

# **METHODOLOGIE D'ANALYSE DES RISQUES MARION**

La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) est issue du CLUSIF (<http://www.clusif.asso.fr/>) et la dernière mise à jour date de 1998.

Il s'agit d'une méthodologie d'audit, qui, comme son nom l'indique, permet d'évaluer le niveau de sécurité d'une entreprise (les risques) au travers de questionnaires pondérés donnant des indicateurs sous la forme de notes dans différents thèmes concourant à la sécurité.

## **Objectif de la méthode**

L'objectif est d'obtenir une vision de l'entreprise auditée à la fois par rapport à un niveau jugé " correct ", et d'autre part par rapport aux entreprises ayant déjà répondu au même questionnaire.

Le niveau de sécurité est évalué suivant 27 indicateurs répartis en 6 grands thèmes, chacun d'eux se voyant attribuer une note de 0 à 4, le niveau 3 étant le niveau à atteindre pour assurer une sécurité jugée correcte.

À l'issue de cette analyse, une analyse de risque plus détaillée est réalisée afin d'identifier les risques (menaces et vulnérabilités) qui pèsent sur l'entreprise.

## **Fonctionnement de la méthode**

La méthode est basée sur des questionnaires portant sur des domaines précis. Les questionnaires doivent permettre d'évaluer les vulnérabilités propres à l'entreprise dans tous les domaines de la sécurité.

L'ensemble des indicateurs est évalué par le biais de plusieurs centaines de questions dont les réponses sont pondérées (ces pondérations évoluent suivant les mises à jour de la méthode).

Les thèmes sont les suivants :

- Sécurité organisationnelle
- Sécurité physique
- Continuité
- Organisation informatique
- Sécurité logique et exploitation
- Sécurité des applications

## **Déroulement de la méthode**

La méthode se déroule en 4 phases distinctes :

### **Phase 0 : Préparation**

Durant cette phase, les objectifs de sécurité sont définis, ainsi que le champ d'action et le découpage fonctionnel permettant de mieux dérouler la méthode par la suite.

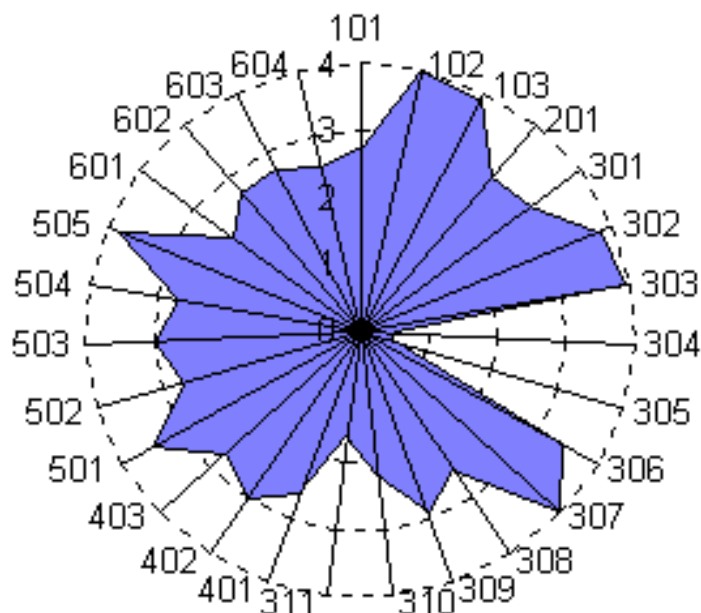
## Phase 1 : Audit des vulnérabilités

Cette phase voit le déroulement des questionnaires ainsi que le recensement des contraintes propres à l'organisme.

Le résultat des questionnaires permet d'obtenir la " rosace " propre à l'entreprise.

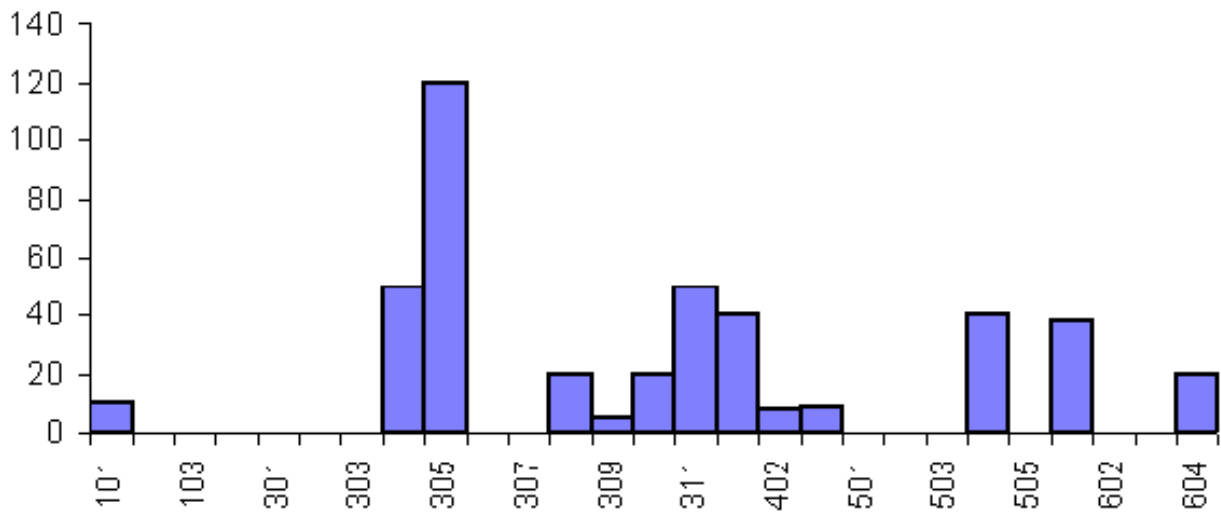
Cette rosace, l'aspect le plus connu de la méthode, présente les 27 indicateurs sur un cercle, avec le niveau atteint. Cela permet de juger facilement et rapidement des domaines vulnérables de l'entreprise, la cohérence et l'homogénéité des niveaux de sécurité des différents indicateurs, et donc d'identifier également rapidement les points à améliorer.

### Exemple de rosace MARION

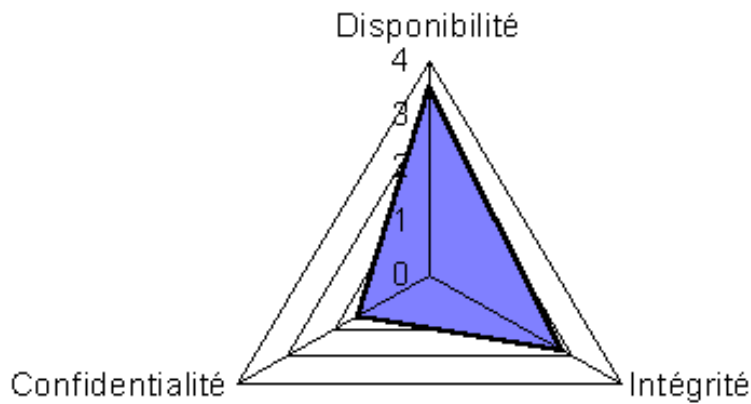


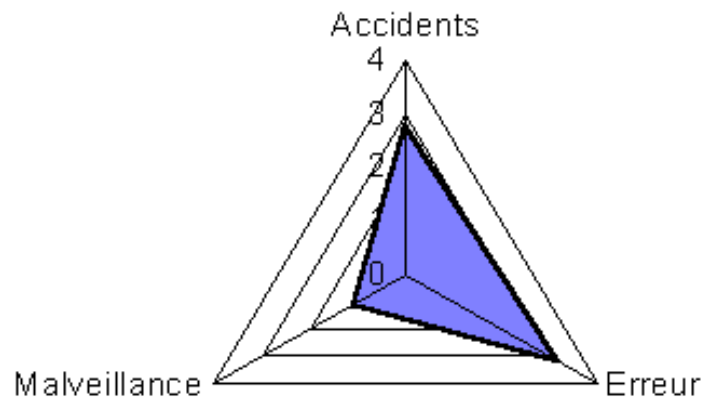
D'autres possibilités de diagrammes existent, parmi lesquels le diagramme différentiel qui permet de mieux comprendre l'importance des différents facteurs (d'après la méthode) et donc également de mettre les vulnérabilités de l'entreprise en perspective. Dans ce diagramme, chaque barre est proportionnelle à la différence entre la cotation 3 et la cotation réelle de l'existant, multipliée par le poids du facteur (le différentiel est nul si le facteur est déjà supérieur à 3)

## Diagramme différentiel



Enfin, il est également possible d'afficher des diagrammes suivant les types de risques.





## Phase 2 : Analyse des risques

Cette phase voit l'exploitation des résultats précédents et permet d'effectuer une ségrégation des risques en Risques Majeurs (RM) et Risques Simples (RS).

Le Système d'Information est alors découpé en fonctions qui seront approfondies en groupes fonctionnels spécifiques, et hiérarchisés selon l'impact et la potentialité des risques les concernant.

En ce qui concerne l'analyse de risque, MARION définit 17 types de menaces :

- Accidents physiques
- Malveillance physique
- Panne du SI
- Carence de personnel
- Carence de prestataire
- Interruption de fonctionnement du réseau
- Erreur de saisie
- Erreur de transmission
- Erreur d'exploitation
- Erreur de conception / développement
- Vice caché d'un progiciel
- Détournement de fonds
- Détournement de biens
- Copie illicite de logiciels
- Indiscrétion / détournement d'information
- Sabotage immatériel
- Attaque logique du réseau

Pour chaque groupe fonctionnel de l'entreprise, chaque fonction est revue en détail afin d'évaluer les scénarios d'attaque possible avec leur impact et leur potentialité.

## **Phase 3 : Plan d'action**

Durant cette ultime phase de la méthode, une analyse des moyens à mettre en oeuvre est réalisée afin d'atteindre la note " 3 ", objectif de sécurité de la méthode, suite aux questionnaires. Les tâches sont ordonnancées, on indique le degré d'amélioration à apporter et l'on effectue un chiffrage du coût de la mise en conformité.

## **Commentaires sur la méthode**

Les commentaires suivants pourraient être faits à la méthode :

- Bien rodée de part son âge, elle offre un moyen de comparer une entreprise par rapport au niveau sécuritaire des autres entreprises européennes.
- On regrettera par contre son manque d'utilisation qui aurait pu permettre d'améliorer la validité de l'aspect statistique des résultats. Il arrive également malheureusement trop souvent que ce comparatif par rapport à " la moyenne " s'arrête là et que les décideurs ne se contentent que de ce niveau, plutôt que de viser l'objectif " 3 ", seuil minimal de sécurité de la méthode.
- Sa démarche sous forme de questionnaire, bien qu'elle puisse être jugée lourde car longue à dérouler, en fait également une méthode facile d'application (du moins durant la phase des questionnaires, la plus connue et la plus réalisée)
- Il est regrettable que la méthode ne soit connue qu'au travers de ses rosaces, certes pratiques et figuratives, alors qu'appliquée complètement, elle permettrait aux entreprises de mieux formaliser leurs travaux de sécurité, donc de les améliorer.
- Contrairement à d'autres approches, la méthode prend en compte aussi bien les aspects techniques qu'organisationnels, ce qui est un avantage non négligeable. Les aspects techniques sont cependant peu approfondis.
- Les rosaces forment des indicateurs synthétiques clairs utilisables par la direction.
- Un gros intérêt de la méthode réside dans son approche par questionnaires exhaustifs qui, outre le recueil d'information, jouent un rôle de sensibilisation et d'information direct lors de leur déroulement.
- Enfin la méthode ne permet pas d'identifier des mesures concrètes à mettre en place pour sécuriser l'entreprise. Cependant, l'identification des risques ayant été réalisée, il devient plus facile de trouver des mesures pour les contrer.

## **Autres méthodes**

On pourra comparer MARION avec d'autres méthodes du CLUSIF, principalement MEHARI, la dernière en date, probablement vouée à remplacer MARION à terme.

D'autres approches existent, parmi laquelle la méthode EBIOS (publique) de la DCSSI (Direction centrale de la sécurité des systèmes d'information).