Guide méthodologique pour réaliser une analyse des risques et une DPIA avec MONARC

Contents

Guide méthodologique pour réaliser une analyse des risques et une DPIA avec MONARC

1 Objet du guide méthodologique

Le guide méthodologique décrit comment réaliser une analyse des risques et une « *Analyse d'Impact relative à la Protection des Données (DPIA*[1]) », afin de répondre aux exigences du GDPR[2] et plus précisément aux exigences :

- de la responsabilité et de la démonstration de la conformité (article 24),
- de la sécurité des données (article 32),
- de la réalisation d'une DPIA (article 35).

Concernant l'article 35, l'objet du guide méthodologique n'est pas de définir les règles qui permettent de déterminer si un traitement est *« susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »*, mais de réaliser la DPIA elle-même.

Concernant l'obligation de mener une DPIA, le groupe 29 ainsi que certaines autorités de contrôle ont déjà émis des lignes directrices.

2 Présentation de MONARC

2.1 Historique

MONARC (Méthode Optimisée d'aNAlyse des Risques CASES) a été développée depuis 2011, dans le but de permettre aux très petites, petites et moyennes entreprises de gérer leurs risques. MONARC est simultanément une méthode et un outil, facile à prendre en main et assistant au maximum l'utilisateur à l'aide de base de connaissances, de valeurs par défaut et de partage de l'information.

CASES (Cyberworld Awareness Security Ehancement Services) est un département du groupement d'intérêt économique « Security Made In Lëtzebuerg » dont le nom d'usage est « SecurityMadeIn.Lu ». En 2011, CASES est déjà très renommé au Luxembourg parce qu'il promeut depuis 2003, la sécurité de l'information via des campagnes thématiques et des séances de sensibilisation au sein du grand public, des entreprises du secteur public et privé, ainsi que dans les écoles fondamentales au Luxembourg.

MONARC comme beaucoup d'outils d'analyse des risques fut d'abord développé sous Excel, mais porté rapidement sur une plateforme Web pour améliorer le partage et la diffusion des modèles de risques. La méthode d'apprentissage « Learning by Doing » est appliquée pour développer les fonctionnalités de l'outil et les bases de connaissances.

---

[1] En anglais DPIA : Data Protection Impact Assessment, en français AIPD : Analyse d'Impact relative à la Protection des données.
[2] En anglais GDPR : General Data Protection Regulation, en français RGPD : Règlement Général sur la Protection des Données.

La présence constante de l'équipe CASES sur le terrain a permis de rencontrer dès 2014, des juristes qui préparaient l'avènement du GDPR. Dès lors, les évolutions de MONARC en furent imprégnées.

Dans le but d'augmenter le nombre d'utilisateurs et de mutualiser les contributions à l'outil, MONARC est réécrit en version « Open Source » en 2016 et sera publié sur Github en 2017. Il est téléchargeable sur « github.com », « monarc-project », via une machine virtuelle qui propose l'outil ainsi que toutes ses bases de connaissances.

En 2016, un autre grand pas fût franchi avec la Déclaration conjointe – Gäichel IX[3] dans laquelle les Premiers ministres luxembourgeois et belges se félicitent de lancer une « *Collaboration au niveau d'un outil d'analyse des risques développé au Luxembourg (MONARC) : Les deux pays vont s'échanger des normes, standards et bonnes pratiques et méthodes de gestion des risques pour notamment pouvoir soutenir les secteurs public et privé en vue d'une mise en conformité avec la Network Information Security directive (NIS directive) et le règlement général sur la protection des données.* ».

La promotion de MONARC et son essor sont désormais assurés.

2.2 Qu'est-ce que MONARC ?

MONARC est une méthode outillée d'analyse des risques qui met qualitativement en œuvre ISO/IEC 27005[4]. Le choix de ce standard international évite l'exotisme et permet aux utilisateurs de trouver une multitude d'ouvrages en support.

MONARC gère les risques de l'information basés sur les critères CID (Confidentialité, Intégrité, Disponibilité). Il propose une modélisation hiérarchique qui permet de visualiser clairement les dépendances entre les actifs primaires[5] et les actifs de supports[6]. Le risque est calculé en fonction de 3 critères : la menace, la vulnérabilité et l'impact sur l'organisme. Le choix de dissocier la menace et la vulnérabilité (plutôt que d'utiliser des scénarios) permet une évaluation du risque en deux phases, mais surtout de placer le focus sur la vulnérabilité, c'est-à-dire les mesures de sécurité en place et l'écart avec les bonnes pratiques du domaine.

Dans sa version de base, MONARC propose deux granularités pour identifier les risques :

- Le modèle optimisé est préconisé pour dérouler la première itération d'analyse des risques. Il s'agit d'une sélection pragmatique des risques les plus courants qui assurent de ne pas s'égarer dans des détails futiles avant de traiter l'essentiel. Ces bases optimisées ont été créées à partir des bonnes pratiques du domaine de la sécurité de l'information et ont été améliorées au fur et à mesure de multiples analyses.

[3] Déclaration conjointe – Gäichel IX, Gäichel, le 4 juillet 2016 - https://www.gouvernement.lu/6144888/declaration-Gaichel.pdf
[4] ISO/IEC 27005:2011 - Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information (www.iso.org).
[5]Actifs primaires ou métiers – Processus, service ou information ayant de la valeur pour l'organisme.
[6]Support aux actifs primaires. Éléments du système d'information composé non exhaustivement par le matériel, les logiciels, les personnes, les bâtiments, les réseaux…

- Le modèle exhaustif provient des bases de connaissances EBIOS[7]. Ces bases permettent une analyse des risques en profondeur, très utile pour les itérations successives d'analyses des risques.

MONARC gère également les risques opérationnels. La différence avec les risques de l'information réside dans le fait que les critères d'impact sont basés sur les valeurs propres à l'organisme : c'est-à-dire sa « Réputation », son « Opération », son « Légale », ses « Finances » sur lesquels est ajouté « l'impact à la Personne », le tout nommé ci-après « ROLFP ». Les risques opérationnels sont calculés en fonction de deux critères, la vraisemblance d'un scénario de risques et l'impact ROLFP. Dans ce cas, le choix du scénario permet de décrire plus facilement, dans un langage naturel, les risques métiers et les risques de gouvernance.

MONARC propose des bases de connaissances qui permettent d'identifier les risques principaux. Une bibliothèque d'actifs de base permet de construire d'autres actifs plus évolués tel un jeu de « Lego ». Cette construction hiérarchique permet une très grande personnalisation des modèles de risques, mais le plus important est que chaque actif ainsi construit peut être échangé et amélioré entre analyses et utilisateurs. Ceci faisant de MONARC un outil basé sur le partage et l'amélioration.

3 Inventaire des traitements

Le registre des traitements est le point de départ pour la mise en conformité. Il est donc nécessaire de procéder à un inventaire de ceux-ci, si ce n'est pas encore fait.

Parmi ces traitements, il est de la responsabilité du « *Responsable du traitement* » de décider lesquels vont faire l'objet de la DPIA.

L'important est d'avoir une démarche pragmatique, qui en fonction de la taille de l'entreprise et du nombre de traitements ou d'opérations de traitements concernés par les analyses d'impacts, permettent de définir la cible de l'analyse des risques, puis celle de l'analyse d'impact.

En d'autres termes, il faut vérifier que l'écart entre cibler uniquement les opérations de traitements concernées ou cibler l'ensemble du système d'information (ou du moins un sous-ensemble fonctionnel entier) n'est pas contre-productif. La méthodologie MONARC permet de réutiliser les évaluations des risques faites sur les services ou processus transversaux. Une fois les évaluations faites pour un traitement ou une opération de traitement, elles ne seront plus à refaire pour les autres.

Note : Avoir réalisé une analyse des risques de l'information sur un ensemble fonctionnel ou la totalité du système d'information va au-delà de la conformité au GDPR. C'est un moyen de maitriser la sécurité et la pérennité de vos activités métiers.

4 Analyse des risques de l'information

La méthode d'analyse des risques MONARC propose une démarche conforme à ISO/IEC 27005. L'outil guide l'utilisateur dans une succession de phases :

[7] EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité. La méthode EBIOS est un outil complet de gestion des risques SSI, créée en 1995 par l'agence nationale de la sécurité des systèmes d'information française (www.ssi.gouv.fr).

Établissement du contexte

Cette phase permet de déterminer le périmètre de l'analyse, de définir les éléments qui feront l'objet du focus de celle-ci, mais également de déterminer pourquoi l'analyse de risque est déroulée. Ces informations sont primordiales, car elles conditionnent toute l'analyse et surtout l'usage qui en sera fait (voir ci-dessous, paragraphe « Identification des actifs »).

Dans cette phase, il y a lieu de s'intéresser aux critères d'évaluation des risques et notamment à la table d'impacts. Par défaut cette table possède une échelle d'évaluation de 0 à 4. Cette échelle est communément utilisée et donc, à moins de disposer de sa propre échelle, le conseil est de ne pas la modifier ou du moins ne pas modifier le nombre d'échelons. En France, la CNIL[8] préconise également une échelle à 4 niveaux (hors 0). Elle propose des libellés d'échelons suffisamment génériques, il suffit simplement de les copier (si ce n'est pas encore fait) et d'éventuellement les contextualiser à l'organisme ou à son activité en fonction des types de données traitées et des impacts possibles à la personne.

La phase d'établissement du contexte permet également de mettre le focus sur les menaces. Dans le cas précis du GDPR, le critère de confidentialité est déterminant et toute menace affectant ce critère doit être prise en considération. Les critères de disponibilité et d'intégrité sont un peu en retrait, mais de nouveau il appartient au responsable du traitement de choisir si l'analyse de risques est mutualisée pour gérer ou non l'ensemble des risques de l'information de l'organisme.

Identification des actifs

Cette phase permet de bien cibler les actifs sur lesquels le focus d'analyse sera porté. Dans le jargon du métier, nous parlons d'actifs primaires ou d'actifs métier. Ils représentent ce qui est important pour l'organisme à savoir ses processus, ses services externes (comme le service après-vente), ses services internes de support (comme la comptabilité ou la gestion des ressources humaines) et l'information essentielle qu'elle soit métier ou à caractère personnel. C'est parmi ces actifs qu'il faut inclure les informations visées par les traitements de données à caractère personnel.

La modélisation est très importante. Il faut avoir une vue précise sur les traitements de données à considérer. Selon l'approche il serait possible d'en omettre ou à l'inverse de les considérer plusieurs fois dans le modèle, ce qui pourrait le rendre compliqué, voir incohérent lorsqu'il faudra positionner les impacts et conséquences.

Explications : un traitement de données peut s'exécuter au sein d'un même service ou d'un même processus, mais peut également être beaucoup plus complexe et transversal par rapport à l'organisation. Par expérience, voici les grandes lignes qui pourront guider le choix du type de modélisation :

a) Vue service (interne ou externe) : La vue service est plutôt verticale (en Silo) dans la structure de l'organisme. Les traitements sont soit internes aux services, soit transversaux et c'est justement dans ce dernier cas que la complexité s'accroît. Les opérations de traitements sont disséminées à travers plusieurs services fonctionnels

[8] CNIL, Commission Nationale de l'Informatique et des Libertés. La CNIL propose des méthodes et outillages, voir le document CNIL-PIA-2-Outillage.pdf (www.cnil.fr)

et bien souvent les responsables métiers n'ont pas la connaissance du workflow entier, il faut ainsi le reconstruire et le documenter, ce qui est coûteux en termes de ressources.

b) Vue processus : La vue processus est de loin, la meilleure. Elle coïncide exactement avec l'organisation des métiers ou les traitements de données très proches des traitements au sens GDPR du terme. Dans tous les cas, les opérations de traitement y sont décrites suffisamment en détail, ainsi que les workflows liés pour être modélisés rapidement. Malheureusement peu d'organismes ont une vue précise et documentée de leurs processus.

c) Vue information : Dans ce cas, l'analyse se focalise sur les données et les opérations de traitements opérées. Cette approche est assez simple, le modèle résultant l'est également, par contre, comme ce dernier ne correspond pas à une vue fonctionnelle de l'organisme, l'analyse ne peut être utilisée pour traiter les risques de l'information. La mutualisation[9] est compliquée, voire impossible.

Quelle que soit la modélisation choisie, il faut prendre en considération le cycle de vie de l'information (création, utilisation, archivage / destruction).

Identification des impacts et conséquences

Dans le domaine de la sécurité de l'information, les critères de sécurité utilisés sont au minimum : la confidentialité, l'intégrité et la disponibilité. Dans MONARC, ces critères sont directement liés avec les conséquences ROLF. Ces conséquences sont généralement déterminées par les métiers, puis sont paramétrées au niveau des actifs primaires et hérités par les actifs de supports. Cet héritage par défaut permet un gain de temps certain, mais doit parfois être affiné au niveau de certains actifs de support.

Identification des risques

Cette phase est fort simplifiée dans MONARC, car chaque actif de support possède un modèle optimisé de risques découlant des exigences de l'annexe A de la norme ISO/IEC 27001. Le modèle optimisé est basé sur les principaux risques déduits de l'absence de bonnes pratiques en sécurité de l'information. La modélisation consiste à décrire les dépendances entre les actifs primaires et les actifs de supports. Les bases de connaissances incluses dans MONARC permettent une identification des risques principaux, les risques contextuels devront être identifiés manuellement.

Évaluation des risques

Dans MONARC, le risque est calculé en fonction de 3 paramètres : la probabilité d'une menace, l'impact sur l'organisme et la vulnérabilité. À ce stade de l'analyse, la probabilité d'occurrence de la menace a été évaluée au cours de la phase « Établissement du contexte ». L'impact a été évalué au cours de la phase « Identification des impacts et

9 Mutualisation : Utilisation d'une seule analyse des risques pour atteindre simultanément plusieurs objectifs. Exemple :

- Amélioration du niveau de sécurité des processus métier (CID --> ROLF de l'organisme), avec ou non un objectif certifiant ISO/IEC 27001
- Conformité juridique au GDPR (CID --> P (Impact à la personne))
- Conformité à d'autres référentiels (CSC, DAC, REMIT, …)
- Recherche de mise en place de bonnes pratiques telles que (ISO/IEC 27002, 27799, …).

conséquences ». Il ne reste donc qu'à évaluer la vulnérabilité en fonction des mesures de sécurité déjà en place. Cette étape exige un niveau de compétences exigées dans le domaine de la sécurité de l'information. Connaître un minimum les bonnes pratiques du domaine pour évaluer les mesures en place est essentiel. Cet exercice devrait être réalisé idéalement par un expert du domaine.

Une fois la vulnérabilité évaluée, les 3 paramètres du risque sont renseignés, la valeur du risque est calculée, et en fonction du seuil d'acceptation du risque, une indication sous forme de code tricolore (Vert, Orange, Rouge) indique si le niveau de risque est acceptable ou non. Le Rouge indiquant clairement que le risque est inacceptable et doit faire l'objet de recommandation(s) pour le traiter.

Traitement des risques

Le traitement des risques consiste à choisir parmi les 4 solutions suivantes :

- Acception du risque : le risque est accepté tel quel, sans aucune mesure additionnelle.
- Réduction du risque : des mesures additionnelles sont mises en place pour réduire le risque à une valeur acceptable
- Partage du risque : cas de la souscription à une assurance, par exemple.
- Refus du risque : la source du risque est éliminée à la base.

Le traitement de « réduction du risque » est le plus utilisé. Comme les risques identifiés par défaut sont basés sur l'absence de bonnes pratiques en sécurité de l'information, MONARC propose pour chacun d'eux, une à trois mesures de sécurité issues du catalogue de bonnes pratiques d'ISO/IEC 27002[10].

Pour chaque risque, il faut estimer l'efficacité des mesures à mettre en place. Cela permet d'évaluer le risque résiduel, c'est-à-dire le risque qui subsiste après avoir mis en place les nouvelles mesures de sécurité.

L'analyse des risques est terminée.

5 Analyse d'impact relative aux risques de l'information

Comme déjà décrit précédemment, une analyse des risques de l'information se concentre sur les intérêts de l'organisme et principalement sur les conséquences que peut avoir une perte de confidentialité, d'intégrité ou de disponibilité (CID) sur la réputation, l'opération, le légal ou les finances de l'organisme.

L'analyse d'impact à la personne se focalise sur la personne et les conséquences que peuvent avoir une perte de confidentialité, d'intégrité ou de disponibilité sur les droits et libertés de celle-ci.

Pour réaliser l'analyse d'impact relative aux risques de l'information, il suffit alors de :

- S'appuyer sur l'analyse des risques de l'information.
- Paramétrer les impacts à la personne.

[10] ISO/IEC 27002 : Technologies de l'information - Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information Information technology — Security techniques.

Pour le calcul des risques, MONARC prend en considération les impacts les plus élevés. Ce qui devrait être naturellement le cas, si une analyse d'impact est requise.

6 Analyse d'impact relative à la conformité juridique

6.1 Personnalisation du modèle de base

L'analyse d'impact relative à la conformité juridique vise à contrôler que le non-respect d'exigences du GDPR relatives aux droits de la personne ou que le traitement lui-même n'a pas un impact élevé sur les droits et libertés de celle-ci. Si c'est le cas, des mesures adéquates doivent être mises en place pour en réduire les risques.

Par défaut, il existe dans MONARC une checklist organisée par thèmes qui reprend les points essentiels d'exigences énoncées dans le GDPR :

- Deux catégories sont relatives à l'organisme, elles n'apparaissent donc qu'une seule fois dans l'analyse :
  - Gouvernance : Concerne la tenue du registre des traitements, la prise en considération du « Privacy by design » et du « Privacy by default », l'étude de technique telle que la pseudonymisation ou le chiffrage, etc.
  - DPO : Concerne les points d'exigences quant à la nécessité de désigner un DPO et de ses compétences et qualités minimums.

- Sept catégories sont relatives aux traitements, elles sont répétées autant de fois qu'il y a de traitements.
  - Principes relatifs au traitement : Concerne la finalité, la transparence, la collecte excessive, etc.
  - Licéité et légitimité : Concerne les conditions de licéité, la collecte du consentement, les catégories particulières de données, etc.
  - Droits de la personne : Concerne tous les droits de la personne concernée (information, accès, rectification, effacement, limitation, portabilité et opposition).
  - Catégories de données : Concerne la liste des catégories de données intervenant dans le traitement.
  - Sous-traitant : Concerne les garanties de sécurité, la coopération, la sous-traitance en cascade, etc.
  - Destinataires : Concerne les clauses contractuelles et la finalité du traitement.
  - Transfert hors UE : Concerne la protection de données, les clauses de transferts, etc.

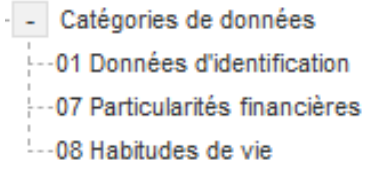
Il faut bien noter que toutes ces informations sont paramétrables et modifiables à souhait. La checklist n'est qu'un point de départ qui permet de démarrer le contrôle de la conformité des traitements. En fonction de la granularité désirée, la liste doit considérer le contexte et s'adapter aux besoins de l'entreprise.

L'expérience montre que la liste proposée par MONARC permet de gagner beaucoup de temps en se focalisant pragmatiquement sur l'essentiel. C'est une base de départ qui, une fois évaluée donne une idée assez précise sur l'état de la conformité d'un point de vue juridique. En fonction de cela, il faut se focaliser sur les points faibles, pour ensuite adapter l'exhaustivité du modèle en fonction de la sensibilité des traitements.

La liste proposée par MONARC évolue au fur et à mesure de son utilisation, il est déjà possible d'en trouver plusieurs variantes qui sont intégrables dans l'analyse grâce aux fonctions d'import/export de modèles. Dans les grandes lignes, les catégories citées ci-dessus peuvent prendre des formes différentes, sachant que le fond reste plus ou moins le même.

Hors des considérations de langages ou de formes et en fonction du contexte, il est possible de créer une variante qui rend le modèle plus détaillé et lisible. Elle consiste pour les catégories de données, les sous-traitants et les destinataires (qui peuvent être multiple) de ne pas qualifier globalement les 3 thèmes et d'utiliser le texte libre pour les lister et les décrire, mais de créer des objets MONARC pour chacun d'eux.

En d'autres termes, si l'on prend pour exemple les catégories de données, l'exercice consiste à créer dans la bibliothèque MONARC un objet de type « Durée de conservation » dont le nom est la catégorie de donnée :



Dans l'exemple ci-dessus, le traitement utilise 3 catégories de données : les données d'identification, le données financières et les habitudes de vie. Pour chacun de ces 3 objets, le modèle va demander de définir la durée de conservation.

L'avantage principal de cette modélisation est la centralisation d'une liste définie de catégories de données propres à tous les traitements. L'utilisation d'une liste personnelle ou d'une liste proposée par l'organisme de contrôle n'est qu'une affaire de choix. À ce jour, il en existe déjà quelques-unes et bien sûr elles sont similaires les unes des autres.

La même adaptation est possible avec les sous-traitants. Plutôt que d'avoir une catégorie générique dans laquelle les aspects de sous-traitance sont décrits globalement, il faut créer un objet par sous-traitant, nommé en conséquence et ayant le tag risque opérationnel « sous-traitant ». La qualification de chaque point de conformité en rapport avec les sous-traitants est de ce fait plus précise.

Il en va de même pour les destinataires. La gestion est rigoureusement identique à la gestion des sous-traitants, le tag est différent. À noter que si une société est à la fois sous-traitante et destinataire pour deux traitements différents, il faut créer deux instances de celle-ci.

Il n'y a pas vraiment de règles qui permettent de définir le bon modèle pour un contexte donné. Tout dépend de la complexité de l'environnement (nombre de fournisseurs par exemple), de la granularité désirée et de l'importance donnée à MONARC dans les preuves de conformité.

6.2 Évaluation des impacts

Le modèle de la checklist est maintenant défini. Il faut évaluer chaque point de conformité dans la terminologie MONARC : évaluer les risques d'impact induits par chacune des non-conformités.

L'évaluation de la checklist est réalisée dans la partie risques opérationnels de MONARC. Avant de la commencer, il faut éventuellement considérer l'option d'utiliser ou non les risques « Bruts ».

Explications des notions de risque « Net », « Visé » et « Brut » :

- Le risque « Net » représente le risque actuel en considérant les mesures déjà en place.
- Le risque « Visé » (ou résiduel) représente le risque tel qu'il sera après avoir mis en place les recommandations formulées
- Le risque « Brut » représente le risque, si aucune mesure n'existait.

Le choix d'utiliser le risque « Brut » est une option. Si effectivement, le traitement est déjà en place, il est possible que cette option soit superflue. Par contre, si l'on considère des cas de mise en œuvre du « Privacy by Design » sur un projet novateur, il est très probable que cette notion de risques bruts soit pertinente. Cette notion est également pertinente pour certains secteurs d'activités au Luxembourg.

Dans la partie risques opérationnels, le calcul du risque se fait en fonction de la vraisemblance du scénario de risque et des impacts ROLFP cités précédemment. La grille de saisie étant fixe, il faut se focaliser sur l'impact à la personne, seule la colonne « P » impact à la personne est à renseigner.

La méthode de remplissage reste quasiment identique à ce qui a été fait dans les risques de l'information, après évaluation de la vraisemblance du scénario et de l'impact à la personne. Le risque est calculé et la situation de risques doit avoir été décrite de façon factuelle. Si le risque de non-conformité est trop grand, il faudra alors le traiter en proposant des recommandations pour mettre en œuvre des mesures qui vont réduire la vraisemblance ou réduire l'impact à la personne. Pour les risques opérationnels, cette granularité est au niveau de chaque risque. Cela permet une meilleure mise en contexte.

7 Analyse d'impact relative aux risques opérationnels (métiers et organisation)

Il reste éventuellement une catégorie de risques qui n'a pas été traitée. Ce sont les risques métier ou les risques propres au traitement de données qui font l'objet de l'analyse d'impact. Ce sont généralement des risques stratégiques ou organisationnels qui peuvent impacter la personne concernée, par exemple, suite à une défaillance dans un workflow de données, ou l'absence de décision ou des incompatibilités dans les opérations de traitements.

À ce niveau, aucune base de connaissances n'existe, les risques sont trop liés au contexte. Par contre, toutes les étapes précédentes vont servir de support.

7.1 Utilisation des modèles de l'analyse des risques

Les risques métiers se paramètrent sur le modèle de risques de l'information au niveau des actifs primaires. Si le modèle « par service » ou « par processus » a été choisi, il est fort probable qu'aucun nouvel objet ne soit à créer. La vue processus est de loin la plus adaptée dans ce contexte. Un organisme qui a la connaissance de ses processus a sans aucun doute la maturité pour décrire les risques métiers.

Si l'analyse est réalisée dans un objectif de « Privacy by Design » la tâche est plus compliquée.

Dans tous les cas, il est très aisé de créer des conteneurs représentant des processus, des services ou des opérations de traitements qui présentent des risques particuliers.

Pour créer des risques, deux solutions :

- Créer des risques uniques à la volée sur chacun des objets
- Créer des « Tags - Risques opérationnels » puis affecter les objets à ces tags, car certains risques sont les mêmes pour plusieurs traitements ou opérations de traitement.

Note : Ne pas oublier de formuler négativement les risques opérationnels en fonction de l'absence de bonnes pratiques, de niveau de sécurité inadéquat, de ressources insuffisantes, de lacunes de traitement, etc. Cette formulation permet d'évaluer le scénario sur une échelle de 1 à n, sachant que plus la valeur est grande, plus le scénario est plausible.

7.1 Évaluation des impacts

L'évaluation et le traitement des risques métiers se font exactement de la même façon que pour la checklist des aspects légaux, avec ou sans le paramétrage des risques « Bruts ».

Concernant la conformité au GDPR, seule la colonne « P » impact à la personne est à renseigner. Si l'analyse sert également pour l'analyse des risques de l'organisme, les colonnes ROLF sont également à renseigner, MONARC prend en considération l'impact le plus grand.

8 Finalisation, preuves et itérations

8.1 Plan de traitement consolidé : liste des mesures à mettre en place

Que ce soit pour l'analyse des risques de l'information, ou les 3 types d'analyses d'impacts, toutes les recommandations formulées pour traiter les risques importants et les non-conformités sont regroupées dans un seul et unique plan de traitement.

D'un point de vue visibilité et transparence, le plan de traitement est primordial, car il permet de centraliser toutes les actions à mettre en œuvre pour être en conformité. Le plan est intégralement retranscrit dans le livrable final.

MONARC permet également de suivre la mise en œuvre du plan de traitement, d'y ajouter le nom des personnes responsables, des délais accordés, des commentaires divers qui documentent la bonne exécution des toutes les actions de mises en conformité.

8.2 Résultats et preuves

Actuellement, le livrable fourni par MONARC est orienté analyse des risques et n'est pas directement adapté pour délivrer les éléments pertinents à une analyse d'impact. Dans tous les cas, les informations sont livrées déjà formatées dans Microsoft Word, ce qui permet une personnalisation rapide et aisée du livrable.

MONARC est un logiciel « Open source », il est fort probable qu'un livrable dédié au GDPR soit programmé à terme.

De mon expérience pour des certifications en sécurité de l'information, le choix de proposer directement un accès à l'analyse MONARC à l'auditeur rend les contrôles plus faciles et plus rapides. Il induit un sentiment de transparence toujours bienvenu lors d'un audit.

8.3 Itération

MONARC est un outil qui met en œuvre une gestion itérative des risques. Il va donc naturellement mettre à jour vos analyses périodiquement dans le respect de la DPIA, qui rappelons-le, est un processus.

9 Conclusion

La réalisation d'une analyse d'impact nécessite une double compétence : c'est un projet de juriste et un projet de sécurité de l'information. Deux mondes, deux approches différentes, mais des compétences complémentaires indispensables.

C'est bien toute la problématique des outils qui visent à assister un projet de conformité. La plupart des outils du marché sont en réalité des checklists généralistes de points de conformité, ce qui ne convient pas du tout au domaine de la gestion des risques bien trop complexe pour être modélisé dans une table bidimensionnelle comme Excel.

L'avantage de MONARC réside dans le fait qu'il est conçu pour gérer les risques de l'information et les risques opérationnels. Il intègre « By Design » la notion d'impact à la personne et des checklists de conformité.

Un bon compromis, de surcroit gratuit qu'il faut adopter.

Thierry Petitgenet, consultant en GRC (Gouvernance, Risques et Conformité)

Fondateur de GRC-Luxembourg.

www.GRC-Luxembourg.lu