Politique relative à la sécurité et à la confidentialité de l'information

Évaluation des risques

(BLD RISK)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait partie intégrante de la méthodologie relative à la sécurité et à la confidentialité de l'information dans la sécurité sociale. Il est destiné aux responsables, aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de la sécurité sociale (IPSS).

Le concept "risque" peut être interprété de plusieurs façons. Dans ces politiques, le concept "risque" est décrit comme la **(mal)chance** ("probabilité") qu'une certaine menace se produise avec un certain **impact** ("gravité") en conséquence.

Le concept "évaluation des risques" réfère à l'ensemble de procédures visant à identifier, analyser et évaluer les risques.

- L'**identification** des risques réfère au processus visant à examiner, reconnaître et décrire les risques.
- L'**analyse** du risque renvoie au processus visant à vérifier la nature d'un risque et à déterminer le niveau de risque.
- L'**évaluation** du risque consiste à comparer le résultat de l'analyse du risque avec des critères de risque prédéterminés dans le but de déterminer si le risque (et/ou son ampleur) est ou non acceptable ou supportable.

Dans la gestion des risques, il est opéré une distinction entre le risque "inhérent" et le risque "résiduel".

- Le risque "**inhérent**" réfère à la probabilité d'un impact négatif en l'absence de mesures de protection.
- Le risque "**résiduel**" renvoie en revanche à la probabilité d'un impact négatif en dépit de mesures prises pour influencer (limiter) le risque (inhérent).

Ce document décrit les politiques relatives à l'évaluation des risques concernant la sécurité et la confidentialité de l'information.

2. Évaluation des risques concernant la sécurité et la confidentialité de l'information

L'organisation souscrit aux politiques suivantes relatives à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité :

1. Dans chaque processus et chaque projet, l'organisation doit réaliser, valider, communiquer et tenir à jour une évaluation des risques concernant la sécurité et la confidentialité de l'information.
2. L'organisation doit communiquer toutes les évaluations des risques comportant un haut risque résiduel à la direction pour débat et décision : traitement ou acceptation.
3. L'organisation doit appliquer les consignes relatives à l'évaluation des risques mentionnées en annexe C de la politique "Évaluation des risques".

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2017		V2017	Intégration EU GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si des erreurs ou des problèmes sont constatés à la lecture du présent document, vous êtes prié en tant que lecteur de transmettre au conseiller en sécurité de la sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'institution une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement aux données de contact.

Définitions

Dans un souci de cohérence de la terminologie et des concepts utilisés dans tous les documents de politique, toutes les définitions relatives à la sécurité et à la confidentialité de l'information sont centralisées dans un document intitulé "Définitions relatives à la sécurité et à la confidentialité de l'information".

Annexe B : Références

Ci-dessous figurent des documents qui ont servi d'inspiration au présent document.

- RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 pages
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 pages
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 pages
- ISACA, "COBIT 5 for Risk", juin 2013, 218 pages
- ISACA, "Risk IT practitioner guide", novembre 2009, 137 pages

Ci-dessous figurent des références aux sites web qui ont servi d'inspiration au présent document :

- https://www.iso.org/isoiec-27001-information-security.html
- https://www.iso.org/fr/standard/54534.html
- https://www.iso.org/fr/standard/54533.html
- http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&qid=1488526812774&from=en
- https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- https://www.enisa.europa.eu/topics/data-protection
- https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia
- https://www.enisa.europa.eu/publications/tsp2-risk
- https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
- http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf
- http://www.ccb.belgium.be/fr
- https://www.ksz-bcss.fgov.be/fr

Annexe C : Consignes relatives à l'évaluation des risques

Une évaluation des risques doit être réalisée en fonction de l'ensemble des circonstances particulières de chaque traitement (ou groupe de traitements comparables).

La probabilité et la gravité du risque pour les droits et libertés de l'intéressé doivent être déterminées en fonction de la nature, du champ d'application, du contexte et des finalités du traitement. C'est donc en fonction de l'ensemble des circonstances particulières de chaque traitement que le responsable du traitement doit, d'une part, évaluer les risques pour la vie privée ainsi que pour les droits et libertés des personnes et, d'autre part, prendre les mesures qui s'imposent pour garantir l'application des dispositions du règlement.

Caractéristiques minimales d'une bonne gestion des risques

Le responsable du traitement décide librement de la procédure et de la méthodologie qu'il souhaite appliquer dans l'évaluation et la gestion des risques, à condition que celles-ci satisfassent à un certain nombre de caractéristiques minimales de fiabilité et d'objectivité. Il s'agit ici de caractéristiques minimales, qui en soi ne garantissent en rien que le(s) traitement(e) visé(s) aura (auront) lieu.

1. Basée sur une méthodologie : la gestion et l'évaluation des risques doivent reposer sur une base méthodologique, de préférence sur des méthodologies existantes en matière de gestion des risques. Des normes internationales, comme celles développées par ISO, ainsi que des codes de conduite développés ou reconnus au niveau européen, sont particulièrement importantes sur ce plan. Le responsable du traitement doit explicitement indiquer la méthodologie choisie et veiller à ce que celle-ci soit appliquée avec cohérence à travers le processus d'évaluation des risques.
2. Structurée : une bonne gestion des risques doit être structurée, avec les étapes suivantes :
   - Définition du contexte pertinent (composé des paramètres internes et externes à prendre en considération dans la maîtrise des risques).
   - Fixation de critères permettant d'évaluer les risques pour les droits et libertés des personnes physiques.
   - Identification et analyse des risques (y compris l'identification des vulnérabilités et des menaces ainsi que l'attribution d'une valeur de risque).
   - Détermination de valeurs de risque acceptables (y compris une définition des valeurs de risque inacceptables).
   - Identification de mesures de limitation de risques ad hoc (mesures techniques et organisationnelles nécessaires pour réduire le risque à un niveau acceptable).
3. Personnalisée : une évaluation des risques représente toujours un travail sur mesure. Une bonne évaluation des risques ne se limite pas à copier des analyses précédemment réalisées, mais requiert une estimation concrète basée sur le contexte spécifique (i.e. en fonction de la nature, du champ d'application, du contexte et des finalités du traitement). Rien n'empêche cependant qu'un responsable du traitement utilise des procédures ou des modèles développés par (ou en collaboration avec) d'autres entités (par exemple au niveau d'un secteur ou d'une branche d'entreprise spécifique) dans la réalisation d'une évaluation des risques.
4. Compréhensible : la conclusion d'une évaluation des risques doit être accessible à un public aussi large que possible. La conclusion ne peut pas être lisible uniquement par des experts (en risques), des techniciens ou du personnel spécialisé. Des synthèses et des aperçus visuels (comme des graphiques en couleurs, des tableaux chiffrés) peuvent favoriser l'accessibilité de l'évaluation des risques (à la fois le processus et sa représentation écrite).
5. Suffisamment nuancée : une évaluation des risques doit comporter suffisamment d'échelles pour permettre une évaluation nuancée des risques identifiés. Prévoir seulement trois échelles (faible, moyenne et élevée) pour évaluer les risques n'est pas suffisant pour aboutir à une appréciation correcte.
6. Communication et consultation : un bon système de maîtrise des risques nécessite la contribution des personnes les mieux placées dans l'identification, l'analyse, l'évaluation et la maîtrise des risques. Ce groupe comportera non seulement le délégué à la protection des données et/ou le conseiller en sécurité, mais aussi les développeurs de nouvelles applications, qui prennent des décisions stratégiques en matière de développement de projets et les membres du personnel (ou leurs représentants), qui utiliseront les données personnelles concernées dans l'exécution de leurs tâches.

7. Gestion et vérification : un rapport écrit et daté des évaluations de risques réalisées doit exister. Un organe mandaté en interne qui prend des décisions (comme le comité de direction, le comité stratégique ou le comité de la sécurité avec un mandat du conseil d'administration) doit être périodiquement informé du résultat (ou statut) du processus d'évaluation des risques. Cet organe mandaté doit formellement approuver l'évaluation des risques ainsi que les mesures destinées à réduire ceux-ci. Le processus d'évaluation des risques ne peut toutefois pas être réduit à un pur processus bureaucratique. Le responsable du traitement doit prendre des mesures adaptées pour veiller à ce que la bonne gestion des risques fasse partie intégrante de la "culture d'entreprise" du responsable du traitement. Une évaluation des risques doit être vérifiée périodiquement et à tout le moins lorsqu'elle est susceptible d'être influencée concrètement par un changement des circonstances. Dans le cadre d'une bonne gestion des risques, le responsable du traitement est supposé prévoir un contrôle au moins tous les deux ans. En outre, il est conseillé de soumettre formellement le résultat à l'approbation du plus haut organe dans l'organisation du responsable du traitement.

Méthodologie d'évaluation et de gestion des risques

C'est au responsable du traitement qu'il incombe d'appliquer une méthodologie lui permettant de satisfaire aux exigences.
Tout responsable du traitement qui entreprend une évaluation des risques appliquera une méthodologie adaptée aux besoins et au contexte de l'organisation.

Une organisation comprend la situation actuelle par :

- l'identification des objectifs (stratégiques et opérationnels), des obligations envers les intéressés, des obligations statutaires et de l'environnement dans lequel l'organisation opère ;
- l'identification des activités, biens et moyens, y compris ceux externes à l'organisation, qui aident à la livraison de ces produits et services ;
- l'identification et l'évaluation des menaces visibles susceptibles d'interrompre les processus et les activités critiques, ainsi que les biens et les moyens qui reposent à leur base.
- l'évaluation de la fréquence, de l'impact et des mesures de contrôle existantes.

Il est important que l'organisation comprenne les dépendances entre les activités, ainsi que toutes les dépendances externes, qui peuvent elles-mêmes être partagées avec des tiers.

Globalement, une bonne gestion des risques comporte les étapes suivantes :

1. Évaluation du risque au niveau de la fréquence, de l'impact et des mesures de contrôle existantes.
2. Analyse de la différence entre les mesures de contrôle existantes pour ce risque et les mesures de contrôle à atteindre pour ce risque.
3. Acceptation du risque résiduel ou prévention, transfert ou réduction du risque à un niveau acceptable.
4. Suivi et monitoring permanents des risques.

Pourquoi une analyse des risques ?

La sécurité et la confidentialité de l'information seront très largement influencées par la gestion des risques, non par la probabilité de certains événements, mais par des risques essentiels qui se réalisent sur la base d'événements inattendus. Sur la base du cadre de référence relatif à la gestion des risques, la stratégie concernant la sécurité et la confidentialité de l'information doit être déterminée à l'aide d'une analyse des processus et flux d'information importants, ainsi que des éléments et moyens d'infrastructure requis.

Il est important que l'organisation se protège contre des événements spécifiques - car elle ne peut pas tout prévoir - mais aussi qu'elle mette en œuvre les mesures nécessaires pour contrer les répercussions sur les activités importantes, quelles que soient la cause et les conséquences.

Une analyse des risques sert à identifier les processus critiques à rétablir après un incident ou une catastrophe grave. Cette analyse a pour but d'analyser les risques spécifiques vis-à-vis des mesures de contrôle existantes conçues pour réduire la probabilité qu'ils se produisent et limiter leurs répercussions.

Les risques sont des vulnérabilités face à des menaces. Une menace est un événement indésirable qui se produit sans avertir et qui est susceptible d'occasionner des dommages à l'organisation. La plupart des menaces se réalisent lorsque la majorité des personnes ne sont pas à proximité. La variable d'une menace est la probabilité que la menace se réalise. La variable d'un risque est le degré de vulnérabilité ou la mesure dans laquelle des mesures de contrôle réduiront l'impact de la menace si elle venait à se réaliser. La variable du processus est la valeur de chaque processus menacé. Cette valeur peut être objective et mesurable, comme la valeur exacte de remplacement d'un matériel, ou subjective, comme la bonne volonté.
Un risque est le résultat direct d'une menace qui se réalise. Exemples de risques : panne de courant causée par une inondation ou une sous-tension, accès non autorisé au centre à la suite d'une effraction ou perte de données résultant de procédures de restauration insuffisantes.

Une analyse des risques est un moyen d'évaluer systématiquement les risques potentiels de plusieurs incidents ou catastrophes graves. Usuellement, les risques d'autres types d'incidents (comme la violation de la confidentialité ou de l'intégrité des données) sont examinés simultanément, mais il ne doit pas en être ainsi.
L'analyse des risques doit permettre de comprendre le degré de perte potentielle (et autres effets indésirables). Il s'agit non seulement de préjudices financiers directs, mais aussi de bien d'autres choses, comme la perte de confiance de l'utilisateur final, l'atteinte à la réputation, les effets régulateurs...

Les événements suivants devraient être considérés comme des incidents ou des catastrophes graves pour l'organisation:

- Interruptions continues d'un système
- Échecs de mises à jour d'ordinateurs, de systèmes ou de logiciels
- Erreurs de programmation désastreuses
- Perte d'un site de production, d'un bureau ou autre site local
- Échec au lancement d'un service aux utilisateurs finaux parce qu'il s'avère ne pas fonctionner ou parce qu'il n'a pas la capacité suffisante pour répondre à la demande.
- Un fournisseur principal est touché par un incident ou une catastrophe grave.
- Un des travailleurs essentiels décède dans un accident de la circulation.

Dans certains cas, l'organisation peut décider de dresser des plans uniquement pour les incidents ou les catastrophes de grande échelle, non spécifiques : dans pareil cas, il est conseillé de ne pas consacrer trop de temps à l'analyse de ce que pourraient être ces événements non spécifiques. En même temps, il peut être précieux de comprendre et d'éviter les risques mineurs pour éviter que les événements mineurs tels qu'une panne de courant puissent subitement entraîner un impact bien plus lourd que prévu, par exemple par l'utilisation de générateurs.

Détermination de scénarios de risques pertinents

Identifier les risques spécifiques liés à la disponibilité ou l'indisponibilité des processus de l'organisation. Les phénomènes à risque possibles doivent être catégorisés, par exemple :

- Naturels : inondation, éclair, tornade
- Organisationnels : incendie, déchets, évacuation, barrage
- Géopolitiques : espionnage, guerre, terrorisme, absence de pouvoir
- Liés au personnel : grève, problèmes de transport, fraude, sabotage, erreurs
- Technologiques : piratage, virus, erreur logicielle ou panne informatique
- Liés aux fournisseurs : faillite, panne, sabotage ou OPA hostile
- Liés à la santé : épidémie de grippe, cancer
- Liés à la production : panne matérielle, pénurie, problème qualitatif, problème de certification

Pour éviter que l'organisation analyse uniquement des symptômes, procède de façon superficielle ou examine uniquement l'évidence, un cadre de référence simple mais complet est indispensable. Le modèle de risque le plus utilisé comprend trois grands domaines de risque :

- Risques liés à l'environnement (également appelés risques externes) : des menaces dans l'environnement industriel ou le climat politique, financier ou économique paralysent l'organisation ou changent significativement les principes fondamentaux de l'existence de l'organisation avec ses objectifs et stratégies.

- Risques liés aux processus (également appelés risques internes) : les processus ne sont pas clairement définis ou pas idéalement adaptés à la stratégie. Ou ils ne sont ni efficaces ni efficients dans la satisfaction des besoins des utilisateurs finaux, n'ont pas de valeur ajoutée ou exposent les actifs financiers, physiques et intellectuels à des pertes inacceptables, un détournement ou un abus.
- Risques liés à l'information pour la prise de décisions (également appelés risques de la direction) : l'information utilisée en soutien des décisions stratégiques, opérationnelles et financières n'est pas pertinente ou fiable. Beaucoup de décisions sont prises sur la base d'indicateurs de performance ou de résultats d'analyses industrielles ou financières. Si les mesures sont inadaptées à la stratégie ou si elles sont irréalistes, incompréhensibles et ne peuvent pas être suivies, c'est que l'organisation ne se concentre pas sur les bons problèmes et le système prévoit des stimuli pour des décisions qui ne sont pas cohérents avec la stratégie. Si l'information utilisée pour la prise de décisions n'est pas fiable ou pertinente, elle sera ignorée ou conduira à des mesures ou à un comportement indésirables.

Ces trois domaines sont étroitement liés entre eux, de sorte qu'ils constituent la base de la classification et de la présentation des risques présents sur le marché et dans l'organisation. Ce modèle permet aux organisations de considérer et d'analyser une large gamme de risques présents.
L'analyse des risques pour tous les sites doit toujours être axée en priorité sur la santé et la sécurité des travailleurs, la sécurité et les conséquences possibles pour l'environnement pour que les fonctions disposent des moyens nécessaires pour réussir.

Les cinq scénarios d'incident/catastrophe les plus récurrents sont les suivants :
- Indisponibilité d'un bâtiment ou d'une infrastructure physique d'importance
- Indisponibilité de travailleurs importants
- Indisponibilité d'une infrastructure ICT importante
- Indisponibilité d'un fournisseur externe important
- Indisponibilité ou fuite d'informations importantes

Détermination des risques inhérents

Outre chaque événement à risque, la probabilité et la fréquence possible de sa survenue doit être évaluée. Les événements inattendus se présentent sous toutes les formes possibles. Même les incidents mineurs, anodins à première vue, peuvent être très lourds de conséquences. De même que des catastrophes très spectaculaires peuvent entraîner un impact très limité. Pour certaines situations (comme les inondations ou les troubles civils), il est possible de trouver des informations sur la fréquence et la probabilité en prenant contact avec l'administration ou la police. Il est toujours préférable de commencer par une analyse des dépendances et des vulnérabilités à partir des processus critiques.

1. Analyse de probabilité
Dans cette phase, la probabilité ou la fréquence d'un incident ou d'une catastrophe grave est identifiée de façon quantitative. Il s'agit ici d'une dimension temporelle où une réponse peut être donnée à la question : "Combien de fois un tel incident ou une telle catastrophe se produit dans tel scénario ?".
La probabilité qu'un incident ou une catastrophe grave se produise doit être induite de diverses sources.
La probabilité doit être mesurée dans le temps. Pendant combien de minutes/heures/jours/semaines/mois les répercussions d'un incident ou d'une catastrophe grave seront visibles ? Combien de jours faut-il pour que l'organisation récupère 75 % de fonctionnalité, c'est-à-dire que 75 % des personnes, moyens et processus soient à nouveaux opérationnels ? Combien de jours faut-il pour que l'organisation puisse remplacer les moyens perdus, comme louer un nouveau bâtiment ou rendre le bâtiment fonctionnel après un incendie ? Il faut décider d'un délai maximum raisonnable après une panne que l'on souhaite mesurer et ensuite évaluer l'impact par intervalle à partir du point impact jusqu'à l'impact maximal. Par exemple, après 10 minutes, 1 heure, 4 heures, 12 heures, 1 jour, 1 semaine, 1 mois, 3 mois.

2. Analyse de l'impact
Dans cette phase, les conséquences d'un incident ou d'une catastrophe grave peuvent être identifiées de façon quantitative. Sur la base de cette phase, les fonctions les plus pertinentes avec leurs priorités de rétablissement et les interdépendances sont élaborées de manière à pouvoir atteindre les objectifs de rétablissement fixés.

L'analyse de l'impact constitue la phase fondamentale. Elle implique l'évaluation de l'impact d'un scénario particulier sur une activité (dans le temps). Le scénario peut être spécifique, comme la survenue de risques inhérents (risques sans mesures de contrôle) ou génériques, comme la perte d'accès à un site. L'analyse de l'impact doit être réalisée sur la base de l'analyse des risques qui a permis d'identifier les risques les plus pertinents qui perturberaient gravement l'organisation. En bref, une analyse de l'impact est un processus structuré dans lequel l'organisation détermine et documente l'impact d'une interruption de processus et d'activités de support. Une analyse de l'impact doit livrer les résultats suivants à l'organisation :

- Identification des processus critiques sensibles au temps
- Analyse des conséquences financières et opérationnelles pour l'organisation
- Estimation des délais dans lesquels les opérations, processus et fonctions sensibles au temps doivent être rétablis
- Estimation des moyens nécessaires pour une reprise et un rétablissement réussis

Le but est de vérifier quelle serait l'ampleur des répercussions d'un incident ou d'une catastrophe grave sur l'organisation. Ceci permet à l'organisation de prioriser les investissements pour améliorer ou garantir la disponibilité, coordonner des mesures et mettre des plans en œuvre pour limiter l'impact d'un incident ou d'une catastrophe grave en cas de souci avec des systèmes critiques et l'organisation.
D'une part, l'organisation examinera les facteurs quantifiables comme la perte de revenus, les amendes, la perte d'intérêts... D'autre part, elle se penchera sur des domaines d'impact moins directs, comme la perte d'utilisateurs finaux, la dégradation de l'image, la perte de confiance, etc. L'organisation regarde quelles sont, pour les activités, les conséquences d'une indisponibilité de durées différentes, comme une demi-journée, une journée, une semaine ou un mois. L'organisation en infère alors la durée maximale d'indisponibilité ("maximum downtime") des applications critiques et des systèmes sur lesquels elles tournent. Sur cette base, l'organisation détermine alors quelles sont les solutions alternatives les plus indiquées.
L'approche implique de premièrement répartir chaque département en processus fonctionnels et en activités critiques. Si cette tâche est difficile en soi, il peut être utile de réaliser une analyse des processus business avant de démarrer cette phase. Pour chaque processus fonctionnel, la personne désignée par l'équipe du programme central devra fournir les informations de base nécessaires sur leur environnement, comme les descriptions de processus et le directeur responsable.
Les processus peuvent être traités séparément s'ils ont différents travailleurs (rôles par exemple), prestataires de services (outsourcing par exemple) ou moyens (systèmes IT par exemple).
Ensuite, l'impact d'un incident sur chaque processus doit être mesuré. Une autre analyse peut être réalisée pour évaluer l'impact de chaque menace potentielle sur l'organisation, mais il peut être tout aussi intéressant (et nettement plus rapide) d'évaluer un "worst case scenario" de perte totale d'accès aux sites, technologies et personnes.
Lors de l'évaluation de l'impact, il faut prendre en compte les répercussions sur l'atteinte des objectifs ainsi que sur les intéressés. Les conséquences possibles (impact secondaire) sont :

Environnement externe

- Non atteinte ou atteinte tardive des objectifs
- Dommage aux relations
- Décisions/exécution affaiblies
- Dommages environnementaux
- Dégradation de la réputation/image

Planning, processus et systèmes

- Endommagement ou perte de moyens, installations, technologies ou informations
- Dommage à la viabilité, coûts imprévus, amendes, dépassements budgétaires
- Fraude ou irrégularités
- Régression de la qualité des produits ou services

Individus

- Santé et sécurité - impact sur les travailleurs et le bien-être général
- Perte de moral/productivité des travailleurs

Aspects légaux et réglementation

- Impact des violations des droits légaux ou des réglementations
- Indemnisations, amendes et responsabilité légale

Ci-dessous quelques exemples de thèmes de risque inspirés des technologies avec leur impact potentiel :

Thème de risque	Impact	Considération pour la direction
Appareils mobiles	• Plus d'appareils mobiles sur le terrain • Plus grande dépendance à la technologie pour rester productif • Plus d'accès à des processus et des workflows externes à l'organisation • Rapportage plus rapide et plus direct des événements • Plus d'appareils mobiles non approuvés par l'organisation (Bring Your Own Device ou BYOD) apportés par des travailleurs ou des fournisseurs ayant accès à l'information.	• Les appareils mobiles doivent être repris dans le plan pour le support aux fonctions importantes dans l'organisation. • Les appareils mobiles utilisés doivent régulièrement être entretenus et améliorés. • Dans la formation, le rôle des appareils mobiles doit aussi être abordé. • Les plans doivent indiquer la présence d'appareils mobiles pour la communication comme les SMS, les réseaux sociaux, les avis, etc. • Les contrats avec les fournisseurs de télécommunications doivent également reprendre les exigences en matière de perte, de vol ou de destruction des appareils mobiles et indiquer comment (dans quel délai) ils doivent être remplacés.
Réseaux sociaux	• Publication et diffusion très rapides d'événements via les réseaux sociaux • Moyen bon marché de diffuser des messages	• L'approche doit comporter une politique et des instructions spécifiques concernant l'utilisation des médias sociaux en cas de crise, en ce compris la liste des porte-paroles reconnus pour l'organisation. • Seules des personnes spécifiquement désignées peuvent publier des messages ou un statut sur les médias sociaux pour l'organisation. • Durant la formation et les exercices, l'utilisation des médias sociaux est également simulée.
Virtualisation des serveurs	• Moindre dépendance aux systèmes physiques pour supporter l'infrastructure IT. • Moins de personnel nécessaire pour le support des environnements virtuels • Gestion de serveurs plus centralisée • Moindre impact sur les activités de maintenance	• Stricte tenue à jour des environnements virtuels dans l'organisation afin de pouvoir les énumérer pour les plans. • Les environnements virtuels doivent être éprouvés en termes de faiblesses. • Emporter des environnements virtuels aux exercices. • Réfléchir au rétablissement virtuel des environnements actifs en permanence
Virtualisation desktop	• Élargissement du site de travail vers des sites externes à l'organisation • Déploiement plus rapide vers un nouvel environnement desktop • Gestion centralisée des desktops • Dépendance à internet et aux télécommunications	• Le desktop virtuel peut être utilisé pour l'environnement temporaire à l'activation du plan • Solution pertinente pour les fonctions importantes dans l'organisation • La sécurisation du desktop virtuel doit être régulièrement contrôlée et améliorée
Cloud computing	• Plus grande dépendance aux prestataires de services externes (leurs plans de rétablissement) • Contrôle moins direct sur les propres processus et l'infrastructure IT • Meilleure flexibilité et moyen plus rapide de déplacer des applications et informations entre différentes infrastructures • Meilleures possibilités de planification de capacité grâce à une plus grande flexibilité • Payer uniquement ce que l'on utilise	• Analyse des risques nécessaire avant de migrer vers des solutions cloud • Clairement fixer et éprouver les exigences des contrats • Exécuter régulièrement des exercices à l'aide d'un cloud service provider • Exercices de récupération de données depuis le cloud service provider (rapidité et exhaustivité) • Veiller à une propre sauvegarde de données indifféremment de la solution de sauvegarde de données du cloud service provider • Régulièrement vérifier le statut du cloud service provider (financier, réputation, évolutions, nouveaux services...)

Thème de risque	Impact	Considération pour la direction
		• Prévoir une propre protection des données dans la solution cloud tant en production que dans l'environnement de back-up (cryptage) • Envisager le cloud pour simuler de grands problèmes d'infrastructure IT ainsi que pour des exercices de restauration à grande échelle

Estimer le niveau d'impact. Lors de la mesure des conséquences financières, l'ampleur des dégâts potentiels doit être quantifiée le mieux possible. Vu qu'il s'agit d'un exercice hypothétique, il peut être difficile à exécuter, mais c'est une base pour un solide business case. La dégradation de la réputation peut être quantifiée s'il existe des exemples du passé ou d'autres utilisateurs finaux. En cas d'impact non quantifiable, une échelle, par exemple de 1 à 5, peut être établie et définie pour les participants afin d'estimer l'impact, où 5 représente un impact lourd et 1 un impact négligeable (une autre échelle peut être utilisée ici, en fonction du niveau de granularité exigée). L'analyse quantitative de l'impact consiste à attribuer des probabilités et une valeur monétaire à des pertes potentielles. L'analyse qualitative de l'impact peut être plus efficace pour décrire les conséquences des risques et vulnérabilités potentielles. L'impact de la réalisation d'un risque doit alors être fixé pour comprendre quel degré de perturbation il pourrait occasionner et donc la rapidité avec laquelle il doit être évité ou planifié. À ce stade, Il faut éviter trop de détails et évaluer l'impact ainsi que la probabilité de façon simple sur une échelle de 1 à 5 par exemple, où une inondation présente un score 5 pour l'impact, mais un score 1 pour la probabilité, de sorte que le score de risque total s'élève à 6 (si on cumule les deux scores). De la même manière, une grande panne réseau peut présenter un score 4 pour l'impact et un score 3 pour la probabilité, pour aboutir à un score total de 7. On peut par exemple décider de traiter uniquement les risques présentant un score supérieur à 5. Pour autant que les moyens soient importants, voire essentiels pour l'organisation, cela a donc des conséquences pour les processus critiques. Et un incident ou une catastrophe grave entraîne un impact significatif.
Indicateurs d'importance :

- Le processus soutient la vie ou la santé et la sécurité des individus.
- Le processus est nécessaire en raison d'exigences légales ou statutaires.
- La perturbation du processus influence directement et nettement les résultats de l'organisation.
- Il y a un impact évident sur la réputation et l'image.

La méthode d'évaluation de l'impact doit être clairement expliquée et les réponses doivent être mises à l'épreuve afin de garantir qu'elles soient cohérentes, précises et approfondies. L'impact potentiel peut être classé : par exemple "critique, élevé, moyen, faible, très faible". Plusieurs critères sont possibles pour déterminer l'impact. Ce n'est donc pas comme si seul un impact financier est possible. Il y a aussi des conséquences au niveau humain ainsi que sur les plans de la sécurité, de la qualité et du management. L'essentiel est qu'un tel schéma soit partout identique dans l'organisation à un moment donné. Sur la base de l'expérience pratique, un tel schéma peut être affiné et adapté, pour autant qu'il soit partout pareil dans l'organisation.
Il est en effet important d'indiquer des événements importants à la fois en interne et en externe qui ont un impact négatif potentiel sur l'organisation et sur le service aux utilisateurs finaux de l'organisation. Il s'agit de pouvoir opérer des choix et de fixer des priorités, le plus objectivement possible. Il s'agit également de demander et d'obtenir la collaboration des intéressés pertinents.
Les résultats de cet exercice permettra de prioriser les domaines à rétablir, en fonction du délai dans lequel ils devraient être rétablis et de la perte potentielle pour l'organisation en cas d'échec. Il y a plusieurs manières de rassembler des informations et de réaliser l'analyse de l'impact business : outil automatisé, questionnaire e-mail, enquête papier, interview face à face, ateliers... On peut recourir aux interviews et à des questionnaires pour interroger les personnes-clés et les intéressés. Certaines personnes ont tendance à surestimer l'importance de leur propre division pour l'organisation, tandis que d'autres sous-estiment totalement leur valeur et se présentent presque comme superflues.
Il est important que les individus qui contribuent à l'analyse de l'impact disposent de données précises et réalistes, car les données de cette phase seront utilisées dans toutes les phases suivantes pour prendre des décisions et affiner le planning.
Enfin, celui qui récolte les informations sur les conséquences des incidents ou des catastrophes graves est crucial pour l'identification des résultats et des décisions de la direction.

Détermination du risque résiduel

Analyser les vulnérabilités en regardant les mesures de contrôle déjà présentes afin de contrer les phénomènes à risque identifiés. Les mesures de contrôle qui réduisent les risques comprennent une protection et des contrôles de l'environnement, la sécurité et les procédures d'urgence, des procédures de sauvegarde et de restauration de données ainsi que des pratiques relatives au personnel. En l'absence de mesures de contrôle pour réduire la probabilité ou l'impact d'un certain risque, celles-ci devront être développées et mises en œuvre. Au final, il subsistera quelques risques qui ne peuvent être évités (comme les attentats terroristes et les catastrophes naturelles). Il est seulement possible de les limiter en développant des règlements spécifiques.
Les mesures de contrôle peuvent réduire le risque de menaces, comme la suppression des produits inflammables, ou réduire les conséquences. Ainsi, l'alarme incendie et les extincteurs automatiques à eau peuvent réduire les dégâts d'un incendie.

L'élimination ou la réduction des conséquences des menaces potentielles s'effectuent par la prise des bonnes mesures de contrôle, procédures et pratiques avant que ne se produisent des incidents ou des catastrophes graves. L'évaluation des risques est axée sur l'identification des menaces potentielles et des mesures de contrôle existantes et peut conduire à des recommandations pour amélioration. Le but de cette activité est soit de réduire une menace potentielle, soit de réduire son impact si un incident ou une catastrophe grave se produit.
Typiquement, l'organisation prévoira des mesures de contrôle pour les éléments d'infrastructure les plus essentiels, partant du principe que les fondamentaux seront préservés et qu'une solution sera trouvée pour les autres. L'organisation doit ici se demander si cette solution lui permet de rétablir les flux d'information critiques.
En outre, ces solutions orientées infrastructure sont relativement onéreuses, vu qu'elles ne "génèrent" rien en tant que telles tant qu'il n'y a pas d'incident ou de catastrophe. Il s'avère généralement difficile d'en justifier le coût, raison de plus pour se limiter aux éléments vraiment essentiels. De même, l'organisation peut se demander si ces mesures de contrôle permettent de réaliser les objectifs. Dans la réalité, on remarque même que les objectifs ne sont pas fixés de façon univoque. Si l'objectif est de pouvoir redémarrer les applications IT, celui-ci sera (on l'espère) bien atteint. Si l'objectif est d'assurer la continuité du service, il apparaît moins clairement si l'objectif sera atteint lorsque l'organisation se concentre sur les éléments d'infrastructure.

Matrice des risques

Sur la base des trois activités précédentes, on doit être en mesure d'élaborer une matrice des risques (résiduels) qui identifie les risques, conjointement à leur probabilité et leur impact, et les mesures de contrôle existantes.
La probabilité, l'impact et les mesures de contrôle pour les risques susceptibles de conduire d'entraîner de lourds incidents ou catastrophes doivent être évalués sur la base de la situation actuelle.
Cette analyse est utilisée de la même manière pour indiquer à la direction quels processus ou services peuvent être arrêtés en premier ou en dernier lorsque l'activité est surchargée ou se rétablit d'un incident ou d'une catastrophe grave.
L'analyse des risques procure à la direction les informations fondamentales pour évaluer l'intérêt de l'approche alternative proposée. La réalisation de l'analyse durant des exercices de simulation (en préparation à des incidents ou des catastrophes) aide à identifier correctement l'impact potentiel ainsi qu'à approuver les résultats généraux et les mesures de contrôle.
Il existe des corrélations entre l'analyse des risques et l'évaluation, ainsi que la gestion des risques dans l'organisation. Une bonne analyse de l'impact business peut aider les managers à opérer des choix bien considérés et à réduire l'impact de plusieurs problèmes, allant des événements mineurs aux grandes catastrophes. Ce n'est qu'au moment où la matrice des risques est prête que le comité de pilotage peut/doit choisir une des quatre options de décision par risque.

- Option de décision 1 : partager le risque

  Le risque est confié en partie à un tiers. Ceci peut se faire via l'assurance classique ou via des accords contractuels avec un fournisseur spécialisé. Il est également possible de payer un tiers pour prendre le risque en charge d'une autre manière. Si une bonne assurance peut largement diminuer l'impact financier d'un incident ou d'une catastrophe grave, elle ne peut jamais faire en sorte que les processus de l'organisation soient rétablis rapidement.

- Option de décision 2 : éviter le risque

  Dans certaines circonstances, il est conseillé d'adapter, de reporter ou de clôturer le service, le produit, l'activité, la fonction ou le processus. Cette option peut être envisagée lorsqu'il n'y a pas de conflit avec les

objectifs, les obligations (statutaires) et les attentes des intéressés. Cette option sera probablement envisagée quand un service, un produit, une activité, une fonction ou un processus a une espérance de vie limitée.

- Option de décision 3 : limiter le risque

  Cette option est utilisée pour limiter les risques financiers ou les risques liés aux biens. Le risque est transféré pour réduire l'exposition de l'organisation au risque ou parce qu'une autre organisation est plus compétente dans la gestion du risque.

- Option de décision 4 : accepter le risque

  Le risque est accepté sans qu'une action soit entreprise. Si l'organisation choisit d'accepter un risque, elle doit savoir qu'elle assure également les conséquences possibles si le risque se réalise. Une organisation décidera rarement d'accepter purement et simplement les risques d'un incident ou d'une catastrophe grave. Même si le risque est inacceptable, le pouvoir d'y faire quelque chose peut être restreint ou le coût nécessaire pour agir et les avantages potentiels peuvent être disproportionnels (évaluation coûts/bénéfices). Dans ces cas, le niveau de risque actuel peut suffire dans la zone de confort de risque (risque résiduel acceptable en fonction du "risk appetite") de l'organisation. Cette option peut être complétée d'un plan pour faire face à l'impact si le risque se réalise. La détermination de la meilleure stratégie pour faire face au risque est l'objet de l'analyse.

Derniers conseils en matière de gestion des risques

- Veillez à un soutien visible de la direction : sans elle, c'est mission impossible.
- Veillez à ce que la direction et le coordinateur des risques collaborent étroitement : des échelles et des critères d'évaluation communs permettent une assimilation meilleure et plus rapide dans l'organisation.
- Ne vous attachez pas uniquement aux dommages/répercussions d'ordre financier, mais aussi aux dommages à la réputation et aux moyens nécessaires à la réparation de ces dommages.
- Ne regardez pas uniquement votre propre organisation, mais considérez également les conclusions des collègues, fournisseurs, partenaires... en matière d'évaluation des risques : échangez les connaissances.
- Soyez conscient du fait que la direction acceptera certains risques : c'est leur privilège et leur mandat : décider de tout laisser (provisoirement) tel quel.
- Utilisez seulement trois questions pour sonder les différents risques : probabilité, impact et état actuel du contrôle.
- Appliquez toujours un délai précis pour la phase d'analyse des risques, sans quoi vous n'aurez jamais fini.
- Veillez à définir le "pire scénario" ("worst case scenario") afin que chacun comprenne la même chose.
- Ne confiez aux partenaires externes que les choses que l'on comprend et dont on connaît le plan des partenaires externes choisis.

Annexe D : Lien avec la norme ISO 27002:2013

Nous renvoyons ici à la (aux) clause(s) principale(s) de la norme ISO 27002:2013 relative à l'objet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	**Oui**
Organisation de la sécurité de l'information	
Personnel sûr	
Gestion des moyens d'exploitation	
Sécurisation des accès	
Cryptographie	
Sécurité physique et de l'environnement	
Sécurisation des processus	
Sécurité de la communication	
Achats, maintenance et développement de systèmes d'information	
Relations fournisseurs	
Gestion des incidents de sécurité	
Aspects de sécurité de l'information de la gestion de la continuité	
Respect	**Oui**

***** FIN DU DOCUMENT *****