CARDYNAL
Utilisation de l'outil d'analyse des risques

Date : 15/10/2019 Version : 1.0 Auteur : François KAAG

Version	Date	Commentaire
1.0	15/10/2019	Version initiale

1 Objet

Ce document présente le fonctionnement de l'outil d'analyse des risques utilisé par CARDYNAL dans ses prestations.

2 Présentation générale

L'outil d'analyse est un tableur Excel implémentant une version condensée de la méthode EBIOS 2010. Il comporte les 9 onglets suivants :

Onglet	Usage
Synthèse	Vue d'ensemble des risques Historique du niveau de risque courant Boutons d'action : Calculer et Reporter
Risques	Liste des risques, de leur caractérisation et de leur criticité. Calcul des niveaux de risque résultant du croisement des risques et des scénarios
Scénarios	Liste des scénarios, de leur caractérisation et de leurs vraisemblances
ScnRisques	Liens entre les scénarios et les risques qui en résultent
Mesures	Liste des mesures de mitigation des risques, avec leur état de réalisation
ScnMes	Liens entre les mesures et les scénarios
Histoire	Liste des versions de l'analyse
Contexte	Facteurs de caractérisation des risques ou des scénarios : scopes, critères, sources, vecteurs, modes d'attaque.
Référentiel	Echelles de vraisemblance, de gravité et de risque Matrice donnant le risque pour une gravité et une vraisemblance

3 Mode opératoire

L'analyse des risques se fait de manière itérative, au fur et à mesure qu'on identifie des scénarios pouvant conduire à des événements indésirables. Les éditions se font dans tous les onglets exclusivement dans les zones de couleur bleu pâle, les autres résultats sont calculés.

- Si nécessaire, on ajoute dans l'onglet **Risques** l'événement indésirable identifié, en précisant la gravité en cas de survenue de l'événement.
- On ajoute dans l'onglet **Scénarios** le ou les scénarios identifiés, en précisant ses niveaux de vraisemblance :
    - Vi – Vraisemblance initiale, avant la mise en œuvre de mesures
    - Vc – Vraisemblance courante, avec les mesures actuellement effectives
    - Vf – Vraisemblance future, avec les mesures programmées

    En l'absence de mesures effectives, la vraisemblance courante doit être égale la vraisemblance initiale ; en l'absence de mesures programmées, la vraisemblance future doit être égale à la vraisemblance courante. Un écart à cette règle serait indiqué dans la colonne ERREUR.

- On ajoute dans l'onglet **ScnRisques** les liens signifiant qu'un scénario peut conduire au risque donné.
- Depuis l'onglet **Synthèse**, le bouton **Calculer** entraine la mise à jour du niveau résultant pour chaque risque dans l'onglet **Risques**, des décomptes et synthèses dans l'onglet **Synthèse**.
- On revient à l'onglet **ScnRisques**, qui a été trié par risque courant décroissant, puis vraisemblance de scénario décroissante et on cherche à réduire les risques de niveau le plus élevé.

- Pour les scénarios les plus vraisemblables amenant à un risque élevé, on recherche quelle mesure pourrait en réduire la vraisemblance, et on l'ajoute dans l'onglet **Mesures** à l'état Programmé (P)
- Dans l'onglet **ScnMes**, on crée le lien entre la mesure et le scénario.
- Ceci doit alors permettre dans l'onglet **Scénarios** de baisser la vraisemblance future du scénario sans provoquer d'erreur, puisqu'il existe une ou plusieurs mesures programmées impactant le scénario.

Une fois la mesure réellement mise en œuvre, on pourra :

- La passer à l'état Effective (E) dans l'onglet **Mesures**
- Reporter la vraisemblance future en vraisemblance courante dans l'onglet **Scénarios**
- Relancer le calcul depuis l'onglet **Synthèse**

4 Aides à la navigation

Des menus contextuels spécifiques sont mis en place sur les identifiants dans les tables et permettent de naviguer rapidement d'un onglet à l'autre. Ils sont appelables par un clic droit sur l'identifiant.

Onglet	Colonne	Actions
Risques	ID	Voir les scénarios liés (vue filtrée sur l'onglet ScnRisques) Faire le calcul des risques (identique au bouton Calculer)
Scénarios	ID	Voir les risques liés (vue filtrée sur l'onglet ScnRisques) Voir les mesures liées (vue filtrée sur l'onglet ScnMes) Faire le calcul des risques
ScnRisques	SCN	Aller au scénario dans l'onglet Scénarios Effacer tous les filtres de la table Faire le calcul des risques
ScnRisques	RSK	Aller au risque dans l'onglet Risques Effacer tous les filtres de la table Faire le calcul des risques
Mesures	ID	Voir les scénarios liés (vue filtrée sur l'onglet ScnMes)
ScnMes	SCN	Aller au scénario dans l'onglet Scénarios Effacer tous les filtres de la table
ScnMes	MES	Aller à la mesure dans l'onglet Mesures Effacer tous les filtres de la table

5 Méthodes de calcul

Lorsqu'un risque est associé à plusieurs scénarios de niveaux de vraisemblance courante V_c^i, la vraisemblance prise en compte pour le risque est :

$$V_c = \mathrm{E}(\log(\sum 10^{V_c^i}))$$

En d'autres termes, 10 scénarios d'un certain niveau de vraisemblance équivalent à un scénario du niveau de vraisemblance immédiatement supérieur.

La même méthode est utilisée pour les vraisemblances initiales et futures. Dans tous les cas, elle est arrondie à la valeur entière et majorée par le niveau de vraisemblance maximum.

Le niveau de risque est alors sélectionné dans la matrice vraisemblance x gravité en prenant en compte cette vraisemblance synthétique.

Dans la synthèse, on utilise une méthode similaire pour déterminer le niveau de risque global, sur un critère donné ou tous risques confondus.

$$R = \log(\sum 10^{R_i})$$

6 Détail par onglet

6.1 Synthèse

L'onglet de synthèse présente trois tables et deux boutons.

Les tables sont :

- Le nombre de risques courants par niveau, critère par critère et au total.
- Les niveaux synthétiques de risque initial, courant et futur, critère par critère et au total.
- Un tableau de l'historique du risque courant, mis à jour par une action manuelle sur le bouton Reporter.

Les deux boutons sont :

- **Calculer**, qui effectue les mises à jour de l'ensemble du tableur après qu'on ait complété les zones de saisie des risques, scénarios, mesures et liens entre ces entités.
- **Reporter**, qui insère dans l'historique du risque courant les valeurs de niveau global actuellement présentées dans la synthèse.

6.2 Risques

La table des risques comporte cinq colonnes saisies (en bleu) et six colonnes calculées.

Les colonnes saisies sont :

- **ID**, un identifiant arbitraire du risque.
- **Crit**, le critère de classification du risque. En sécurité de l'information, ce sont classiquement les critères de Disponibilité, Intégrité, Confidentialité et Preuve, mais d'autres usages peuvent être possibles, par exemple si on utilise l'outil pour une étude d'impact sur la vie privée ou l'analyse de risque d'un dispositif médical.
- **Scope** est un attribut arbitraire permettant au sein d'une analyse de catégoriser les risques, par exemple s'ils sont liés à une nouvelle fonction qu'on veut évaluer séparément avant de l'intégrer.
- **Libellé** explicite ou illustre l'événement redouté et son vecteur.
- **Gravité** représente l'impact de l'événement redouté

Les colonnes calculées sont :

- Les vraisemblances cumulées **SVi**, **SVc** et **SVf**, qui sont de simples intermédiaires de calcul. Ces colonnes pourraient être masquées, elles sont présentées en police gris pâle.
- Les niveaux de risque initial, courant et futur, respectivement **Ri**, **Rc** et **Rf** tels que calculés lorsqu'on agit sur le bouton **Calculer** de l'onglet de synthèse.

6.3 Scénarios

La table des scénarios comporte huit colonnes saisies et trois colonnes calculées. Parmi les huit colonnes saisies, trois sont des éléments de caractérisation qui permettent d'orienter la réflexion lors de la création de nouveaux scénarios ou la recherche d'un scénario existant :

- **Source** représente l'agent qui provoque le déclenchement du scénario : administrateur, autre personnel, intrus, aléa technique ou climatique, etc.
- **Vecteur** représente l'actif sur lequel le scénario s'exerce : matériel, logiciel, personne, processus, etc.
- **Mode** caractérise le type d'action mis en œuvre : mésusage ou altération, dépassement des limites de fonctionnement, perte ou vol, espionnage, etc.

Les cinq autres colonnes saisies sont l'identifiant arbitraire du scénario (**ID**), son descriptif (**Libellé**) et les trois niveaux de vraisemblance initiale (**Vi**), courante (**Vc**) et future (**Vf**) accordés à ce scénario.

Les trois colonnes calculées permettent un contrôle de cohérence. Ce sont le nombre de mesures effectivement appliquées permettant de réduire la vraisemblance du scénario (**M.Eff**), le nombre de mesures programmées ayant le même effet (**M.Prog**) et un test d'erreur (**ERREUR**) qui passera à VRAI et en rouge si les vraisemblances courante ou future décroissent sans qu'il y ait de mesures associées.

6.4 ScnRisques

Ce tableau comporte deux colonnes saisies et quatre colonnes calculées.

Les colonnes saisies sont l'identifiant d'un scénario et l'identifiant d'un risque qu'il engendre.

Les deux premières colonnes calculées sont le libellé du scénario et le libellé du risque, elles permettent de s'assurer que l'on n'a pas fait d'erreur dans la sélection de leurs identifiants.

Les deux colonnes suivantes sont la vraisemblance courante du scénario et le niveau courant du risque. Le niveau de risque n'est mis à jour que lorsqu'on lance le calcul depuis l'onglet **Synthèse**. A l'issue de ce calcul, le tableau a été trié par risque décroissant, puis vraisemblance décroissante, ce qui permet de repérer rapidement les scénarios sur lesquels il est intéressant d'agir.

6.5 Mesures

Ce tableau comporte trois colonnes saisies :

- **ID**, un identifiant arbitraire de la mesure
- **Libellé**, un descriptif de la mesure. Ce sera logiquement le titre du chapitre correspondant dans une politique de gestion du risque qui n'est pas détaillée ici.
- **Etat**, marqueur qui est à E pour une mesure Effective, P pour une mesure Programmée.

6.6 ScnMes

Ce tableau comporte deux colonnes saisies et neuf colonnes calculées.

Les colonnes saisies sont l'identifiant d'une mesure et l'identifiant du scénario dont elle permet de faire baisser la vraisemblance.

Les deux premières colonnes calculées sont les libellés du scénario et de la mesure, elles permettent de s'assurer qu'on n'a pas fait d'erreur dans le choix de leurs identifiants.

Les sept colonnes suivantes sont des rappels d'information qui permettent de vérifier la cohérence sans avoir besoin de changer d'onglet :

- L'état de la mesure, **E**ffective ou **P**rogrammée
- Les vraisemblances initiale, courante et future du scénario
- Le nombre de mesures à l'état Effective pour ce scénario
- Le nombre de mesures à l'état Programmé pour ce scénario
- Un indicateur d'erreur, positionné à VRAI et en rouge si la vraisemblance courante est différente de la vraisemblance initiale sans mesure effective, ou la vraisemblance future différente de la vraisemblance courante sans mesure programmée.

Les six dernières colonnes sont identiques à celles qui se trouvent dans la table des scénarios, le report ici n'est qu'une commodité de navigation.

6.7 Histoire

C'est un simple tableau de version, à renseigner à la main lorsqu'on archive des versions de l'analyse selon un processus de gestion documentaire qui n'est pas décrit ici.

6.8 Contexte

C'est ici que se trouvent les tables permettant de caractériser les risques (Critère, Scope) ou les scénarios (Source, Vecteur, Mode). Les données dans ces tables sont utilisées en aide à la saisie dans les onglets de risques et de scénarios.

6.9 Référentiel

C'est ici que se trouvent les échelles de vraisemblance, de gravité et de niveau de risque, ainsi que la matrice GV2R permettant d'attribuer un niveau de risque en fonction d'une gravité et d'une vraisemblance. Les données dans ces tables sont utilisées en aide à la saisie dans les onglets de risque et de scénarios.

7 Ecarts à EBIOS

Les écarts visent à alléger le processus d'analyse en fusionnant certains concepts, éventuellement au prix d'une perte de détail.

EBIOS différencie les événements redoutés, qui sont la perte d'un critère sur un bien essentiel, des risques qui sont la survenue d'un événement redouté du fait d'un certain bien support.

Ici, chaque ligne de risque correspond à un événement redouté, les causes de survenue sont amalgamées. La notion de bien essentiel reste implicite.

Dans EBIOS, un scénario est lié au critère de l'atteinte finale aux biens essentiels. C'est une notion qui peut amener à de la confusion, par exemple lorsque la panne d'un système de sauvegarde (perte de disponibilité) doit être caractérisée comme un scénario portant sur l'intégrité. Par ailleurs, un même scénario peut avoir des effets selon plusieurs critères. C'est pourquoi ici on a éliminé la notion de critère de la description d'un scénario.

On conserve en revanche les attributs descriptifs de source, de vecteur (bien support) et de mode, fort utiles lorsqu'on recherche a postériori si un scénario a déjà été envisagé.

De ces deux choix découle que le lien entre scénario et risque est libre, sans contrôle de cohérence sur le critère (qui n'existe plus pour le scénario) ou sur le vecteur (qui n'existe plus pour le risque).