des éléments de base (des clés publiques, en particulier) doit présenter des garanties de solidité au même titre que le protocole d'authentification.
04B03-04	Les procédures de gestion des clés révoquées garantissent-elles que les systèmes de contrôle prennent en compte ces révocations en temps réel et testent systématiquement que les clés ne sont pas révoquées?
04B03-05	Les processus qui assurent l'authentification sont-ils sous contrôle strict.

Service et Sous-Service	Question

04D Contrôle, détection et traitement des incidents sur le réseau étendu

04D01 Surveillance (en temps réel) du réseau étendu

04D01-01	A-t-on défini un ensemble de règles pour qu'une entité puisse être connectée au réseau étendu considéré comme un espace de confiance?
04D01-02	Le système dispose-t-il d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur des ports non ouverts, etc.)?
04D01-03	Emploie-t-on un système de détection d'intrusion et d'anomalies sur le réseau étendu?
04D01-04	Existe-t-il une (ou plusieurs) application capable d'analyser les divers diagnostics individuels d'anomalies sur le réseau étendu et de déclencher une alerte à destination du personnel d'exploitation?
04D01-05	Existe-t-il, parmi le personnel d'exploitation, une équipe permanente ou sous astreinte permanente capable de réagir en cas d'alerte de la surveillance du réseau étendu?
04D01-06	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe d'intervention et sa disponibilité est-elle suffisante pour faire face à cette attente?
04D01-07	Les paramètres définissant les alarmes sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
04D01-08	Toute inhibition du système d'alerte lié au réseau étendu déclenche-t-elle une alarme auprès de l'équipe de surveillance?
04D01-09	Existe-t-il un archivage (sur disque, cassette, DON, etc.) de tous les éléments ayant permis de détecter une anomalie ou un incident?
04D01-10	Les procédures de surveillance du réseau étendu et de détection d'anomalies et la disponibilité de l'équipe de surveillance font-elles l'objet d'un audit régulier?

Service et Sous-Service	Question

04D02 Analyse en temps différé des traces, logs et journaux d'événements sur le réseau étendu

04D02-01	A-t-on fait une analyse approfondie des événements ou succession d'événements sur le réseau étendu pouvant avoir un impact sur la sécurité (connexions refusées, reroutages, reconfigurations, évolutions de performances, accès à des informations ou des outils sensibles, etc.)?
04D02-02	Enregistre-t-on ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure?
04D02-03	Existe-t-il une application capable d'analyser ces enregistrements ainsi que les mesures de performances, d'en déduire des statistiques, un tableau de bord et des diagnostics d'anomalies examinés par une structure ad hoc?
04D02-04	La structure chargée d'analyser ces éléments de synthèse (ou éventuellement les journaux des incidents, et événements liés à la sécurité) a-t-elle l'obligation de le faire à période fixe et déterminée et a-t-elle la disponibilité suffisante?
04D02-05	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe de surveillance et sa disponibilité est-elle suffisante pour faire face à cette attente?
04D02-06	Les paramètres définissant les éléments à enregistrer et les synthèses effectuées sur ces éléments sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
04D02-07	Toute inhibition du système d'enregistrement et de traitement des enregistrements déclenche-t-elle une alarme auprès de l'équipe de surveillance?
04D02-08	Les enregistrements ou les synthèses sont-ils conservés sur une longue durée?
04D02-09	Les procédures d'enregistrement, de traitement des enregistrements et d'analyse des synthèses ainsi que la disponibilité de l'équipe d'analyse et d'intervention font-elles l'objet d'un audit régulier?

Service et Sous-Service	Question

04D03 Traitement des incidents du réseau étendu

04D03-01	Y a-t-il une équipe (hot line) accessible en permanence, chargée de recueillir les appels liés au réseau étendu et de signaler et d'enregistrer tous les incidents?
04D03-02	Y a-t-il un système support de la gestion des incidents?
04D03-03	Ce système centralise-t-il et prend-il en compte aussi bien les incidents détectés par l'exploitation que ceux signalés par les utilisateurs?
04D03-04	Ce système permet-il un suivi et une relance automatiques des actions nécessaires?
04B03-05	Ce système incorpore-t-il une typologie des incidents avec élaboration de statistiques et de tableau de bord des incidents à destination du RSSI?
04D03-06	Le système de gestion d'incidents est-il strictement contrôlé vis-à-vis de toute modification illicite ou indue? Un contrôle strict requiert une protection renforcée pour pouvoir modifier un enregistrement et un audit de toute modification des enregistrements ou un contrôle par scellement électronique de toute modification.
04B03-07	Chaque incident réseau majeur fait-il l'objet d'un suivi spécifique (nature et description, priorité, solutions techniques, études en cours, délai prévu de résolution, etc.)?

Service et Sous-Service	Question

5 Domaine du réseau local

05B Contrôle d’accès au réseau local de « données »

05B01 Gestion des profils d’accès au réseau local de « données »

05B01-01	Les droits d'accès au réseau local et aux diverses parties de ce réseau en cas de partitionnement, sont-ils définis par rapport à des ""profils"" métiers regroupant des ""rôles"" ou des ""fonctions"" dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil)? Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de ""groupe"". Par ailleurs les droits attribués éventuellement à des partenaires doivent être pris en compte. Les profils d'accès doivent comprendre les profils d'accès à chaque partitionnement du réseau, depuis un poste connecté directement sur le réseau et depuis les diverses possibilités prévues de connexion depuis l'extérieur du réseau (postes nomades, télétravail, partenaires, etc.)
05B01-02	A-t-on introduit, dans les règles de définition des droits (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte, en particulier la localisation du poste du demandeur (réseau interne, étendu, externe), la nature de la connexion utilisée (LAN, LS, Internet, type de protocoles, etc.) ou la classification du sous-réseau demandé?
05B01-03	Les profils permettent-ils également de définir des créneaux horaires et calendaires de travail (heures début et fin de journée, week-end, vacances, etc.)
05B01-04	Ces profils et l'attribution de droits aux différents profils, en fonction du contexte, ont-ils reçu l'approbation des propriétaires d'information et du RSSI?
05B01-05	Les processus de définition et de gestion des droits attribués aux profils sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les droits attribués aux profils soit très limitée, que la matérialisation de ces droits sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.
05B01-06	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des droits attribués à chaque profil et des procédures de gestion des profils?

Service et Sous-Service **Question**

05B02 Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)

05B02-01	La procédure d'attribution d'autorisations d'accès au réseau local nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ou de l'organisme responsable de la prestation en cas de droits attribués à des partenaires?
05B02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs?
05B02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations d'accès au réseau local à un individu (directement ou par le biais de profils) est-il strictement contrôlé? Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.
05B02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès au réseau local lors de départs de personnel interne ou de fin de mission de personnel externe à l'entreprise ou de changements de fonctions?
05B02-05	Y a-t-il une liste indiquant l'ensemble des personnes ayant des autorisations d'accès au réseau local?
05B02-06	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des autorisations d'accès au réseau local attribués au personnel ou à des partenaires?

Service et Sous-Service	Question

05B03 Authentification de l'accédant lors des accès au réseau local depuis un point d'accès interne

05B03-01	Y a-t-il un mécanisme d'authentification et de contrôle d'accès de chaque utilisateur avant tout accès à une ressource du réseau local?
05B03-02	Le processus de définition ou de modification de l'authentifiant support du contrôle d'accès pour les accès internes vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque? Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des ""standards systèmes"", des prénoms, de l'anagramme de l'identifiant, de dates, etc. Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques, processus de génération évalué ou reconnu publiquement, clés de chiffrement de longueur suffisante, etc.
05B03-03	Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité? La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce), soit à frapper un code qui change à chaque instant (carte à jeton), soit à présenter un caractère biométrique.
05B03-04	La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supports de l'authentification (mots de passe, numéro d'appelant, etc.), ainsi que leur transmission entre le poste appelant et les équipements de sécurité, font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité? Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.
05B03-05	A-t-on mis en place une dévalidation automatique de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur?
05B03-06	La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton, etc.) permet-elle d'inhiber instantanément l'ancien authentifiant et permet-elle un contrôle effectif de l'identité du demandeur?
05B03-07	Les paramètres de l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé

	pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.
05B03-08	Les processus qui assurent l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification..

Service et Sous-Service	Question

05B04 Authentification de l'accédant lors des accès au réseau local depuis un site distant via le réseau étendu

05B04-01	Les règles d'appartenance au réseau étendu exigent-elles l'authentification de chaque utilisateur avant tout accès sortant empruntant le réseau étendu?
05B04-02	Les règles d'appartenance au réseau étendu et les contrôles effectués permettent-ils d'accorder la même confiance aux utilisateurs du réseau étendu qu'aux utilisateurs locaux?
05B04-03	La pertinence des règles d'appartenance au réseau étendu est-elle régulièrement auditée?
05B04-04	L'application des règles d'appartenance au réseau étendu par l'ensemble des entités autorisées à se connecter au réseau étendu est-elle régulièrement auditée?

Service et Sous-Service	Question

05B05 Authentification de l'accédant lors des accès au réseau local depuis l'extérieur

05B05-01	Y a-t-il un mécanisme d'authentification et de contrôle d'accès de chaque utilisateur pour toute connexion au réseau local depuis l'extérieur?
05B05-02	Le processus de définition ou de modification de l'authentifiant support du contrôle d'accès pour les accès externes vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque? Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des ""standards systèmes"", des prénoms, de l'anagramme de l'identifiant, de dates, etc. Dans le cas d'authentifiants fixes (numéro de l'appelant), procédure de call-back. Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques, processus de génération évalué ou reconnu publiquement, clés de chiffrement de longueur suffisante, etc."
05B05-03	Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité? La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce) soit à frapper un code qui change à chaque instant (jeton type SecureId), soit à présenter un caractère biométrique.
05B05-04	La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supports de l'authentification (mots de passe, numéro d'appelant, etc.), ainsi que leur transmission entre le poste appelant et les équipements de sécurité, font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité? Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.
05B05-05	A-t-on mis en place une dévalidation automatique du poste ou de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur?
05B05-06	La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton, etc.) permet-elle d'inhiber instantanément l'ancien authentifiant et permet-elle un contrôle effectif de l'identité du demandeur?
05B05-07	Les paramètres de l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé

	pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.
05B05-08	Les processus qui assurent l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.

Service et Sous-Service	Question

05B06 Authentification de l'accédant lors des accès au réseau local depuis un sous-réseau WiFi

05B06-01	Tout sous-réseau WiFi est-il isolé du réseau local par un pare-feu?
05B06-02	Y a-t-il un mécanisme d'authentification et de contrôle d'accès de chaque utilisateur pour toute connexion au réseau local depuis un sous-réseau WiFi?
05B06-03	Le processus de définition ou de modification de l'authentifiant support du contrôle d'accès pour les accès depuis un sous-réseau WiFi vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque?
05B06-04	Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité?
05B06-05	La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supports de l'authentification (mots de passe), ainsi que leur transmission entre le poste appelant et les équipements de sécurité, font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité? Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.
05B06-06	A-t-on mis en place une dévalidation automatique du poste ou de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur?
05B06-07	La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton, etc.) permet-elle d'inhiber instantanément l'ancien authentifiant et permet-elle un contrôle effectif de l'identité du demandeur?
05B06-08	Les paramètres de l'authentification pour les accès depuis un sous-réseau WiFi sont-ils sous contrôle strict?
05B06-09	Les processus qui assurent l'authentification pour les accès depuis un sous-réseau WiFi sont-ils sous contrôle strict?

Service et Sous-Service **Question**

05D Contrôle, détection et traitement des incidents du réseau local

05D01 Traitement des incidents du réseau local

05D01-01	A-t-on analysé les événements ou successions d'événements pouvant être révélateurs de comportements anormaux ou d'actions illicites et en a-t-on déduit des points ou indicateurs de surveillance?
05D01-02	Le système dispose-t-il d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur des ports non ouverts, etc.)?
05D01-03	Emploie-t-on un système de détection d'intrusion et d'anomalies?
05D01-04	Existe-t-il une (ou plusieurs) application capable d'analyser les divers diagnostics individuels d'anomalies et de déclencher une alerte à destination du personnel d'exploitation?
05D01-05	Existe-t-il, parmi le personnel d'exploitation, une équipe permanente ou sous astreinte permanente capable de réagir en cas d'alerte de la surveillance réseau?
05D01-06	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe d'intervention et sa disponibilité est-elle suffisante pour faire face à cette attente?
05D01-07	Les paramètres définissant les alarmes sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
05D01-08	Toute inhibition du système d'alerte déclenche-t-elle une alarme auprès de l'équipe de surveillance?
05D01-09	Existe-t-il un archivage (sur disque, cassette, DON, etc.) de tous les éléments ayant permis de détecter une anomalie ou un incident?
05D01-10	Les procédures de surveillance du réseau et de détection d'anomalies et la disponibilité de l'équipe de surveillance font-elles l'objet d'un audit régulier?

Service et Sous-Service	Question

05D02 Analyse en temps différé des traces, logs et journaux d'événements sur le réseau local

05D02-01	A-t-on fait une analyse approfondie des événements ou succession d'événements pouvant avoir un impact sur la sécurité (connexions refusées, reroutages, reconfigurations, évolutions de performances, accès à des informations ou des outils sensibles, etc.)?
05D02-02	Enregistre-t-on ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure?
05D02-03	Existe-t-il une application capable d'analyser ces enregistrements ainsi que les mesures de performances, d'en déduire des statistiques, un tableau de bord et des diagnostics d'anomalies examinés par une structure ad hoc?
05D02-04	La structure chargée d'analyser ces éléments de synthèse (ou éventuellement les journaux des incidents, et événements liés à la sécurité) a-t-elle l'obligation de le faire à période fixe et déterminée et a-t-elle la disponibilité suffisante?
05B02-05	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe de surveillance et sa disponibilité est-elle suffisante pour faire face à cette attente?
05D02-06	Les paramètres définissant les éléments à enregistrer et les synthèses effectuées sur ces éléments sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
05D02-07	Toute inhibition du système d'enregistrement et de traitement des enregistrements déclenche-t-elle une alarme auprès de l'équipe de surveillance?
05D02-08	Les enregistrements ou les synthèses sont-ils conservés sur une longue durée?
05D02-09	Les procédures d'enregistrement, de traitement des enregistrements et d'analyse des synthèses ainsi que la disponibilité de l'équipe d'analyse et d'intervention font-elles l'objet d'un audit régulier?

Service et Sous-Service **Question**

05D03 Traitement des incidents du réseau local

05D03-01	Y a-t-il une équipe (hot line) accessible en permanence, chargée de recueillir les appels liés au réseau étendu et de signaler et d'enregistrer tous les incidents?
05D03-02	Y a-t-il un système support de la gestion des incidents?
05D03-03	Ce système centralise-t-il et prend-il en compte aussi bien les incidents détectés par l'exploitation que ceux signalés par les utilisateurs?
05D03-04	Ce système permet-il un suivi et une relance automatiques des actions nécessaires?
05D03-05	Ce système incorpore-t-il une typologie des incidents avec élaboration de statistiques et de tableau de bord des incidents à destination du RSSI?
05D03-06	Le système de gestion d'incidents est-il strictement contrôlé vis-à-vis de toute modification illicite ou indue?
05D03-07	Chaque incident réseau majeur fait-il l'objet d'un suivi spécifique (nature et description, priorité, solutions techniques, études en cours, délai prévu de résolution, etc.)?

Service et Sous-Service	Question

7 Domaine de la sécurité des Systèmes et de leur architecture

07A Contrôle d'accès aux systèmes et applications

07A01 Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)

07A01-01	Les droits d'accès aux différentes parties du SI (applications, bases de données, systèmes, etc.) sont-ils définis par rapport à des « profils » métiers regroupant des « rôles » ou des « fonctions » dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil)? Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de ""groupe.
07A01-02	Est-il possible d'introduire, dans les règles de définition des droits (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte tels que la localisation du demandeur ou les réseaux utilisés, ou fonction des moyens employés (protocoles, chiffrement, etc.) ou de la classification des ressources accédées?
07A01-03	Les profils permettent-ils également de définir des créneaux horaires et calendaires de travail (heures début et fin de journée, week-end, vacances, etc.)?
07A01-04	Ces profils et l'attribution de droits aux différents profils ont-ils reçu l'approbation des propriétaires d'information et/ou du RSSI?
07A01-05	Les processus de définition et de gestion des droits attribués aux profils sont-ils sous contrôle strict?
07A01-06	Peut-on contrôler à tout moment la liste des profils et l'ensemble des droits attribués à chaque profil?
07A01-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des droits attribués à chaque profil et des procédures de gestion des profils?

Service et Sous-Service **Question**

07A02 Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)

07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant)?
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs?
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé?
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions?
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence)? Dans ce cas les autorisations déléguées ne doivent plus être autorisées à la personne qui les a déléguées. Cette dernière doit cependant avoir la possibilité de les reprendre, en annulant ou en suspendant la délégation.
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours?
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués?

Service et Sous-Service	Question

07A03 Authentification de l'accédant

07A03-01	Le processus de distribution ou de modification de l'authentifiant garantit-il que seul le titulaire de l'identifiant peut y avoir accès (diffusion initiale confidentielle, changement de mot de passe sous le seul contrôle de l'utilisateur, etc.)?
07A03-02	Le processus de création ou de modification d'un authentifiant vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque? Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des ""standards systèmes"", des prénoms, de l'anagramme de l'identifiant, de dates, etc. Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques utilisant des clés de chiffrement : longueur de clé suffisante, processus de génération évalué ou reconnu publiquement, etc."
07A03-03	Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité? La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce) soit à frapper un code qui change à chaque instant (carte à jeton), soit à présenter un caractère biométrique.
07A03-04	La conservation et l'utilisation par l'utilisateur (ou par des systèmes représentant l'utilisateur) ou par les systèmes cibles d'éléments de référence supports de l'authentification ainsi que leur transmission entre l'utilisateur et les systèmes cibles font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité? Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué. La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission. Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.
07A03-05	En cas de répétition de tentatives infructueuses d'authentification, existe-t-il un processus déclenchant une dévalidation automatique de l'identifiant de l'utilisateur, éventuellement du terminal lui-même, ou un ralentissement du processus d'authentification empêchant toute routine automatique de tentative de connexion?
07A03-06	La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton, etc.) permet-elle d'inhiber instantanément l'ancien authentifiant et permet-elle un contrôle effectif de l'identité du demandeur?
07A03-07	Les paramètres de l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les

	règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.
07A03-08	Les processus qui assurent l'authentification sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification (y compris des processus visant à détecter les tentatives de violation et les processus de réaction à ces tentatives de violation).

Service et Sous-Service **Question**

07A04 Filtrage des accès et gestion des associations

07A04-01	Tout accès au système requiert-il la présentation d'un identifiant reconnu par le système?
07A04-02	Tout identifiant reconnu par le système correspond-il à une personne physique unique et identifiable, directement ou indirectement? Nota : Dans le cas où une application en appelle une autre ou déclenche un appel système, il se peut que l'application ne transfère pas au système cible l'identifiant ayant initialisé la demande. Le lien entre cet appel et l'identifiant et la personne d'origine doit cependant rester possible a posteriori.
07A04-03	Tous les comptes génériques ou par défaut ont-ils été supprimés?
07A04-04	L'acceptation de l'identifiant par le système est-elle systématiquement sujette à une authentification? L'authentification systématique requiert que ce processus soit effectivement mis en œuvre pour l'ensemble des sous-systèmes (moniteur de télétraitement, SGBD, traitements par lots, etc.) et pour toutes les demandes d'accès en provenance des applications ainsi que pour toutes les voies et ports d'accès, y compris depuis des ports réservés tels que la télémaintenance éventuelle.
07A04-05	Y a-t-il une répétition de la procédure d'authentification en cours de session pour les transactions jugées sensibles?
07A04-06	Y a-t-il une dévalidation automatique de l'identifiant de l'utilisateur, en cas d'absence d'échange après un délai défini, nécessitant une nouvelle identification - authentification?
07A04-07	Y a-t-il un contrôle systématique du profil du demandeur, de son contexte et de l'adéquation de ce profil et du contexte avec l'accès demandé, en fonction de règles de contrôle d'accès formalisées?
07A04-08	Les paramètres de définition et de gestion des règles de filtrage des accès sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les paramètres de sécurité du filtrage des accès soit très limitée, qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.
07A04-09	Les processus qui assurent le filtrage des accès sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de filtrage d'accès (y compris des processus visant à détecter les tentatives de modification et les processus de réaction à ces tentatives de modification).
07A04-10	Procède-t-on à des tests périodiques de pénétration du système informatique et à des audits techniques spécialisés approfondis?

Service et Sous-Service	Question

07C Gestion et enregistrement des traces

07C01 Enregistrement des accès aux ressources sensibles

07C01-01	A-t-on procédé a une analyse spécifique des accès à journaliser et des paramètres concernant ces accès à conserver?
07C01-02	Utilise-t-on un outil ou une application de contrôle permettant de journaliser et d'enregistrer les accès aux ressources sensibles (applications, fichiers applicatifs, bases de données, etc.)?
07C01-03	Les règles spécifiant les accès à journaliser et enregistrer sont-elles formalisées et ont-elles été approuvées par les propriétaires d'information ou le RSSI?
07C01-04	Les règles spécifiant les accès à journaliser et enregistrer incluent-elles les éléments essentiels pour une investigation en cas d'anomalie? Ces règles devraient spécifier pour chaque type d'accès (système, SGBD, etc.) les éléments fondamentaux à enregistrer, par exemple l'identifiant, le service ou l'application demandée, la date et l'heure, le point d'appel s'il est connu, etc.
07C01-05	Existe-t-il un archivage (sur disque, cassette, DON, etc.) de tous ces enregistrements, conservés sur une longue période et de manière infalsifiable?
07C01-06	Les paramètres de définition et de gestion des règles d'enregistrement des *login* et applications appelées sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les paramètres de définition et de gestion des règles d'enregistrement des *login* et applications appelées soit très limitée, qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.
07C01-07	Les processus qui assurent l'enregistrement des *login* et applications appelées sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus d'enregistrement (y compris des processus visant à détecter les tentatives de modification et les processus de réaction à ces tentatives de modification).

Service et Sous-Service	Question

8 Domaine de la production informatique

08E Gestion et traitement des incidents

08E01 Détection et traitement (en temps réel) des anomalies et incidents

08E01-01	A-t-on analysé les événements ou successions d'événements pouvant être révélateurs de comportements anormaux ou d'actions illicites et a-t-on mis en place des points ou indicateurs de surveillance en conséquence?
08E01-02	Le système dispose-t-il d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur stations voisines ou sur des transactions sensibles)?
08E01-03	Existe-t-il une application capable d'analyser les diagnostics individuels d'anomalie et de déclencher une alerte à destination du personnel d'exploitation?
08E01-04	Existe-t-il, parmi le personnel d'exploitation, une équipe permanente ou sous astreinte permanente capable de réagir en cas d'alerte de la détection d'anomalie?
08E01-05	A-t-on défini, pour chaque cas d'alerte, la réaction attendue de l'équipe d'intervention et sa disponibilité est-elle suffisante pour faire face à cette attente?
08E01-06	Les paramètres définissant les alarmes sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
08E01-07	Toute inhibition du système d'alerte déclenche-t-elle une alarme auprès de l'équipe de surveillance?
08E01-08	Existe-t-il un archivage (sur disque, cassette, DON, etc.) de tous les éléments ayant permis de détecter une anomalie ou un incident?
08E01-09	Les procédures de détection d'anomalies et la disponibilité de l'équipe de surveillance font-elles l'objet d'un audit régulier?

Service et Sous-Service **Question**

08E Gestion et traitement des incidents

08E02 Surveillance, en temps différé, des traces, logs et journaux

08E02-01	A-t-on fait une analyse approfondie des événements ou successions d'événements pouvant avoir un impact sur la sécurité (connexions refusées, reconfigurations, évolutions de performances, accès à des informations ou des outils sensibles, etc.)?
08E02-02	Enregistre-t-on ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure?
08E02-03	Existe-t-il une application capable d'analyser ces enregistrements ainsi que les mesures de performances, d'en déduire des statistiques, un tableau de bord et des diagnostics d'anomalies examinés par une structure ad hoc?
08E02-04	La structure chargée d'analyser ces éléments de synthèse (ou éventuellement les journaux des incidents, et événements liés à la sécurité) a-t-elle l'obligation de le faire à période fixe et déterminée et a-t-elle la disponibilité suffisante?
08E02-05	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe de surveillance et sa disponibilité est-elle suffisante pour faire face à cette attente?
08E02-06	Les paramètres définissant les éléments à enregistrer et les synthèses effectuées sur ces éléments sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
08E02-07	Toute inhibition du système d'enregistrement et de traitement des enregistrements déclenche-t-elle une alarme auprès de l'équipe de surveillance?
08E02-08	Les enregistrements ou les synthèses sont-ils conservés sur une longue durée?
08E02-09	Les procédures d'enregistrement, de traitement des enregistrements et d'analyse des synthèses ainsi que la disponibilité de l'équipe d'analyse et d'intervention font-elles l'objet d'un audit régulier?

Service et Sous-Service	Question

08E03 Gestion et traitement des incidents systèmes et applicatifs

08E03-01	Y a-t-il une équipe (hot line) accessible en permanence, chargée de recueillir les appels et de signaler et d'enregistrer tous les incidents?
08E03-02	Y a-t-il un système support de la gestion des incidents?
08E03-03	Ce système centralise-t-il et prend-il en compte aussi bien les incidents détectés par l'exploitation que ceux signalés par les utilisateurs?
08E03-04	Ce système permet-il un suivi et une relance automatiques des actions nécessaires?
08E03-05	Ce système incorpore-t-il une typologie des incidents avec élaboration de statistiques et de tableau de bord des incidents à destination du RSSI?
08E03-06	Le système de gestion d'incidents est-il strictement contrôlé vis-à-vis de toute modification illicite ou indue? Un contrôle strict requiert une protection renforcée pour pouvoir modifier un enregistrement et un audit de toute modification des enregistrements ou un contrôle par scellement électronique de toute modification.
08E03-07	Chaque incident système ou applicatif majeur fait-il l'objet d'un suivi spécifique (nature et description, priorité, solutions techniques, études en cours, délai prévu de résolution, etc.)?

Service et Sous-Service	Question

9 Domaine de la Sécurité applicative

09A Contrôle d'accès applicatif

09A01 Gestion des profils d'accès aux données applicatives

09A01-01	Les droits d'accès aux différentes applications et données applicatives sont-elles définies par rapport à des « profils » métiers regroupant des « rôles » ou des « fonctions » dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil)? Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de « groupe ».
09A01-02	Est-il possible d'introduire, dans les règles de définition des droits (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte tels que la localisation du demandeur ou les réseaux utilisés, ou fonction des moyens employés (protocoles, chiffrement, etc.) ou de la classification des ressources accédées?
09A01-03	Les profils permettent-ils également de définir des créneaux horaires et calendaires de travail (heures début et fin de journée, week-end, vacances, etc.)?
09A01-04	Ces profils et l'attribution de droits aux différents profils ont-ils reçu l'approbation des propriétaires d'information et/ou du RSSI?
09A01-05	Les processus de définition et de gestion des droits attribués aux profils sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les droits attribués aux profils soit très limitée, que la matérialisation de ces droits (sous forme de tables par exemple) soit strictement sécurisée et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.
09A01-06	Peut-on contrôler à tout moment la liste des profils et l'ensemble des droits attribués à chaque profil?
09A01-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des droits attribués à chaque profil et des procédures de gestion des profils?

Service et Sous-Service	Question

09A02 Gestion des autorisations d'accès aux données applicatives (attribution, délégation, retrait)

09A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant)?
09A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs?
09A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé? Un contrôle strict requiert une reconnaissance formelle de la signature (électronique ou non) du demandeur, que la matérialisation des profils attribués aux utilisateurs sous forme de tables soit strictement sécurisée et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.
09A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions?
09A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence)? Dans ce cas les droits délégués ne doivent plus être autorisés à la personne qui les a délégués. Cette dernière doit cependant avoir la possibilité de les reprendre, en annulant ou en suspendant la délégation.
09A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours?
09A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués au personnel et des procédures de gestion des profils attribués?

Service et Sous-Service **Question**

09D Disponibilité des données

09D01 Enregistrement de Très Haute Sécurité

09D01-01	A-t-on pris en compte la possibilité de destruction de toute information sur support informatique et en a-t-on déduit des procédures qui pourraient servir à la reconstitution à partir d'originaux?
09D01-02	A-t-on recensé pour chaque fichier les moyens non informatiques permettant de reconstituer les informations?
09D01-03	A-t-on sécurisé ces moyens (doubles d'archives, protection renforcée, etc.) contre une destruction accidentelle ou malveillante?
09D01-04	A-t-on analysé les conséquences d'une entrée faussée de données découverte tardivement ou d'une altération des processus de traitement et a-t-on mis en place, en conséquence, des moyens permettant de reconstituer après traitements les données d'origine et permettant ainsi de corriger les données altérées (ex. : journaux avant, après la mise à jour d'une donnée critique)?
09D01-05	La durée de reconstitution des données est-elle totalement compatible avec les besoins des utilisateurs?
09D01-06	Audite-t-on, de manière impromptue, que ces moyens sont effectivement mis en place et que les procédures sont bien respectées?

Service et Sous-Service	Question

09G Détection et gestion des incidents et anomalies applicatifs

09G01 Détection des anomalies applicatives

09G01-01	A-t-on analysé les événements ou successions d'événements pouvant être révélateurs de comportements anormaux ou d'actions illicites et en a-t-on déduit des points ou indicateurs de surveillance?
09G01-02	Dans les applications, est-il prévu des capteurs d'événements sensibles et l'enregistrement de ces événements (type d'événement, identifiant de l'utilisateur, date et heure, etc.)?
09G01-03	Existe-t-il un système de pistage intégré dans certains processus sensibles (audit-trail) enregistrant les événements pouvant servir à établir des diagnostics d'anomalies?
09G01-04	Les applications sensibles disposent-elles d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur des stations voisines ou tentatives infructueuses de transactions sensibles)?
09G01-05	Existe-t-il un archivage de tous ces éléments de diagnostic?
09G01-06	Existe-t-il une application capable d'analyser les diagnostics individuels enregistrés et donnant lieu à un tableau de bord transmis à une structure ad hoc?
09G01-07	Le système de diagnostic d'anomalie émet-il une alarme en temps réel à une structure permanente ou placée sous astreinte, chargée et capable de réagir sans délai?
09G01-08	A-t-on défini pour chaque cas d'alerte, la réaction attendue de l'équipe de surveillance et sa disponibilité est-elle suffisante pour faire face à cette attente?
09G01-09	Les paramètres définissant les éléments à enregistrer et les analyses de diagnostic effectuées sur ces éléments sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite?
09G01-10	Toute inhibition du système d'enregistrement et de traitement des enregistrements déclenche-t-elle une alarme auprès de l'équipe de surveillance?
09G01-11	Les procédures d'enregistrement, de traitement des enregistrements et d'analyse des diagnostics ainsi que la disponibilité de l'équipe d'analyse et d'intervention font-elles l'objet d'un audit régulier?

Service et Sous-Service	Question

10 Domaine de la sécurité des projets et développements applicatifs

10A Respect de la législation concernant les relations avec le personnel et avec les tiers

10A03 Protection de la confidentialité des développements applicatifs

10A03-01	Les procédures de développement imposent-elles une analyse de la confidentialité des applications développées et une classification des objets mis en œuvre au cours des développements (documentation, code source, code objet, notes d'étude, etc.)?
10A03-02	En cas de développement portant sur une application confidentielle, existe-t-il des procédures particulières de gestion de la documentation?
10A03-03	En cas de développement portant sur une application confidentielle, a-t-on mis en place des profils permettant de limiter la diffusion d'information confidentielle aux seules personnes en ayant réellement besoin?
10A03-04	Les codes sources, objets et la documentation font-ils l'objet d'une procédure de gestion d'accès stricte précisant, en fonction des phases de développement, les profils ayant accès à ces éléments ainsi que les conditions de stockage et de contrôle d'accès correspondantes? Une procédure et des conditions de gestion d'accès strictes doivent permettre de garantir que tout accès au code ou à la documentation est fait par une personne autorisée dans des conditions autorisées.
10A03-05	Les paramètres de contrôle de la gestion des droits attribués au personnel de développement sont-ils sous contrôle strict? Un contrôle strict requiert que la liste des personnes habilitées à changer les profils par projets attribués au personnel de développement et les paramètres de contrôle d'accès aux environnements et objets de développement soit très limitée, qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.
10A03-06	Les processus qui assurent le filtrage des accès aux objets de développement (documentation et codes) sont-ils sous contrôle strict? Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de filtrage d'accès (y compris des processus visant à détecter les tentatives de modification et les processus de réaction à ces tentatives de modification).
10A03-07	En cas de développements confiés à des SSII et de progiciels, les conditions ci-dessus sont-elles imposées contractuellement à l'éditeur, au partenaire ou au sous-traitant?
10A03-08	La gestion des droits d'accès aux objets de développement et les procédures et mécanismes de protection font-ils régulièrement l'objet d'un audit?

Service et Sous-Service **Question**

11 Domaine environnement de travail

11C Protection des postes de travail

11C01 Contrôle d’accès au poste de travail

11C01-01	L'accès au poste de travail en lui-même (hors connexion au réseau) est-il protégé par un mot de passe ou un système d'authentification?
11C01-02	Le processus de création ou de modification de l'authentifiant vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque? Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des ""standards systèmes"", des prénoms, de l'anagramme de l'identifiant, de dates, etc. Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques utilisant des clés de chiffrement : longueur de clé suffisante, processus de génération évalué ou reconnu publiquement, etc.
11C01-03	Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité? La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce), soit à présenter un caractère biométrique.
11C01-04	Le processus d'authentification est-il permanent (carte à puce) ou doit-il être réinitialisé après une courte période d'inactivité?
11C01-05	Le poste de travail est-il protégé contre toute introduction de logiciel par d'autres personnes que les administrateurs du poste?
11C01-06	L'inhibition du service de contrôle d'accès au poste est-elle détectée dynamiquement lors de la connexion au réseau d'entreprise ou, à défaut, régulièrement auditée?

Service et Sous-Service **Question**

11C02 Protection de la confidentialité des données contenues dans le poste de travail ou sur un serveur de données (disque logique pour le poste de travail)

11C02-01	Les données sensibles contenues éventuellement sur le poste de travail ou sur un disque logique de données partagées hébergé sur un serveur de données sont-elles chiffrées?
11C02-02	Les éléments du processus de chiffrement sont-ils fortement protégés contre toute altération, modification ou inhibition?
11C02-03	Les postes de travail sont-ils équipés d'un système d'effacement empêchant effectivement de relire toute donnée effacée sur le disque local ou sur un disque partagé?
11C02-04	Le poste de travail est-il équipé d'un système d'effacement réel et efficace des fichiers temporaires créés sur le disque local ou sur un disque partagé?
11C02-05	Le processus ou les directives concernant le chiffrement des fichiers s'étend-il aux messages, aux pièces jointes des messages et aux adresses de messagerie?
11C02-06	Les utilisateurs ont-ils reçu une formation à l'utilisation des moyens de chiffrement et d'effacement des informations à supprimer, leur indiquant, en particulier, les conditions à respecter pour que ce chiffrement ne puisse être contourné?
11C02-07	Procède-t-on à des audits réguliers de l'utilisation des moyens de chiffrement et d'effacement par les utilisateurs?

Service et Sous-Service **Question**

12 Domaine juridique et réglementaire

12A Respect de la législation concernant les relations avec le personnel et avec les tiers

12A01 Respect de la législation extérieure et de la législation concernant la protection de la vie privée

12A01-01	Existe-t-il un recueil regroupant l'ensemble des dispositions légales ou réglementaires liées au système d'information et à la protection de la vie privée des personnes et des données nominatives, applicables à l'entreprise ou à l'organisme?
12A01-02	Ces règles précisent-elles la conduite à tenir en ce qui concerne la correspondance privée, les messages électroniques personnels et les communications personnelles reçues ou émises par le personnel avec des ressources appartenant à l'entreprise?
12A01-03	Les règles concernant les dispositions légales ou réglementaires liées au système d'information et au respect de la vie privée sont-elles rendues facilement accessibles à l'ensemble du personnel (Intranet, par exemple)?
12A01-04	Le document concernant les dispositions légales liées au système d'information et à la protection de la vie privée, s'il existe, fait-il l'objet d'une procédure régulière de mise à jour avec validation par un juriste?

11. Scénarios de risques

Scénario 1 Collecte non nécessaire

12 – Non-conformité à la législation et à la réglementation
30 Réglementation des renseignements personnels
31 Collecte non nécessaire

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP
	01E13	PRP – Organisation de la gestion de la PRP – Exigences relatives à l'engagement du personnel
	01E14	PRP – Organisation de la gestion de la PRP – Exigences relatives au personnel en emploi

Évaluation **MIN (01E01; 01E02; 01E13; 01E14)**

Type	Numéro du sous-service	Libellé
Dissuasion	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (01E01; 12A01)**

Scénario 1

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

31 Collecte non nécessaire

Type	Numéro du sous-service	Libellé
Prévention	01E03	PRP – Organisation de la gestion de la PRP – PRP – Procédure préalable à la collecte
	01E04	PRP – Organisation de la gestion de la PRP – Procédure de collecte des informations visées par les dispositions légales en matière de PRP
	01E05	PRP – Organisation de la gestion de la PRP – Inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP
	08C08	Gestion des supports de données et de programmes – PRP – Processus de conservation, d'archivage et de destruction de renseignements personnels
	10C01	PRP – Gestion de la PRP dans les projets liés aux technologies de l'information – Prise en considération des exigences en matière de PRP dans les méthodes de développement

Évaluation **MIN (01E03; 01E04; 01E05; 08C08; 10C01)**

Type	Numéro du sous-service	Libellé
Protection	01E03	PRP – Organisation de la gestion de la PRP – PRP – Procédure préalable à la collecte
	01E04	PRP – Organisation de la gestion de la PRP – Procédure de collecte des informations visées par les dispositions légales en matière de PRP
	01E05	PRP – Organisation de la gestion de la PRP – Inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP
	08E04	Gestion et traitement des incidents - PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP

Évaluation **MIN (01E03; 01E04; 01E05; 08E04)**

Scénario 1

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

31 Collecte non nécessaire

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurances – Assurance des dommages immatériels

Évaluation **01D02**

Scénario 2 Communication non autorisée

12 – Poursuite judiciaire
30 Réglementation des renseignements personnels
32 Communication non autorisée

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C01	Engagement du personnel, clauses contractuelles
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP
	01E13	PRP – Organisation de la gestion de la PRP – Exigences relatives à l'engagement du personnel
	01E14	PRP – Organisation de la gestion de la PRP – Exigences relatives au personnel en emploi

Évaluation **MIN (01C01; 01E01; 01E02; 01E13; 01E14)**

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et des instances dirigeantes
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (01B01; 01E01; 12A01)**

Scénario 2

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

32 Communication non autorisée

Type	Numéro du sous-service	Libellé
Prévention	01E06	PRP – Procédures de communication des informations visées par les dispositions légales en matière de PRP
	01E07	PRP – Consentement à la communication
	01E08	PRP – Authentification de l'identité des personnes autorisées à prendre connaissance d'un renseignement personnel
	01E13	PRP – Exigences relatives à l'engagement du personnel
	01E14	PRP – Exigences relatives au personnel en emploi
	01E15	PRP – Gestion des relations avec les fournisseurs
	08C07	PRP – Contrôle de la diffusion des médias (imprimés, disquette, CD, etc.) contenant des informations visées par les lois sur la PRP
	09A01	Gestion des profils d'accès aux données applicatives
	09A02	Gestion des autorisations d'accès aux données applicatives (attribution, délégation et retrait)
	10C01	PRP– Gestion de la PRP dans les projets liés aux technologies de l'information – Prise en considération des exigences en matière de PRP dans le développement et la gestion de projet

Évaluation **MIN (MAX (09A01; 09A02); 01E06; 01E07; 01E08; 01E13; 01E14; 01E15; 08C07; 10C01)**

Scénario 2 :

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

32 Communication non autorisée

Type	Numéro du sous-service	Libellé
Protection	01E06	PRP – Organisation de la gestion de la PRP – Procédures de communication des informations visées par les lois sur la PRP
	01E07	PRP – Consentement à la communication
	01E08	PRP – Authentification de l'identité des personnes autorisées à prendre connaissance d'un renseignement personnel
	08C07	Gestion des supports de données et des programmes – PRP – Contrôle de la diffusion des supports (imprimé, disquette, CD, etc.) contenant des informations visées par les dispositions légales en matière de PRP
	08E04	Gestion et traitement des incidents – PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP
	09A01	Gestion des profils d'accès aux données applicatives
	09A02	Gestion des autorisations d'accès aux données applicatives (attribution, délégation et retrait)

Évaluation **MIN (MAX (09A01; 09A02); 01E06; 01E07; 01E08; 08C07; 08E04)**

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurances – Assurance des dommages immatériels

Évaluation **01D02**

Scénario 3 Utilisation illicite de renseignements personnels

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

33 Utilisation illicite de renseignements personnels

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C01	Engagement du personnel, clauses contractuelles
	01C04	Sensibilisation et formation à la sécurité
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP
	01E13	PRP – Organisation de la gestion de la PRP –Exigences relatives à l'engagement du personnel
	01E14	PRP – Organisation de la gestion de la PRP – Exigences relatives au personnel en emploi

Évaluation **MIN (01C01; 01C04; 01E01; 01E02; 01E13; 01E14)**

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	07C01	Enregistrement des accès aux ressources sensibles
	08E01	Détection et traitement, en temps réel, des anomalies et des incidents
	08E02	Surveillance, en temps différé, des traces, des *logs* et des journaux
	09G01	Détection des anomalies applicatives
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (MAX (08E01; 08E02; 09G01); 01B01; 01E01; 07C01; 12A01)**

Scénario 3

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

33 Utilisation illicite de renseignements personnels

Type	Numéro du sous-service	Libellé
Prévention	01E09	PRP – Utilisation des renseignements personnels anonymes
	01E10	PRP – Qualité des renseignements personnels
	01E11	PRP – Utilisation des renseignements personnels aux bonnes fins
	01E15	PRP – Gestion des relations avec les fournisseurs
	10C01	PRP – Gestion de la PRP dans les projets liés aux technologies de l'information – Prise en considération des exigences en matière de PRP dans les méthodes de développement

Évaluation **MIN (01E09; 01E10; 01E11; 01E15; 10C01)**

Type	Numéro du sous-service	Libellé
Protection	04D01	Surveillance, en temps réel, du réseau étendu
	04D02	Analyse en temps différé des traces, des *logs* et des journaux d'événements sur le réseau étendu
	04D03	Traitement des incidents du réseau étendu
	05D01	Surveillance, en temps réel, du réseau local
	05D02	Analyse en temps différé des traces, des *logs* et des journaux d'événements sur le réseau local
	05D03	Traitement des incidents du réseau local
	08E01	Détection et traitement, en temps réel, des anomalies et des incidents
	08E02	Surveillance, en temps différé, des traces, des *logs* et des journaux
	08E04	Gestion et traitement des incidents – PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP

Évaluation **MIN (MAX (08E01; 08E02); 04D01; 04D02; 04D03; 05D01; 05D02; 05D03; 08E04)**

Scénario 3

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

33 Utilisation illicite de renseignements personnels

Type	Numéro du sous-service	Libellé
Palliative	Aucune mesure de ce type	

Type	Numéro du sous-service	Libellé
Récupération	Aucune mesure de ce type	

Scénario 4 Accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire)

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

34 Accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire)

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C01	Engagement du personnel, clauses contractuelles
	01C04	Sensibilisation et formation à la sécurité
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP
	01E13	PRP – Organisation de la gestion de la PRP – Exigences relatives à l'engagement du personnel
	01E14	PRP – Organisation de la gestion de la PRP – Exigences relatives au personnel en emploi

Évaluation **MIN (01C01; 01C04; 01E01; 01E02; 01E13; 01E14)**

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et du management
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	07C01	Enregistrement des accès aux ressources sensibles
	08E01	Détection et traitement, en temps réel, des anomalies et des incidents
	08E02	Surveillance, en temps différé, des traces, des *logs* et des journaux
	09G01	Détection des anomalies applicatives
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (MAX (08E01; 08E02; 09G01); 01B01; 01E01; 07C01; 12A01)**

Scénario 4

30 Réglementation des renseignements personnels

34 Accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire)

Type	Numéro du sous-service	Libellé
Prévention	01E15	PRP – Gestion des relations avec les fournisseurs
	07A01	Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)
	07A02	Gestion des autorisations d'accès et des privilèges (attribution, délégation et retrait)
	07A05	PRP – Contrôle d'accès aux renseignements personnels
	09A01	Gestion des profils d'accès aux données applicatives
	09A02	Gestion des autorisations d'accès aux données applicatives (attribution, délégation et retrait)
	10A03	Protection de la confidentialité des développements applicatifs
	11C02	Protection de la confidentialité des données contenues dans le poste de travail ou sur un serveur de données

Évaluation **MIN (MAX (07A01; 07A02; 07A05; 09A01; 09A02; 10A03; 11C02); 01E15; 10A03; 11C02)**

Type	Numéro du sous-service	Libellé
Protection	08E01	Détection et traitement, en temps réel, des anomalies et des incidents
	08E02	Surveillance, en temps différé, des traces, des *logs* et des journaux
	08E03	Gestion et traitement des incidents systèmes et applicatifs
	08E04	Gestion et traitement des incidents – PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP

Évaluation **MIN (08E01; 08E02; 08E03; 08E04)**

Scénario 4

30 Réglementation des renseignements personnels

34 Accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire)

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurance des dommages immatériels

Évaluation **01D02**

Scénario 5 Accès par une personne non autorisée (habilitation non reconnue)

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

35 Accès par une personne non autorisée (habilitation non reconnue)

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C01	Engagement du personnel, clauses contractuelles
	01C04	Sensibilisation et formation à la sécurité
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP
	01E13	PRP – Organisation de la gestion de la PRP – Exigences relatives à l'engagement du personnel
	01E14	PRP – Organisation de la gestion de la PRP – Exigences relatives au personnel en emploi

Évaluation MIN (01C01; 01C04; 01E01; 01E02; 01E13; 01E14)

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et du management
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	07C01	Enregistrement des accès aux ressources sensibles
	08E01	Détection et traitement, en temps réel, des anomalies et des incidents
	08E02	Surveillance, en temps différé, des traces, des *logs* et des journaux
	09G01	Détection des anomalies applicatives
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation MIN (MAX (08E01; 08E02;09G01); 01B01; 01E01; 07C01; 12A01)

Scénario 5

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

35 Accès par une personne non autorisée (habilitation non reconnue)

Type	Numéro du sous-service	Libellé
Prévention	04B01	Profil de sécurité des entités connectées au réseau étendu
	04B02	Authentification de l'entité accédante lors des accès entrants depuis le réseau étendu
	04B03	Authentification de l'entité accédée lors des accès sortants vers d'autres entités par le réseau étendu
	05B03	Authentification de l'accédant lors des accès au réseau local depuis un point d'accès interne
	05B04	Authentification de l'accédant lors des accès au réseau local depuis un site distant via le réseau étendu
	05B05	Authentification de l'accédant lors des accès au réseau local depuis l'extérieur
	05B06	Authentification de l'accédant lors des accès au réseau local depuis un sous-réseau WI-FI
	07A03	Authentification de l'accédant
	07A04	Filtrage des accès et gestion des associations
	07A05	PRP – Contrôle d'accès aux renseignements personnels
	10A03	Protection de la confidentialité des développements applicatifs
	11C02	Protection de la confidentialité des données contenues dans le poste de travail ou sur un serveur de données

Évaluation **MAX (MIN (04B01; 04B02; 05B03; 05B04; 05B05; 05B06); MIN (07A03; 07A04; 07A05; 10A03; 11C02)**

Scénario 5

30 Réglementation des renseignements personnels

35 Accès par une personne autorisée (habilitation reconnue), mais illégitime (accès non nécessaire)

Type	Numéro du sous-service	Libellé
Protection	08E01	Détection et traitement, en temps réel, des anomalies et des incidents
	08E02	Surveillance, en temps différé, des traces, des *logs* et des journaux
	08E03	Gestion et traitement des incidents systèmes et applicatifs
	08E04	Gestion et traitement des incidents – PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP

Évaluation **MIN (08E01; 08E02; 08E03; 08E04)**

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurance des dommages immatériels

Évaluation **01D02**

Scénario 6 Détention au-delà de la limite prévue au calendrier de conservation

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

36 Détention au-delà de la limite prévue au calendrier de conservation

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C04	Sensibilisation et formation à la sécurité
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP

Évaluation **MIN (01C04; 01E01; 01E02)**

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et du management
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (01B01; 01E01; 12A01)**

Scénario 6

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

36 Détention au-delà de la limite prévue au calendrier de conservation

Type	Numéro du sous-service	Libellé
Prévention	08C08	Gestion des supports de données et de programmes – PRP – Processus de conservation, d'archivage et de destruction des informations visées par les dispositions légales en matière de PRP
	10C01	PRP – Gestion de la PRP dans les projets liés aux technologies de l'information – Prise en considération des exigences en matière de PRP dans le développement et la gestion de projet

Évaluation **MIN (08C08; 10C01)**

Type	Numéro du sous-service	Libellé
Protection	01E05	PRP – Organisation de la gestion de la PRP – Inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP
	08E04	Gestion et traitement des incidents – PRP – Processus de gestion des incidents relatifs aux informations visées par les dispositions légales en matière de PRP

Évaluation **MIN (01E05; 08E04)**

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurance des dommages immatériels

Évaluation **01D02**

Scénario 7 Non destruction de renseignements personnels dont l'objet est accompli

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

37 Non-destruction de renseignements personnels dont l'objet est accompli

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C04	Sensibilisation et formation à la sécurité
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP

Évaluation **MIN (01C04; 01E01; 01E02)**

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et du management
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (01B01; 01E01; 12A01)**

Scénario 7

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

37 Non-destruction de renseignements personnels dont l'objet est accompli

Type	Numéro du sous-service	Libellé
Prévention	01E15	PRP – Gestion des relations avec les fournisseurs
	08C08	Gestion des supports de données et de programmes – PRP – Processus de conservation, archivage et de destruction des informations visées par les dispositions légales en matière de PRP
	09D01	PRP – Gestion de la PRP dans les projets liés aux technologies de l'information - Prise en considération des exigences en matière de PRP dans le développement et la gestion de projet

Évaluation **MIN (01E15; 08C08; 09D01)**

Type	Numéro du sous-service	Libellé
Protection	01E05	PRP – Organisation de la gestion de la PRP – Inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP
	08C07	PRP – Contrôle de la diffusion des supports (imprimé, disquette, CD, etc.)

Évaluation **MIN (01E05; 08C07)**

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurance des dommages immatériels

Évaluation **01D02**

Scénario 8 Refus d'une demande d'accès ou d'une demande de rectification concernant un renseignement personnel

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

38 Refus d'une demande d'accès ou d'une demande de rectification concernant un renseignement personnel

Type --> confidentialité
Agression --> erreur humaine

Type	Numéro du sous-service	Libellé
Structurelle	01C04	Programme de sensibilisation et de formation à la sécurité
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	01E02	PRP – Organisation de la gestion de la PRP – Programme de formation et de sensibilisation à la PRP

Évaluation **MIN (01C04; 01E01; 01E02)**

Type	Numéro du sous-service	Libellé
Dissuasion	01B01	Devoirs et responsabilités du personnel et du management
	01E01	PRP – Organisation de la gestion de la PRP – Politique relative à la PRP
	12A01	Respect de la réglementation extérieure et de la législation concernant la protection de la vie privée

Évaluation **MIN (01B01; 01E01; 12A01)**

Type	Numéro du sous-service	Libellé
Prévention	01E07	PRP – Consentement à la communication
	01E08	PRP – Authentification de l'identité des personnes autorisées à prendre connaissance d'un renseignement personnel
	01E12	PRP – Procédure relative à l'accès aux renseignements personnels et à leur rectification

Évaluation **MIN (01E07; 01E08; 01E12)**

Scénario 8

12 – Poursuite judiciaire

30 Réglementation des renseignements personnels

38 Refus d'une demande d'accès ou d'une demande de rectification concernant un renseignement personnel

Type	Numéro du sous-service	Libellé
Protection	01E05	PRP – Organisation de la gestion de la PRP – Inventaire des fichiers d'informations visées par les dispositions légales en matière de PRP
	01E07	PRP – Consentement à la communication
	01E08	PRP – Authentification de l'identité des personnes autorisées à prendre connaissance d'un renseignement personnel
	01E12	PRP – Procédure relative à l'accès aux renseignements personnels et à leur rectification

Évaluation **MIN (01E05; 01E07; 01E08; 01E12)**

Type	Numéro du sous-service	Libellé
Palliative	**Aucune mesure de ce type**	

Type	Numéro du sous-service	Libellé
Récupération	01D02	Assurance des dommages immatériels

Évaluation **01D02**

12. ANNEXES

Annexe A – Tableau des liens existant entre les mesures de protection des renseignements personnels, le modèle de pratiques en la matière et les articles de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*

Risque PRP	Modèle de pratiques PRP			Loi sur l'accès – (LCJTI)
Question	**Pratique**	**Sous-pratique**	**Bien livrable**	**Article**
01E01-01				63.2
01E01-04				63.2
01E01-08	PG 2.1	1, 2	1	
01E03-02	PS 1.2, PS 4.1, PS 4.2	Toutes	2, 18 à 20	
01E03-03	PS 1.2, PS 4.1, PS 4.2	Toutes celles des PS 4	2, 18 à 20	
01E03-04	PS 1.2, PS 4.1, PS 4.2	Toutes	2, 18 à 20	65, 76
01E03-05	PS 1.2	2	2	64
01E03-07	PS 1.3			
01F03-08	PS.1.3			
01E04-01	PS 1.2- à 1.6	Toutes	1 à 8	64
01E04-04	PS 1.6		8	65
01E04-05				63.1
01E04-06				64, 67.3
01E04-07	PS 1.3, PS 1.4	2	5 (2^{e} paragraphe)	66
01E05-01	PS 8.1	1, 2	43	76
01E05-04				76
01E05-06	PS 8.1	4, 5	44 (excluant la mise à jour)	76
01E05-07				(45)
01E06-01	PS 5.1 à-5.4	Toutes	28 à 35	60, 63.2
01E06-04	PS 5.1 à 5.4	Toutes	28 à 35	60, 63.2
01E06-05				63.1
01E06-06	PS 5.1-à 5.4	Toutes	28 à 35	62, 67.1, 67.2
01E06-07	PS 5.1à 5.4	Toutes	28 à35	59, 60
01E06-08				70.1
01E06-09	PS 5.3	2	32	67.3
01E06-12	PS 5.3	1	31 (1er paragraphe)	68, 68.1, 63.2
01E06-13	PS 5.3	1	31 (1 ^{er} paragraphe)	70
01E06-14	PS 5.3	1	31 (1 ^{er} paragraphe)	

Risque PRP	Modèle de pratiques PRP			Loi sur l'accès – (LCJTI)
Question	**Pratique**	**Sous-pratique**	**Bien livrable**	**Article**
01E07-01	PS 5.4	1, 2, 3	34, 35	53, 59
01E07-06	PS 5.4	3	35	
01E09-01	PS 4.3	1	24, 25	
01E10-01	PS 6.2	2	39, 40	72
01E11-01	PS 1.2, PS 4.1, PS 4.2	Toutes	2, 18, 19, 20	65, 65.1, 76
01E11-05				63.1
01E11-06				67.3, 65.1
01E11-07				(24)
01E12-04	PS 2.1	1, 2, 3	9	83, 86
01E12-05				84
01E14-04				158, 163
01E15-02	PS 5.3	4	32	67.2
01E15-04	PS 5.3	2, 3, 4	32, 33	67.3
01E15-06				(26)
01E15-07				70.1
07A05-01	PS 3.1 à 3.3	Toutes	10, 11	62
07A05-04	PS 3.1, PS3.2, PS 3.3	Toutes	10, 11	62
07A05-05	PS 3.3	2	15, 16	
08C08-01	PS 6.1	1	36	
08C08-02				(20)
08C08-03	PS 7.1	1, 2	41, 42	
08C08-06				63.1,(20)
08C08-08	PS 7.1	1, 2	41, 42	67.2
08C08-09				73
08C08-11				(17)
08C08-12				(17)
08C08-13				(20)
10C01-01	PG 2.2	1 à 4	3	
10C01-02	PG 2.2	1 à 4	3	
10C01-03	Modèle PRP : p. 14 à 18. Processus reliés : p. 117 et 118. Ex. : p. 141.			
10C01-04	Modèle PRP : p. 14 à 18. Processus reliés : p. 117, 118, 126 et 127			
10C01-05	Modèle PRP : p. 14 à 18. Processus reliés : p. 117, 118, 126 et 127			
10C01-06	PG 2.2			
10C01-07	PG 2.4	1 à 3	5, 6	
10C01-08	PG 2.3		4	
10C01-09	PG 2.5	1 à 6	7, 8	
10C01-10	PG 2.8, PG 2.9	1 à 7	11, 12	

Note : Le Modèle de pratiques a été conçu avant l'adoption du projet de loi n^{o} 86 et n'a pas été mis à jour depuis. Certaines pratiques énumérées dans ce modèle peuvent ne plus être conformes avec le nouveau contexte législatif.

Annexe B – Scénarios initiaux de risques Méhari

La méthode Méhari regroupe les scénarios de risques en douze catégories ou conséquences, chacune pouvant avoir plusieurs causes (ou événements menaçants). Les scénarios de risques définis originalement dans la méthode sont énumérés ci-dessous, mais ils sont adaptés au contexte de l'administration publique québécoise.

1. Non-disponibilité passagère de ressources

   Absence de personnel

   - Absence de personnel d'exploitation (conflit social du personnel d'exploitation)
   - Départ de personnel stratégique
   - Disparition de personnel stratégique

   Accidents ou pannes mettant hors service une ou plusieurs ressources matérielles

   - Accident de nature électrique (court-circuit)
   - Accident causé par l'eau ou des liquides (fuite d'une canalisation, liquides renversés accidentellement, etc.).
   - Panne rendant indisponible un équipement du réseau
   - Panne rendant indisponible un système informatique central (serveur, imprimante, système de sauvegarde, etc.)
   - Panne rendant indisponible un système informatique central (serveur, imprimante, système de sauvegarde, etc.)
   - Panne rendant indisponible un système terminal mis à la disposition des utilisateurs (PC, imprimante, périphérique spécifique, etc.)
   - Servitude indispensable HS : arrêt de la climatisation entraînant l'arrêt des équipements informatiques (panne grave ou rupture de canalisation d'eau)
   - Accident de nature électrique externe à l'entreprise (court-circuit extérieur, coupure d'un câble, défaillance extérieure, etc.) empêchant le fonctionnement des systèmes centraux
   - Accident de nature électrique externe à l'entreprise (court-circuit extérieur, coupure d'un câble, défaillance extérieure, etc.) rendant indisponible l'environnement de travail des utilisateurs

   Bogue logiciel

   - Arrêt d'une application critique causé par un bogue d'un système ou d'un progiciel
   - Arrêt d'une application critique causé par un bogue d'un logiciel interne
   - Arrêt d'une application critique causé par un bug d'un progiciel spécifique utilisateur

Impossibilité d’assurer la maintenance

- Défaillance matérielle d'un équipement du réseau étendu impossible à résoudre par la maintenance, ou non-disponibilité du prestataire
- Défaillance matérielle d'un équipement du réseau local impossible à résoudre par la maintenance, ou non-disponibilité du prestataire
- Défaillance matérielle d'un système informatique central impossible à résoudre par la maintenance, ou non-disponibilité du prestataire
- Blocage applicatif impossible à résoudre par la maintenance, en raison de la disparition du prestataire ou du fournisseur

Vandalisme depuis l’extérieur

- Tir d'armes légères ou lancement de projectiles depuis la rue rendant indisponibles des équipements du réseau étendu
- Tir d'armes légères ou lancement de projectiles depuis la rue rendant indisponibles des équipements du réseau local
- Tir d'armes légères ou lancement de projectiles depuis la rue rendant indisponibles des systèmes informatiques centraux

Vandalisme intérieur

- Petit vandalisme sur les équipements du réseau étendu par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.)
- Petit vandalisme sur les équipements du réseau local par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.)
- Petit vandalisme sur les systèmes informatiques centraux par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.)
- Vandalisme touchant l'ensemble d'une salle informatique et télécom par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.)
- Petit vandalisme sur le câblage ou des baies de câblage du réseau étendu par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.)
- Petit vandalisme sur le câblage ou des baies de câblage du réseau local par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.)

Indisponibilité totale des locaux

- Interdiction totale d'accès aux locaux décrétée par les autorités entraînant un arrêt du réseau étendu
- Interdiction totale d'accès aux locaux décrétée par les autorités entraînant un arrêt des systèmes centraux

- Interdiction totale d'accès aux locaux décrétée par les autorités empêchant les utilisateurs d'accéder à leurs bureaux

2. Destruction d’équipements

Catastrophe naturelle ou accidentelle

- Catastrophe naturelle ou accidentelle : Chute de la foudre endommageant gravement des équipements du réseau étendu
- Catastrophe naturelle ou accidentelle : Chute de la foudre endommageant gravement des équipements du réseau local
- Catastrophe naturelle ou accidentelle : Chute de la foudre endommageant gravement des systèmes centraux

Incendie

- Accident interne (corbeille à papier, cendrier, etc.) endommageant gravement des équipements du réseau étendu
- Accident interne (corbeille à papier, cendrier, etc.) endommageant gravement des équipements du réseau local
- Accident interne (corbeille à papier, cendrier, etc.) endommageant gravement des systèmes centraux
- Accident interne (corbeille à papier, cendrier, etc.) endommageant gravement l'ensemble d'une salle d’informatique et télécom
- Court-circuit provoquant un incendie qui endommage gravement des équipements du réseau étendu
- Court-circuit provoquant un incendie qui endommage gravement des équipements du réseau local
- Court-circuit provoquant un incendie qui endommage gravement des systèmes centraux

Inondation

- Inondation causée par une canalisation percée ou crevée et rendant indisponibles des équipements du réseau étendu
- Inondation causée par une canalisation percée ou crevée et rendant indisponibles des équipements du réseau local
- Inondation causée par une canalisation percée ou crevée et rendant indisponibles des systèmes centraux
- Inondation causée par une canalisation percée ou crevée et rendant indisponible toute une salle d’informatique et télécom
- Catastrophe naturelle, telle que la crue d'une rivière, la remontée de la nappe phréatique, le débordement du réseau d'égouts ou une tornade avec destruction de la couverture, mettant hors service des équipements du réseau étendu

- Catastrophe naturelle, telle que la crue d'une rivière, la remontée de la nappe phréatique, le débordement du réseau d'égouts ou une tornade avec destruction de la couverture, mettant hors service des équipements du réseau local
- Catastrophe naturelle, telle que la crue d'une rivière, la remontée de la nappe phréatique, le débordement du réseau d'égouts ou une tornade avec destruction de la couverture, mettant hors service des systèmes centraux
- Inondation causée par l'extinction d'un incendie voisin et mettant hors service des équipements du réseau étendu
- Inondation causée par l'extinction d'un incendie voisin et mettant hors service des équipements du réseau local
- Inondation causée par l'extinction d'un incendie voisin et mettant hors service des systèmes centraux

Terrorisme ou sabotage par des agents extérieurs

- Explosifs déposés à proximité des locaux sensibles et mettant hors service des équipements du réseau étendu
- Explosifs déposés à proximité des locaux sensibles et mettant hors service des équipements du réseau local
- Explosifs déposés à proximité des locaux sensibles et mettant hors service des systèmes centraux

3. Performances dégradées

Modification d’un logiciel

- Dégradation involontaire des performances applicatives à l'occasion d'une opération de maintenance corrective ou évolutive d’un logiciel ou d’un progiciel

Modification du matériel

- Dégradation involontaire de performances, à l'occasion d'une opération de maintenance matérielle évolutive d'un équipement du réseau étendu (hors télémaintenance)
- Dégradation involontaire de performances, à l'occasion d'une opération de maintenance matérielle évolutive d'un équipement du réseau local (hors télémaintenance)
- Dégradation involontaire de performances, à l'occasion d'une opération de maintenance matérielle à la suite d'une panne d'un système central

Surutilisation accidentelle de ressources informatiques ou réseau

- Dégradation des performances du réseau étendu causée par une saturation accidentelle de ressources résultant d'un incident ou d'une panne sur un équipement du réseau

- Dégradation des performances du réseau local causée par une saturation accidentelle de ressources résultant d'un incident ou d'une panne sur un équipement du réseau
- Dégradation des performances applicatives causée par une saturation accidentelle de ressources résultant d'un incident système

Surutilisation malveillante de ressources informatiques ou réseau

- Dégradation des performances applicatives causée par la saturation répétitive malveillante de moyens informatiques par un groupe d'utilisateurs
- Dégradation de performances du réseau étendu causée par la saturation du réseau par un ver
- Dégradation de performances du réseau local causée par la saturation du réseau par un ver

4. Destruction de logiciels

Effacement de code exécutable ou de configurations

- Effacement direct de code exécutable par une personne autorisée (exploitation, support informatique, maintenance, etc.)
- Écrasement total ou pollution massive des configurations du réseau étendu par un membre du personnel autre qu'un administrateur
- Écrasement total ou pollution massive des configurations du réseau local par un membre du personnel autre qu'un administrateur
- Écrasement total ou pollution massive des configurations systèmes par un membre du personnel autre qu'un administrateur
- Écrasement total ou pollution massive des configurations applicatives par un membre du personnel autre qu'un administrateur

Écrasement accidentel d'un logiciel

- Écrasement accidentel d'un disque fixe contenant des programmes exécutables causé par une panne de matériel

Effacement accidentel d'un logiciel

- Effacement accidentel d'un logiciel exécutable causé par une erreur humaine

Vol ou effacement d'un support amovible

- Vol ou effacement d'un support amovible contenant le code source d'un logiciel dans les locaux informatiques par une personne autorisée
- Vol répété de bandes archives de programmes dans les locaux de stockage des médias par une personne non autorisée

Effacement ou destruction de logiciels ou de configurations utilisateurs

- Effacement de configurations utilisateurs par un virus
- Effacement de logiciels utilisateurs par un virus

5. Altération d’un logiciel

   Altération malveillante des fonctionnalités prévues d’une application via une bombe logique ou une porte dérobée

   - Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée, par les équipes de développement
   - Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée, par le personnel de maintenance
   - Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée, par le personnel d'exploitation
   - Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée, par un utilisateur

   Modification volontaire des fonctionnalités prévues d’une application informatique

   - Modification volontaire des fonctionnalités prévues d'une application par les équipes de développement
   - Modification volontaire des fonctionnalités prévues d'une application par la maintenance
   - Modification volontaire des fonctionnalités prévues d'une application par le personnel d'exploitation

   Modification volontaire ou accidentelle des fonctionnalités prévues d’une fonction bureautique (macro-instruction, feuille de calcul, etc.)

   - Modification malveillante des fonctions ou des macro-instructions d'un fichier bureautique (Excel, Access, etc.) par une personne ayant accès à l'espace de travail partagé où le fichier est archivé
   - Modification malveillante des fonctions ou des macro-instructions d'un fichier bureautique (Excel, Access, etc.) stocké sur le poste de travail de l'utilisateur
   - Modification accidentelle ou malencontreuse des fonctions ou des macro-instructions d'un fichier bureautique (Excel, Access, etc.) par un utilisateur d'un fichier partagé

6. Altération de données

   Accident de traitement

   - Accident d'exploitation
   - Altération accidentelle des données pendant la maintenance

- Altération accidentelle des données pendant une opération de maintenance à chaud

Erreur de saisie

- Erreur pendant le processus de saisie

7. Manipulation de données

Données applicatives faussées pendant la transmission

- Données applicatives faussées pendant la transmission sur le réseau étendu par un pirate agissant de l'extérieur
- Données applicatives faussées pendant la transmission par un membre du personnel manipulant un équipement de réseau local
- Données applicatives faussées pendant la transmission par un membre du personnel branchant un équipement parasite en coupure sur le réseau local (*man in the middle*)
- Données applicatives faussées pendant la transmission entre un utilisateur nomade et le réseau interne

Rejeu de transaction

- Rejeu de transaction

Saisie faussée de données

- Saisie faussée de données par un agent autorisé, mais déloyal
- Saisie faussée de données par un membre du personnel usurpant l'identité d'un utilisateur autorisé

Substitution volontaire de supports

- Substitution volontaire de supports de données par un tiers non autorisé
- Substitution volontaire de supports de données par une personne autorisée (légitimement)

Manipulation de fichiers

- Manipulation de fichiers de données par un tiers non autorisé usurpant l'autorité d'un utilisateur autorisé
- Manipulation de fichiers de données par un membre du personnel autorisé illégitime

Falsification de messages

- Faux messages écrits par un membre du personnel usurpant l'identité d'une personne accréditée avec falsification de signature
- Messages faussés pendant la transmission entre un utilisateur nomade et le réseau interne
- Faux messages transmis par l'utilisation d'un faux site ou serveur simulant un site ou serveur à l'interne

8. Divulgation de données ou d'informations

Accès au système et consultation

- Accès au système et consultation en ligne par un pirate qui, de l'extérieur, se connecte sur un port ouvert du réseau étendu
- Accès au système et consultation en ligne par un tiers autorisé à pénétrer dans les locaux et ayant un accès physique au réseau local interne (prise LAN dans une salle de réunion)
- Accès au système et consultation en ligne par un membre du personnel autorisé illégitime

Captation d'informations fugitives

- Branchement d'un équipement parasite sur le réseau local (gaines techniques) dans les locaux, par une personne autorisée à y pénétrer
- Modification distante d'un équipement de réseau, pour piéger les messages échangés, par un utilisateur autorisé à se connecter sur le réseau interne
- Modification d'un équipement de réseau, pour piéger les messages échangés, par un administrateur réseau
- Modification d'un équipement de réseau, pour piéger les messages échangés, par un pirate qui se connecte à un équipement de réseau via une liaison de télémaintenance
- Modification d'un équipement de réseau, pour piéger les messages échangés, par un pirate qui s'y connecte en exploitant une faille connue, mais non corrigée à la suite d'une intervention ou d'une nouvelle installation
- Écoute de la connexion d'un utilisateur nomade qui, de l'extérieur, se connecte au réseau interne
- Compromission électromagnétique
- Transfert de données sensibles détournées par un pirate ayant connecté un équipement en usurpant l'identité d'une entité connectée au réseau étendu

Vol de documents écrits ou imprimés

- Vol de listages ou d'impressions pendant la phase de diffusion à l'extérieur des locaux sensibles
- Vol de listages ou d'impressions par un membre du personnel autorisé illégitimement à pénétrer dans les locaux de la production

- Vol répétitif de documents dans des bureaux par un membre du personnel ne faisant pas partie du service
- Vol répétitif de documents dans des bureaux par un ancien membre du personnel ayant conservé ses droits
- Vol de documents dans des bureaux par un visiteur
- Vol de documents dans des bureaux par un espion ayant pénétré illégalement dans les locaux
- Vol de documents dans des bureaux par une personne autorisée à y pénétrer en dehors des heures ouvrables (femmes de ménage, agents de sécurité, etc.)
- Vol de courrier sensible, dans le local du courrier, en dehors des heures ouvrables

Détournement d'informations en transit

- Détournement de télécopies par vol dans un local où est situé un télécopieur
- Détournement de télécopies par transfert de poste par un membre du personnel

Détournement d'informations temporaires
générées par les systèmes

- Détournement d'informations par un administrateur système ayant accès à des ressources utilisateurs non effacées après utilisation

9. Détournement de fichiers de données

Accès au système et copie de fichiers de données applicatives

- Copie répétée de fichiers de données applicatives par un pirate qui, de l'extérieur, se connecte sur un port ouvert du réseau étendu
- Copie répétée de fichiers de données applicatives par un pirate qui, de l'extérieur, se connecte sur un port de télémaintenance réseau
- Copie répétée de fichiers de données applicatives par une personne qui ne fait pas partie du personnel, mais qui a un accès aux locaux et la possibilité de se connecter sur le LAN
- Copie répétée de fichiers de données applicatives par un pirate qui se connecte directement sur un port de télémaintenance système
- Copie répétée de fichiers de données applicatives par un pirate qui, de l'extérieur, se connecte via un sous-réseau WiFi
- Copie ponctuelle de fichiers de données applicatives par un pirate qui se connecte via une liaison modem ouverte sur Internet à partir d'un poste utilisateur lui-même connecté au réseau interne avec des sessions ouvertes sur des serveurs autorisés
- Accès au système et copie de fichiers de données applicatives par un agent autorisé illégitime

- Accès au système et copie de fichiers de données applicatives par un membre du personnel exploitant une faille de sécurité laissée ouverte après une opération de maintenance
- Accès au système et copie de fichiers de données applicatives par un membre de l'équipe du développement via une porte dérobée placée dans une application
- Accès aux disques système et copie de fichiers de données applicatives par le personnel de maintenance à l'occasion d'une opération de maintenance
- Accès aux réseaux de stockage et lecture de fichiers de données applicatives par un serveur non autorisé

Vol de supports de données applicatives

- Vol de supports de données applicatives pendant l'exploitation par une personne autorisée à manipuler les supports
- Vol de supports de données applicatives pendant le transport
- Vol de fichiers de données applicatives dans les locaux de stockage des médias sur le site, par une personne non autorisée
- Vol de fichiers de données applicatives dans les locaux de stockage des médias hors site, par une personne non autorisée

Accès aux serveurs et copie de fichiers bureautiques

- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un pirate qui, de l'extérieur, se connecte sur un port ouvert du réseau étendu
- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un pirate qui, de l'extérieur, se connecte sur un port de télémaintenance réseau
- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par une personne ne faisant pas partie du personnel, mais qui a un accès aux locaux et la possibilité de se connecter sur le LAN
- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un pirate se connectant directement sur un port de télémaintenance système
- Copie ponctuelle de fichiers bureautiques partagés (serveur de données partagées) par un pirate se connectant via une liaison modem ouverte sur Internet à partir d'un poste utilisateur lui-même connecté au réseau interne avec des sessions ouvertes sur des serveurs
- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un membre du personnel usurpant l'identité d'une personne autorisée
- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un membre du personnel utilisant des outils de bidouilleur (*hacker*)
- Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un membre du personnel exploitant une faille de sécurité laissée ouverte après une opération de maintenance
- Copie répétée de fichiers bureautiques par un membre du personnel non autorisé sur le poste de travail

- Divulgation de fichiers bureautiques par un agent de maintenance intervenant sur un poste de travail

Détournement du code source

- Détournement du code source d'une application stratégique par un membre de l'équipe de développement

10. Perte de fichiers de données ou de documents

Effacement par bombe logique

- Effacement de fichiers de données applicatives par bombe logique introduite par un administrateur ou un ingénieur système

Effacement de supports par virus

- Effacement des fichiers bureautiques personnels, par un virus
- Effacement des fichiers bureautiques partagés, par un virus

Effacement malveillant direct de supports

- Effacement massif de fichiers d'archives de données par le personnel d’exploitation

Perte accidentelle de fichiers

- Perte accidentelle de fichiers de données applicatives par un automate
- Perte accidentelle de fichiers de données applicatives par vieillissement ou pollution

Vol de supports

- Vol de supports d'archives personnelles dans un bureau
- Vol de micro-ordinateurs portables en dehors des locaux

Perte accidentelle de documents

- Perte d'archives patrimoniales ou de documents ayant valeur de preuve à la suite d’un incendie

11. Sinistre immatériel

Effacement de fichiers par bombe logique

- Destruction ou pollution massive de fichiers de données applicatives et de leurs sauvegardes par voie logique par un ingénieur système de l'équipe d'exploitation
- Destruction ou pollution massive de fichiers programmes (codes sources) et de leurs sauvegardes par voie logique par un ingénieur système de l'équipe d'exploitation

Effacement malveillant des supports

- Effacement malveillant de l'ensemble des supports de données sensibles (supports opérationnels, sauvegardes et archives) par le personnel d'exploitation

12. Non-conformité à la législation et à la réglementation

Attaque d'une tierce société

- Attaque d'une tierce société ayant des connexions autorisées avec le ministère ou l’organisme public, par du personnel interne
- Attaque d'une tierce société n'ayant pas de connexion autorisée avec le ministère ou l’organisme public, par du personnel interne
- Attaque d'une tierce société par un pirate ayant pénétré le système d'information (rebond)

Violation des droits de propriété industrielle

- Utilisation de logiciels sans licences