Analyse de risques applicable au plan catastrophe

1. Avertissement

Les normes minimales de la Banque Carrefour de la sécurité sociale précisent que les CPAS "*doivent à l'aide d'une méthodologie commune approuvée par le groupe de travail "Sécurité de l'Information" ou de toute autre méthodologie qui tienne compte des principes de base y décrits, réaliser une analyse de risques permettant l'élaboration d'un plan de continuité*".

L'analyse de risques sert à faire un inventaire des risques présumés. Il appartient au conseiller en sécurité de les évaluer, de présenter le résultat de son analyse de risques au secrétaire et de présenter le résultat de leurs analyses conjointes au Conseil de l'Action sociale qui décidera de les assumer ou non. Cet inventaire sert de base à l'élaboration du plan trisannuel de sécurité puisque le conseiller en sécurité y inscrira les actions à entreprendre pour couvrir les risques choisis par le Conseil de l'Action sociale. Enfin, l'analyse de risque soutient également le plan de continuité ou plan catastrophe.
L'analyse de risque doit être mise à jour dès que les risques changent : nouveaux risques (nouveaux serveurs, nouvelle informatique, nouveau bâtiment, nouvelle organisation), disparition de risques (suppression de la déchiqueteuse, départ d'une vieille photocopieuse, etc.).

Attention : le fait que l'analyse de risques montre que X risques nécessitent d'être réduits ne veut pas dire que ces X risques doivent être traités en un an. Les risques prioritaires seront pris en considération et compensés dès que possible. Les autres risques sont à inscrire dans le plan de sécurité trisannuel.

L'analyse ne doit ni être envoyée au SPP IS ni au Comité sectoriel de la sécurité sociale. Elle reste la propriété du CPAS qui aura le loisir de la montrer en cas d'audit.
Ce document n'est pas le même que le questionnaire annuel envoyé par le SPP IS au nom du Comité sectoriel de la sécurité sociale.

Le questionnaire annuel est destiné à permettre au Comité sectoriel de la sécurité sociale d'évaluer l'évolution de l'application des normes minimales au sein des CPAS.

L'analyse de risques proposée ici n'a pas valeur de contrainte. Chaque conseiller en sécurité de CPAS est libre de choisir sa méthodologie pour autant qu'elle réponde à la norme minimale. Le but de l'analyse proposée ici est de mettre à disposition des CPAS une méthodologie simple dans son concept et facile à appliquer. Cette méthodologie a été revue et agréée par la Banque Carrefour de la sécurité sociale.

2. Caractéristiques de la méthodologie proposée.

Cette méthodologie a les particularités suivantes: elle n'est pas complète au sens technique du terme mais elle est suffisante pour les CPAS puisqu'elle limite sa portée aux données à caractère social conservées soit sous format papier soit sous format logique (informatique).
L'analyse est réduite aux services manipulant les données à caractère social transitant par la BCSS:

- le RIS,
- la loi 65,
- la comptabilité (même si les données de la comptabilité ne sont pas des données transitant par la BCSS, les données sociales issues du logiciel social pour l'obtention du RIS y sont intégrées),
- autres activités impliquant la manipulation et la conservation de données à caractère social,

La simplicité et l'aspect pratique sont visés puisque l'analyse de risques précède le plan catastrophe ou de continuité et aide à le réaliser. Elle repose sur les principes des normes minimales de sécurité de la BCSS et sur les principes de sécurité de base : confidentialité, intégrité, disponibilité, auditabilité (possibilité de vérifier l'existence ou non d'une chose, d'un événement).

Compte tenu que chaque CPAS a sa propre organisation en matière de gestion des RIS, de loi 65 et d'autres tâches légales, aucune liste d'activité n'a été élaborée. Il appartient à chaque conseiller en sécurité d'appliquer les principes énoncés ci-dessus, pour rappel, les risques liés aux accès aux données à caractère social.

3. A qui s'adresse cette analyse de risques ?

Cette analyse de risques s'adresse aux conseillers et conseillères en sécurité qui la réaliseront en collaboration avec leur secrétaire. Elle sera ensuite soumise à l'approbation du conseil de l'action sociale.

4. Principe de l'analyse de risques.

Le principe de l'analyse de risques est de déterminer les services du CPAS susceptibles d'être les plus touchés ou impactés[1] par une catastrophe ou un incident ayant des répercussions sur eux. Le but de cette analyse est de pouvoir anticiper les conséquences des risques évalués par le conseiller en sécurité, le secrétaire – le Président – les informaticiens et les responsables de services en prévoyant des actions correctives si le risque n'est pas supportable.

Voyons un exemple concret pour illustrer ce principe.
Si le risque d'une inondation est bien réel pour un CPAS et que les dégâts créés par cette inondation empêcheront le CPAS d'accomplir ses tâches légales pendant 3 semaines, le CPAS peut avoir **trois** réactions :

1. le risque est **acceptable** et aucune action n'est prise,
2. le risque n'est pas acceptable **pour certains services** et le CPAS prend les mesures dès aujourd'hui pour lui permettre de redémarrer ses activités clef endéans la période qu'il se fixe (24h, 48h, 72h ou plus),

[1] Services impactés: services ayant subi ou susceptibles de subir des conséquences sur leur fonctionnement.

3. le CPAS estime que ce risque **n'est pas tolérable pour l'ensemble de ses services** et prévoit de pouvoir recommencer toutes ses activités endéans la période qu'il se fixe (24h, 48h, 72h ou plus).

Il va de soi que le conseiller en sécurité peut éventuellement déjà disposer de certains outils: inventaire des besoins pour redémarrer (local, mobilier, informatique, connexions), politique de sécurité, assistance extérieure, back-ups réalisés et conservés par une société en dehors du CPAS, etc.

5. Qu'est-ce qu'un risque et qu'est-ce qu'un risque supportable?

a) Le risque.

Un risque est la probabilité qu'un danger survienne et ne commette des dégâts empêchant le CPAS de fonctionner partiellement ou totalement.

Certains risques sont connus, d'autres moins. Il ne faut toutefois ni surestimer ni sous-estimer leur survenance. A cet égard, le conseiller en sécurité peut obtenir des informations auprès :

- de la police pour les risques de vol, d'agression, de vandalisme ou autre,
- des compagnies d'assurance qui disposent de statistiques et d'informations utiles en matière d'incendie, d'inondation, d'agression ou autre,
- de l'IRM (Institut royal météorologique) qui connaît les zones à risque d'inondation,
- de certaines associations professionnelles pour les risques informatiques (CLUSIB, SANS, …).

Il découle de tout ceci que le risque zéro n'existe pas. S'il n'y a pas eu de vol dans la région depuis 4 ans, cela ne signifie naturellement pas qu'aucun vol n'aura lieu dans le CPAS, a fortiori si aucune précaution n'est prise.

b) Le risque supportable.

Un risque supportable est un risque que le CPAS peut se permettre d'assumer sans prendre de mesure de sécurité spécifique.

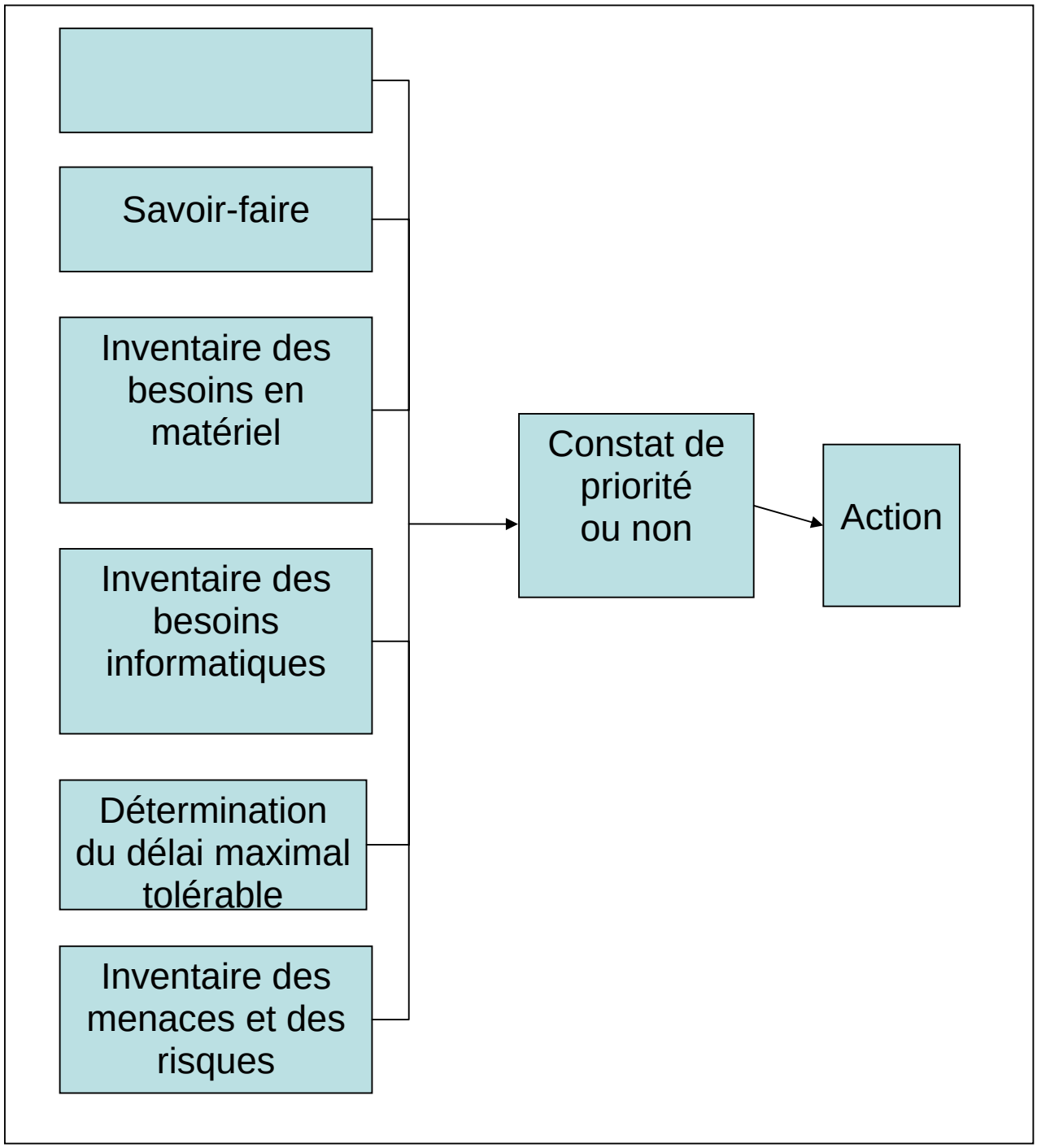
Exemple : si le CPAS considère que la perte de son serveur est un risque supportable, c'est qu'il pense pouvoir le remplacer et le reconfigurer rapidement sans aucune gêne dépassant ses estimations (24h, 48h, 72h ou plus) pour le bon fonctionnement de ses services.

Pour mesurer les risques et l'importance à leur accorder, une méthodologie relativement simple peut être appliquée.

1. Les activités d'un CPAS sont multiples et diverses. Elles sont à la base de la raison d'être du CPAS et de son fonctionnement.
2 Exécuter ces activités nécessite, par conséquent, du savoir, du personnel et du matériel.
3. Accomplir ces activités implique de travailler avec de l'informatique.
4. Le conseiller en sécurité en collaboration avec le secrétaire/Président et éventuellement d'autres personnes (informaticien, conseillers, etc.) détermineront la durée maximale tolérable d'indisponibilité, c'est-à-dire le temps maximum pendant lequel le CPAS, le service, la cellule ou certains membres du personnel pourront rester sans travailler. Ils proposeront cette durée maximale tolérable d'indisponibilité au Conseil de l'Action Sociale et/ou au Bureau Permanent. Le Conseil de l'Action Sociale ou le Bureau Permanent décidera.
5. Enfin, ces activités ne sont pas toutes susceptibles de subir le même risque. Une médiation de dettes sera éventuellement une activité moins risquée et moins prioritaire qu'une allocation de revenu d'intégration social.
6. Les services d'un CPAS n'ont pas tous la même priorité. Il appartient au Conseil de l'Action Sociale et/ou au Bureau Permanent de déterminer la priorité de redémarrage.
7. La conclusion de l'analyse de risque devra permettre de déclencher des actions correctives destinées à permettre au CPAS de continuer à prester ses services dans les délais prévus.

Sur base de cette étude, le conseiller en sécurité pourra développer des priorités d'action qu'il intégrera dans son plan de sécurité trisannuel.

6. LOGIQUE DE L'ANALYSE DE RISQUE



Les services

6A. Les services

Tous les CPAS de Belgique ont les mêmes buts mais s'organisent de façon différente suivant leurs capacités et leurs besoins. Les activités ne seront donc pas abordées mais bien les services, même si le service se réduit à un e personne dans certains CPAS ou que cette personne réalise les activités de plusieurs services à la fois.

Voici quelques exemples de services :

- service RIS,
- service de médiation de dette,
- service d'aide familiale,
- autres…

Ces services n'ont pas tous la même importance ni urgence mais ils ont tous le même objectif: aider les personnes qui en ont fait la demande.

Savoir-faire

6B. Le savoir-faire.

Le savoir-faire des assistants sociaux, des agents administratifs et du personnel dans son ensemble joue naturellement un rôle essentiel : traiter, gérer et exécuter les missions mais aussi évaluer les problèmes tant dans leur travail quotidien que dans la reprise des activités et dans l'évaluation des risques.

Ainsi, une activité prioritaire peut émerger. Supposons que veiller à payer les bénéficiaires des RIS à heure et à date fixe reçoive la priorité n°1. Dans ce cas-là, le CPAS veillera à apporter toute l'attention nécessaire à l'accomplissement de cette activité, quel que soit l'état de fonctionnement du CPAS. En cas de catastrophe, le Conseil de l'Action sociale peut naturellement décider de

s’accorder un jour, deux jours, voire trois jours ou plus pour redevenir opérationnel et payer les bénéficiaires.

Le conseiller en sécurité effectuera donc l’inventaire des activités par service avec l’aide du responsable pour n’oublier aucun élément nécessaire au bon fonctionnement du service.

Les risques seront également examinés par le chef de service et le conseiller en sécurité et des propositions communes de réductions de risque seront rédigées.

Inventaire des besoins en matériel

6C. L’inventaire des besoins en matériel.

Ce qui est valable pour les activités des services l’est aussi pour les besoins de fonctionnement.

Si malgré le fait que les risques aient pu être limités, une catastrophe survenait, il faudrait pouvoir redémarrer. Réaliser un inventaire facilite par ailleurs la compréhension de certains risques : état de l’installation électrique, état des murs et des sols, fissures, exposition au vol, entretien des extincteurs, etc.

On fera donc un inventaire du matériel nécessaire pour le ou les services qui devront redémarrer et un inventaire informatique.

Exemple : pour accomplir l’activité X, voici l’inventaire :

- inventaire physique : une chaise, un bureau, un téléphone, des documents standards pour faire des demandes à l’administration fédérale, un fax, etc.
- inventaire informatique : un clavier, une souris, un écran, un PC, un Windows XP avec Word, Excel, programme XXX qui permet de calculer les dettes de Mr Y, etc., un modem, un hub, 2 switchs, un antivirus, un parefeu, un back up,…

Détermination du délai maximal tolérable

6D. Détermination du délai maximal tolérable

Imaginons une durée maximale d'interruption de fonctionnement d'un service admise et fixée par l'autorité responsable (Conseil de l'action sociale ou le Bureau Permanent) d'**X** jours.

Cette procédure de détermination de durée doit être répétée pour tous les services exécutés par le CPAS dans le cadre du traitement des données sociales transitant par la Banque Carrefour de la Sécurité sociale et des activités prioritaires.

Exemples : service RIS : 72 h ou 3 jours,
service de médiation de dette : 120 h ou 5 jours,
service d'aide familiale : 96 h ou 4 jours.

Les points communs à ces diverses activités seront ensuite rassemblés et examinés pour préparer une réponse adéquate en prévoyant les moyens à mettre en place pour redémarrer et alimenter le plan catastrophe qui sera établi plus tard sur base des priorités ainsi dégagées.

Exemple : pour redémarrer le service RIS, le service de médiation de dettes et le service d'aide familiale,une durée de 4 jours (96h) a été accordée par le conseil de l'action sociale.

Sachant qu'il faudra :

- un ou plusieurs serveurs,
- le logiciel social,
- les back-ups,
- 5 bureaux pour 5 personnes,
- 3 lignes téléphoniques,
- 5 antivirus,
- 5 OS,
- 1 connexion Publilink,

- un programme de paiement Dexia,
- 5 chaises,
- 5 bureaux,
- 2 armoires,
- 1 fax
- etc.

Le CPAS pourra-t-il se procurer tous ces éléments endéans le délai fixé (4 jours) en fonction des risques ?

Fin de la première étape.

Le CPAS dispose maintenant :

- d'un inventaire physique,
- d'un inventaire informatique,
- d'une détermination d'un délai maximal qu'en cas de catastrophe, il devra mettre à profit pour se procurer l'ensemble des éléments inventoriés et nécessaires pour effectuer sa ou ses activités.

A ce stade, le CPAS peut déjà dresser un constat : que risque-t-il de manquer pour pouvoir effectuer les activités stratégiques ? Cette réflexion vaut pour l'instant présent. En effet, cette analyse de risque peut mettre en évidence des manques (absence de disques de secours, d'encre, d'air conditionné, etc.), des risques autres que matériels (problème de personnel, de formation, d'information, qui répare quoi ou entretient quoi ?).

Inventaire des risques

7. Inventaire des risques.

Une fois les inventaires établis, chaque service effectue des activités exposées à des menaces dont une liste est dressée ci-après. Cette liste n'est pas exhaustive car il y en a environ 250 mais chaque conseiller en sécurité pourra déterminer lui-même ce qu'il considère comme une menace propre à son CPAS. Exemple : vandalisme et incendie. A côté de ces menaces, vous trouverez les risques découlant des menaces.

Menaces	Risques
Perte de courant.	Perte de données ou d'intégrité des données (corruption des bases de donnes, par exemple, qui fait que les données ne sont plus exactes).
Erreur de manipulation intentionnelle ou non.	Perte de données, difficulté de corriger ou de réencoder les bonnes informations.
Virus, vers, troyens, malwares, spywares.	Perte d'informations, de matériel (disque dur), blocage d'accès à internet, destruction irréversible de données.
Abus.	Perte de confidentialité et diffusion d'informations non autorisée si accès abusif à des informations confidentielles.
Désastre naturel (hors incendie et tremblement de terre), inondation, tempête, affaissement, autres.	Perte de données, de matériel, d'accès aux informations, impossibilité de travailler, impossibilité d'effectuer les missions légales du CPAS.
Hacking (tentative de pénétration du réseau de l'extérieur ou de l'intérieur).	Perte de confidentialité, diffusion de données confidentielles à l'extérieur, modification des données, suppression – modification éventuelle des données, blocage des accès, publication des données sur internet, etc.
Surcharge du système informatique.	Une mauvaise utilisation du matériel (surcharge de la mémoire, mauvaise synchronisation des environnements, absence de mises à jour, absence de maintenance) peut provoquer des problèmes de fonctionnement et de sauvegarde entraînant des pertes irrémédiables de données.

Menaces	Risques
Défaillance du programme de back up.	Perte des sauvegardes des données, impossibilité de redémarrer sur des bases saines, impossibilité de vérifier l'origine des données.
Le feu.	Le feu est une menace mais les dégâts causés par l'eau aspergée pour éteindre l'incendie en est une autre. Les risques sont multiples : impossibilité de recommencer à travailler, disparition d'informations essentielles, difficulté de se procurer du nouveau matériel ou des programmes, perte financière conséquente (obligation de racheter les licences).

Le secrétaire, le conseiller en sécurité et l'informaticien (s'il y en a un) doivent examiner la liste des risques par service et les conséquences qu'ils auraient sur leur bon fonctionnement. Comment ces services pourraient-ils recommencer à travailler en fonction des dégâts subis ?

Il est à conseiller de regarder chaque menace par service et d'évaluer la probabilité[2] de sa survenance.

Exemple.
Service de paiement du RIS.
Lieu : salle du 1er étage.
Situation : bureau ancien, meubles en acier, grande concentration de papier.
Inventaire : 2 Pc, 2 imprimantes, 4 chaises, 3 armoires à classeur, 2 téléphones, 2 manuels de procédure, ….

Menace : vol.
Risque : faible car système de détection d'intrusion et pourcentage de vol faible dans la région. De plus, le public n'a pas accès aux locaux des assistants sociaux.

[2] Probabilité de survenance: risque que quelque chose arrive, exemple: la probabilité de survenance d'un accident de voiture augmente avec le nombre de kilomètres parcourus par an. Une personne qui parcourt 20.000 km /an a un risque de survenance d'accident beaucoup plus faible qu'une personne parcourant 100.000 km/an.

Menace : incendie.

Risque : élevé. Le bâtiment est ancien et contient beaucoup de bois. Personne n'a reçu de formation à la lutte contre l'incendie et les pompiers sont à 11 km. Aucun service ne pourrait recommencer à travailler.

L'ensemble des informations apportées par cette évaluation des menaces a plusieurs conséquences :

- la mise en évidence des menaces permet au CPAS d'y parer ou de tenter d'y apporter une réponse visant à diminuer le ou les risques en fonction des activités stratégiques à réaliser ;
- la mise en évidence des menaces révèle la fragilité du CPAS dans ses éventuelles tentatives de recommencer ses activités après une catastrophe,
- la nécessité de préparer un plan de sécurité à trois ans prenant en compte les faiblesses à compenser selon leur importance stratégique,
- la possibilité pour le CPAS de se préparer à affronter des incidents dont les gravités variables n'imposent pas toujours les mêmes investissements mais bien les mêmes démarches.

Constat de priorité ou non

8. Constat de priorité ou non.

En fonction de la situation propre au CPAS, en fonction de sa situation géographique, en fonction du personnel (exemple : une seule personne détient l'information), le conseiller en sécurité dresse l'inventaire des menaces et des risques qu'il revoit avec le responsable de la gestion journalière et propose des actions destinées à diminuer le ou les risques. Parmi l'ensemble de ses propositions de diminution de risques, il y a lieu de mettre en évidence une ou plusieurs priorités qui, après agréation par le Conseil de l'Action sociale, seront

réalisées dans un futur plus ou moins proche. Les autres actions visant à diminuer les risques seront inscrites dans son plan trisannuel.

Fin de la deuxième étape.

Le CPAS dispose maintenant d'un inventaire des menaces et des risques. Le conseiller en sécurité a fait valider un constat de priorité ou non. S'il y a des priorités, il les inscrit dans son planning et dans son plan de sécurité trisannuel

Action

9. Résultats – Action.

Cette analyse de risque est liée :

- d'une part aux données sociales gérées par le CPAS et transitant par la BCSS ;
- d'autre part aux besoins à compenser pour créer un plan catastrophe fiable,

Elle apporte des informations importantes et utiles autorisant le CPAS à cibler ses vulnérabilités et à les diminuer. Il vaut mieux tenter d'éviter une catastrophe que la réparer et il vaut mieux savoir comment la réparer que de ne disposer d'aucune préparation face à l'imprévisible.

Sur base de cette analyse, des actions devront être menées pour diminuer le ou les risques suivant plusieurs critères de priorité :

- l'importance du risque,
- l'importance du service pour le CPAS,
- l'importance des moyens à mettre en œuvre.

Le tableau ci-dessous a pour but d'aider le conseiller en sécurité à suivre la logique exposée ci-dessus et de lui faciliter le processus à suivre.

N'oubliez jamais que la gestion du ou des risques passe aussi par la gestion et le soutien du responsable de la gestion journalière.

G. Kempgens

Conseiller en sécurité SPP IS

Tableau d'exemples destinés à facilité la compréhension de l'analyse de risques.

Service	Menaces	Conséquences	Niveau de risques[3]	Justification	Action nécessaire pour diminuer le risque	Remplaçable / non remplaçable dans les délais fixés	Réalisé – non réalisé	Prioritaire – non prioritaire
Service : RIS. **Délai de redémarrage pour le service RIS : 3 jours ouvrables.**								
RIS	Interruption du courant électrique.	Pertes de données dans le système informatique	F	Il y a très peu de pannes de courant. De plus, le système informatique est doté d'un UPS (batterie) permettant d'empêcher la perte des données.	Disposer d'un UPS	Remplaçable rapidement.	En ordre	SO[4]
		Fragilisation du matériel informatique.	F	L'UPS agit comme stabilisateur d'alimentation électrique..	Idem	Idem	En ordre	SO

[3] F = faible, donc rien à faire, M = moyen, donc réagir en fonction du risque, E = élevé, réagir rapidement pour faire disparaître le risque.

[4] SO = sans objet puisque tout est en ordre.

Service	Menaces	Conséquences	Niveau de risques[5]	Justification	Action nécessaire pour diminuer le risque	Remplaçable / non remplaçable dans les délais fixés	Réalisé – non réalisé	Prioritaire – non prioritaire
RIS	Inondation	Destruction des données.	M	Le service informatique est situé sous un Velux. En cas de fuite, l'eau ruissellera jusqu'aux prises électriques installées dans le plancher.	Installer un détecteur d'eau relié à la centrale incendie.	Oui car les back ups sont stockés à l'extérieur.	Oui.	Non.
		Destruction du matériel informatique.			Installer un coupe circuit.	Oui car le fournisseur s'est engagé à remplacer le matériel rapidement.	Oui mais engage-ment informel.	Priorité moyenne.
		Destruction des archives.			Installer les archives soit ailleurs soit sur des étagères en hauteur.	Non car les archives sont par terre et ne peuvent pas être remplacées.	Non.	Oui.
		Destruction des supports informatiques (back up).			Les back ups de données seront sauvés mais pas ceux de la comptabilité.	Stocker tous les back ups à l'extérieur.	Non.	Oui.

[5] F = faible, donc rien à faire, M = moyen, donc réagir en fonction du risque, E = élevé, réagir rapidement pour faire disparaître le risque.

Service	Menaces	Conséquences	Niveau de risques[6]	Justification	Action nécessaire pour diminuer le risque	Remplaçable / non remplaçable dans les délais fixés	Réalisé – non réalisé	Prioritaire – non prioritaire
RIS	Mise à jour de l'antivirus	Destruction des données. Destruction éventuelle des disques durs. Blocage des accès à internet. Possibilité d'intrusion. Possibilité de vol de données.	E	Problème de mise à jour récurrent. La mise à jour ne fonctionne pas correctement et l'antivirus reste parfois une semaine sans mise à jour.	Contacter le fournisseur et arriver à obtenir des mises à jour fonctionnelles.	Non. Obligation de racheter du matériel et de réinstaller toute la configuration du serveur ainsi que les données.	Non.	Prioritaire.

Important : prendre en compte :

1 : les services qui manipulent des données à caractère social obtenues via la BCSS (RIS, loi 65, autre tel que la comptabilité);

2 : l'ensemble des services qui permettent aux services qui manipulent les données à caractère social obtenues via la BCSS de fonctionner.

[6] F = faible, donc rien à faire, M = moyen, donc réagir en fonction du risque, E = élevé, réagir rapidement pour faire disparaître le risque.

Tableau vierge pour les conseillers en sécurité.

Service	Menaces	Conséquences	Niveau de risques[7]	Justification	Action nécessaire pour diminuer le risque	Remplaçable / non remplaçable dans les délais fixés	Réalisé – non réalisé	Prioritaire – non prioritaire
Service : **Délai de redémarrage :**								

[7] F = faible, donc rien à faire, M = moyen, donc réagir en fonction du risque, E = élevé, réagir rapidement pour faire disparaître le risque.