cases.lu
Secure. Innovate. Lead.

MÉTHODE OPTIMISÉE D'ANALYSE DES RISQUES

Modèles de risques personnalisables

Gouvernance simplifiée basée sur les risques

Adaptation plus rapide aux normes et aux lois actuelles

Génération automatique de rapports

F

SOMMAIRE

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

SECURITY
MADEIN.LU

MONARC,
Méthode Optimisée d'Analyse des Risques

CASES[1] promeut la sécurité de l'information par l'adoption de mesures comportementales, organisationnelles et techniques. Acquérir les bons réflexes, adopter les bonnes pratiques, prendre les mesures nécessaires et les adapter de façon proportionnelle : tout cela fait partie des responsabilitées qui incombent à une organisation, peu importe sa taille, pour assurer une bonne sécurité de l'information. Mais la sécurité se gère avant tout par le biais d'une analyse des risques, réalisée de façon régulière.

Bien que la rentabilité de l'approche par analyse de risques soit garantie, l'investissement que représente cette démarche en termes de coûts et savoir-faire nécessaire constitue un obstacle pour beaucoup d'organisations, surtout les PME.

Pour remédier à cette situation et faire profiter toutes les entités, petites et grandes, des avantages de l'analyse des risques, CASES a développé une méthode optimisée d'analyse des risques : MONARC (Méthode Optimisée d'Analyse des Risques CASES), permettant une gestion précise et itérative des risques.

L'avantage de MONARC réside dans la capitalisation des analyses des risques déjà réalisées dans des contextes métiers similaires : les mêmes vulnérabilités apparaissent régulièrement dans de nombreuses entreprises, celles-ci sont confrontées à des menaces identiques et engendrent des risques de même nature. La plupart des sociétés possèdent des serveurs, des imprimantes, une flotte de smartphones, des antennes wi-fi, etc. dont les vulnérabilités et menaces sont les mêmes. Il suffit dès lors de généraliser des scénarios de risques[2] de ces actifs[3] (aussi appelés objets) par contexte et/ou métier.

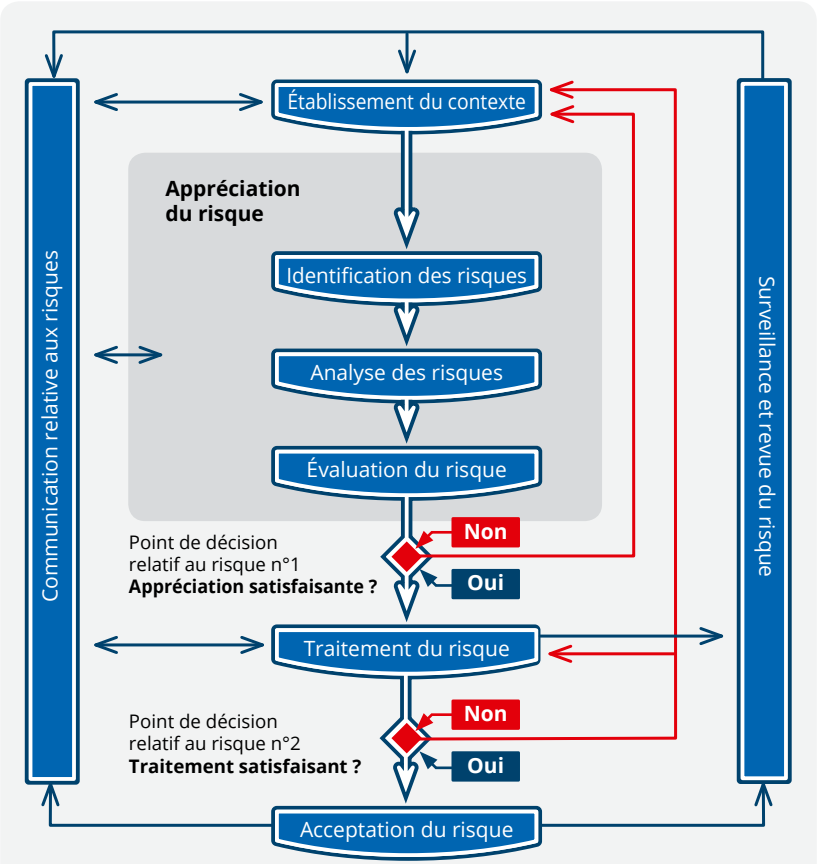
[1] CASES : Cyberworld Awareness and Security Enhancement Services : www.cases.lu

[2] Un scénario de risques est une liste plus ou moins complète de menaces et de de vulnérabilités correspondant à un actif ou à un groupe d'actifs.

[3] Actifs = ensemble des éléments matériels et immatériels qui jouent un rôle dans les activités d'une entité.

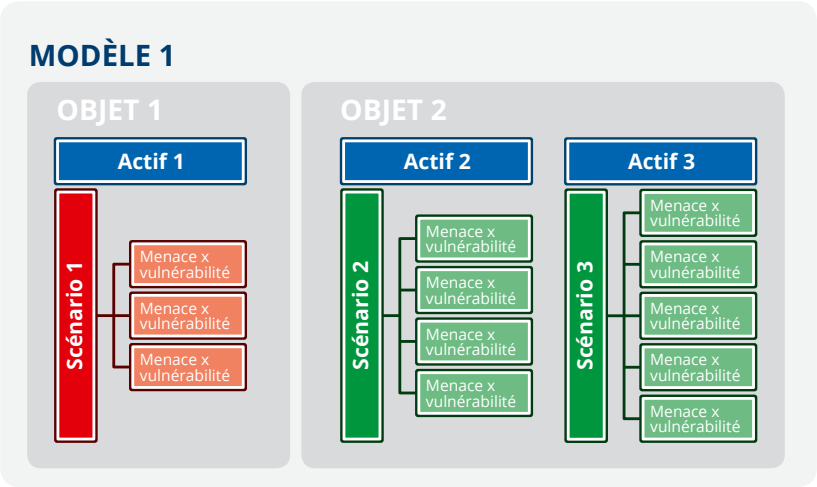
Introduction – modélisation des risques

MONARC simplifie la gestion des risques en proposant une solution de gestion des risques, et même de gouvernance de la sécurité de l'information, basée sur l'état de l'art du domaine. Elle permet de réaliser en peu de temps une analyse à partir de modèles existants et personnalisables, tout en restant conforme avec la norme internationale ISO/IEC 27005:2011.



Itération finale, première itération ou itérations ultérieures

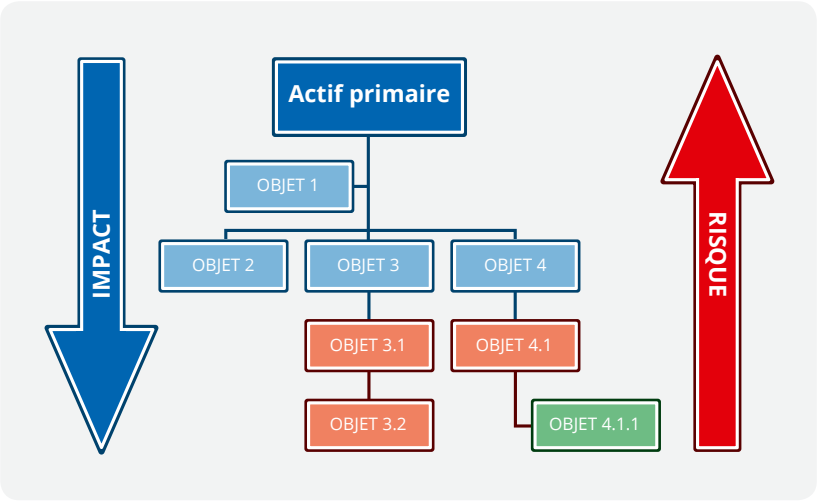
MONARC s'appuie sur une bibliothèque de modèles de risques proposant des objets composés de scénarios de risques par actifs ou groupes d'actifs. Cette approche facilite la gestion des risques les plus courants et permet de gagner en objectivité ainsi qu'en efficacité. MONARC étant complètement itérative, ces résultats peuvent être approfondis et ajustés à la maturité de chaque organisation en augmentant la granularité des scénarios de risques.



L'analyse des risques est faite en décrivant les actifs primaires (processus métiers ou informations selon la norme ISO/IEC 27005:2011) et en y associant des objets modélisant les risques prédéfinis en cascade, c'est-à-dire en construisant un arbre d'objets. L'impact est défini au niveau le plus haut et hérité dans tous les objets de risques vers le bas pour faire le calcul du risque :

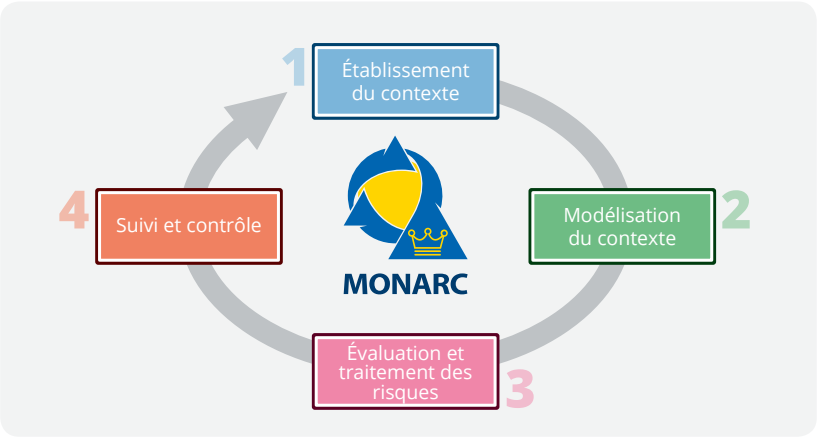
Risque = Menace x Vulnérabilité x Impact.

Les autres aspects (menaces et vulnérabilités) des risques sont calculés au niveau de chaque objet et escalés vers l'actif primaire, qui regroupe tous les risques identifiés avec leurs estimations.

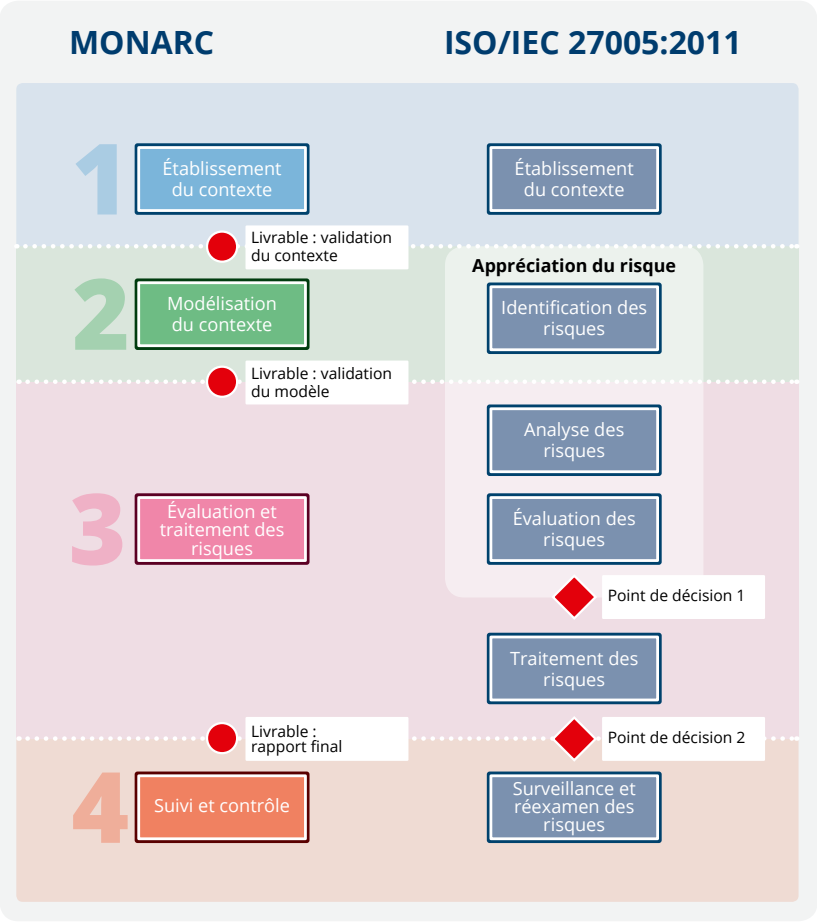


Parmi les modèles de risques proposés, on trouve l'aide à la mise en conformité de certaines normes et lois en vigueur, en particulier, le règlement européen pour la protection des données à caractère personnel (GDPR), la certification ISO/IEC 27001 ou encore la norme PCI-DSS. Ces modèles sont partageables à discrétion et chaque utilisateur de la communauté MONARC peut concevoir, améliorer et partager ses propres expériences pour plus d'efficacité face aux risques.

La méthode se déroule en 4 phases

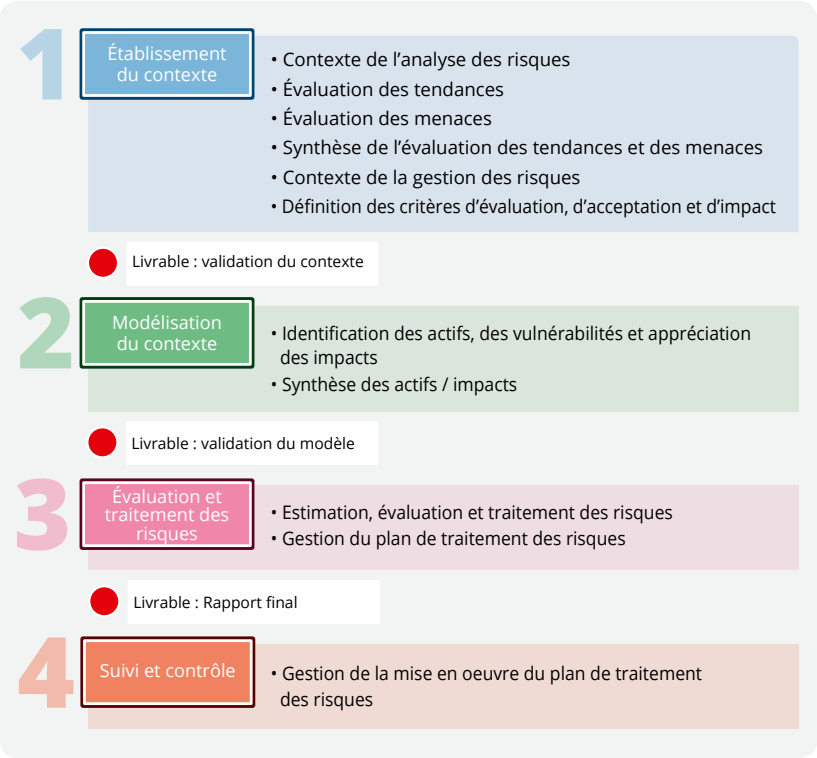


A chaque itération complète, l'analyse peut être approfondie, avec un niveau de détail et d'exigence plus élevé. Les 4 phases de MONARC respectent entièrement la norme internationale ISO/IEC 27005:2011 qui décrit les lignes directrices relatives à la gestion des risques liés à la sécurité de l'information. Un comparatif avec MONARC est visualisé sur la Figure 2.



Chaque phase livre un rapport, qui formalise les décisions et résultats obtenus.

Résumé de la méthode



Le fait de pouvoir choisir le niveau d'exhaustivité (périmètre, granularité, scénarios d'attaques/scénarios de risques) en fonction de la maturité de l'organisme, représente également un élément important d'optimisation de l'approche MONARC. Même si à première vue, cette approche peut sembler écarter certains aspects, il ne faut pas oublier qu'elle est conçue comme une solution pragmatique et itérative pour répondre aux besoins de tout type d'organisme. De cette manière, les entités à maturité faible ou disposant de peu de ressources financières ou humaines, ont la possibilité de choisir un niveau de sécurité initial peu élevé et adapté à leurs savoir-faire et moyens financiers. Elles peuvent ensuite l'améliorer graduellement.

Grâce à sa grande flexibilité, MONARC peut non seulement intégrer des niveaux de granularité différents, mais aussi réduire le nombre de risques à traiter dans une 1ère itération. Cette approche améliore nettement la rapidité, l'efficacité, l'accessibilité et l'acceptation de l'analyse des risques.

Se basant sur la norme ISO/IEC 27005:2011 et s'inspirant des bases de connaissances d'EBIOS et de l'expérience recueilli par CASES, l'approche MONARC profite des méthodes éprouvées, et les adapte aux besoins réels des entreprises et autres organismes pour ainsi réduire la complexité et les coûts d'une analyse des risques.

La modélisation MONARC inclue les concepts suivants :

- **L'étendue de l'analyse des risques** – que faut-il prendre en compte ?
    - La liste des actifs primaires ainsi que les impacts causés par une perte de confidentialité, d'intégrité ou de disponibilité.
- **La granularité de l'analyse des risques** – quel niveau de détail faut-il exiger ?
    - La liste des actifs secondaires.
    - La liste des menaces qui doivent être associées aux actifs secondaires ainsi que les probabilités de ces menaces.
    - La liste des vulnérabilités qui doivent être associées aux actifs secondaires ainsi que l'aisance d'exploitation de ces vulnérabilités.
- **Les traitements des risques autorisés** ainsi que leur efficacité maximale.
- **Le seuil des risques acceptables** (grille d'acceptation des risques).

PHASE 1 - Définition du contexte

Cette 1ère étape vise à faire le point sur le contexte, les enjeux et les priorités propres à l'entreprise ou l'organisation qui désire analyser ses risques. Il s'agit d'identifier notamment les activités essentielles et les processus critiques de l'entreprise, afin d'orienter l'analyse des risques vers les éléments les plus importants. Pour ce faire, un kick-off meeting est organisé avec les membres du management et les personnes clés. L'objectif est de savoir ce qui fait vivre l'entreprise et ce qui pourrait la détruire, d'identifier les processus-clés, les menaces internes et externes, les vulnérabilités organisationnelles, techniques et humaines.

1) **Contexte de l'analyse des risques** : collecte de toutes les informations relatives à l'organisation permettant de définir le périmètre et les limites de l'analyse des risques. Dans cette phase, certains éléments pourront être exclus de l'analyse des risques (moyennant justification). L'environnement du marché et son impact prévisible sur l'évolution de l'organisation sera pris en compte afin de tracer les scénarios en termes d'évolution des vulnérabilités et des attaques probables.

2) **Définition des critères d'évaluation, d'acceptation et d'impact** : MONARC utilise une méthode d'évaluation qualitative. Les vulnérabilités, menaces et impacts sont estimés sur une échelle de 0 à 4. Il faut ensuite définir une grille d'acceptation des risques, c'est-à-dire définir une valeur maximale du risque (R = M x V x I) à partir de laquelle celui-ci ne pourra plus être accepté et devra être traité.

   Par exemple si R > ou = 18, le risque devra être traité.

3) MONARC propose des échelles d'estimation des menaces, vulnérabilités et impacts prédéfinies, qu'il est possible d'adapter selon les besoins de l'entreprise. On pourra notamment adapter la probabilité d'occurrence des menaces par rapport à une exposition accrue ou réduite ou ajuster la qualification des vulnérabilités en fonction des mesures de sécurité en place. Le niveau d'impact direct en termes de confidentialité, intégrité et disponibilité et leurs conséquences adjacentes sur le business peuvent être définis par actif primaire (les coûts pour l'organisation, les atteintes à la réputation, les dommages sur la vie privée, les conséquences judiciaires, etc.)

Avantage :
la réutilisation d'objets préconçus donne à l'analyse des risques une objectivité supérieure, puisque la liste des actifs, des menaces et vulnérabilités à prendre en considération a été sélectionnée par des experts externes à l'entité et sont valides pour tout un contexte. Cette approche promeut également l'échange d'expériences et la réalisation de benchmarks contextuels à l'essor des essais interlaboratoires.

PHASE 2 - Modélisation des risques

Cette phase comprend la modélisation des arbres d'objets et est finalisée par un rapport qui doit être validé par la direction.

1) Identification des actifs

Les actifs ont été définis dans la phase précédente. Ils doivent maintenant être détaillés et formalisés dans un schéma qui représente leurs interdépendances.

Un actif primaire désigne un service, un processus ou une information.

Un actif secondaire est un élément de support à un actif primaire (comme p.ex. le serveur de fichiers).

Identifier les actifs d'une organisation est une étape essentielle et tout ce qui a de la valeur pour l'entité devrait y figurer. Cependant, il n'est pas opportun de commencer la première analyse des risques avec une liste exhaustive d'actifs primaires et secondaires en considérant tous les scénarios de risques imaginables. Le choix de la granularité doit être fait en fonction du nombre et de l'importance des actifs primaires et secondaires, ainsi que du nombre d'itérations déjà réalisées (on aura davantage de détails à la 3ème itération qu'à la 1re).

Notons qu'il n'est pas nécessaire d'avoir une liste complète de tous les actifs. Il faut garder les principes de la proportionnalité et de la nécessité en tête.

2) Identification des vulnérabilités

L'identification des menaces et vulnérabilités est réalisée au travers des « objets MONARC ». Ici, on peut encore une fois décider du niveau de granularité désiré, soit en optant pour des risques affectant l'organisation et exploitant des vulnérabilités communes, soit en descendant plus profondément dans l'expertise technique.

3) Évaluation des impacts

Les impacts sont définis au niveau des actifs primaires (processus ou informations), en respectant les informations collectées lors de la phase de l'établissement du contexte. Les actifs secondaires héritent de l'impact de l'actif primaire auquel ils sont rattachés (arbre d'objets). Il est possible de modifier manuellement les impacts au niveau des actifs secondaires.

Le gestionnaire des risques construit l'arbre de risques en liant des objets MONARC préconçus aux actifs primaires. Ainsi, il a recours à des actifs et scénarios de risques associés, conçus par des experts externes, correspondant au niveau de maturité visé par l'entité.

Le gestionnaire des risques n'a pas besoin de rechercher tous les scénarios de risques pertinents, mais peut se fier aux scénarios déjà répertoriés par des experts.

Avantage :
Le responsable de la sécurité peut proposer des objets (listes de scénarios de risques prédéfinis) et veiller à ce que chaque département utilise les mêmes objets et se conforme à une seule taxonomie. Ainsi, il va pouvoir comparer les différentes analyses faites dans le département et même les lier dans une analyse « corporate ». Il peut aussi faire progresser la granularité en ajoutant des actifs et des scénarios supplémentaires correspondants. Par exemple, lors de l'émergence de nouvelles menaces.

PHASE 3 - Évaluation et traitement des risques

Calcul du risque / seuil

IMPACT \ M x V	0	1	2	3	4	6	8	9	12
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	6	8	9	12
2	0	2	4	6	8	12	16	18	24
3	0	3	6	9	12	18	24	27	36
4	0	4	8	12	16	24	32	36	48

$$\sum R = M \times V \times I$$

R = Risque · **M** = Menace · **V** = Vulnérabilités **I** = Impact

L'évaluation consiste à chiffrer les menaces, les vulnérabilités et les impacts pour calculer les risques.

Pour ce faire, il est nécessaire d'avoir des informations de qualité sur la vraisemblance exacte des menaces, l'aisance d'exploitation des vulnérabilités et les impacts potentiels... D'où l'intérêt de se fier à des métriques qui ont été validées par des experts.

Lorsque l'évaluation des risques identifie un risque supérieur au niveau acceptable (grille d'acceptation des risques), des mesures de traitement de ce risque doivent être mises en place pour réduire le risque à un niveau acceptable.

1) **Estimation, évaluation et traitement des risques** : appréciation qualitative de la probabilité d'occurrence des menaces et qualification des vulnérabilités par rapport aux actifs modélisés. Le calcul du niveau de risque est systématiquement calculé sur la base de la formule suivante :

Risque = **M**enace x **V**ulnérabilité x **I**mpact

La méthode permet de trier les risques en ordre ascendant ou descendant en fonction de plusieurs critères, par exemple, le niveau de risque, l'impact, la probabilité des menaces, etc. Ceci permet de comparer les niveaux de risques par rapport au seuil d'acceptation.
Le traitement des risques peut suivre les quatre types de traitement proposés dans la norme ISO/IEC 27005:2011 modification, refus, acceptation et partage.

2) **Gestion du plan de traitement des risques** : hiérarchisation des recommandations selon leur niveau d'importance et les priorités de l'organisation. Une table interactive est mise à disposition pour favoriser la gestion du plan de traitement.

3) **Rapport final :** génération du livrable final qui présente les résultats et toutes les informations relatives à l'analyse des risques.

PHASE 4 - Suivi et contrôle

Lorsque le premier traitement des risques a été réalisé, il faut entrer dans une phase de gestion continue de la sécurité avec un suivi et un contrôle récurrent des mesures de sécurité, afin de pouvoir améliorer celles-ci de façon durable.

Cette 4ème phase permet aussi d'optimiser continuellement la sécurité en augmentant la granularité des objets utilisés respectivement en élargissant l'étendue de l'analyse des risques.

Avantage :
Le responsable de la sécurité sera en mesure de fixer des probabilités minimales ou maximales pour certaines menaces. Il pourra également déterminer l'aisance d'exploitation de certaines vulnérabilités.

Gouvernance

MONARC offre plusieurs possibilités de gouvernance :

- Adaptation des impacts pour la perte de confidentialité, d'intégrité ou de disponibilité pour certains domaines d'activités, respectivement certains actifs primaires.
- Adaptation des grilles d'acceptation des risques.
- Adaptation des profils d'exigences en ajoutant ou en retirant des domaines d'activité.
- Adaptation des profils d'exigences en offrant différents niveaux de maturité (granularité).
- Adaptation des matrices d'exigences en changeant les référentiels d'exigences (facteurs endogènes comme actifs, menaces, vulnérabilités et mesures).

De nouvelles bibliothèques de modèles peuvent être ajoutées en cours de route, selon les besoins.

Enfin, MONARC possède une communauté d'utilisateurs qui permet de renforcer la performance d'une analyse des risques par des échanges d'expériences.

Club MONARC

Le Club MONARC rassemble les utilisateurs de la méthode MONARC. Il permet des rencontres à intervalles réguliers afin d'échanger les expériences et de faire progresser l'outil. Les utilisateurs pourront également travailler ensemble sur des bibliothèques communes d'objets.

Le Club MONARC leur donnera en outre un accès privilégié aux évènements organisés par SECURITYMADEIN.LU et leur permettra d'apparaître dans l' « Ecosystème » de la cybersécurité, afin de souligner leur démarche qualitative.

www.cases.lu
services@cases.lu

cases.lu
cyberworld awareness and
security enhancement services
LUXEMBOURG

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

SECURITY
MADEIN.LU