# *EBIOS Risk Manager*

# Bilan et propositions d'améliorations

| | | |
|---|---|---|
| Date | : | 04/05/2022 |
| Statut | : | Soumis à l'approbation du CA avant diffusion aux membres |
| Classification | : | Diffusion publique |
| Nombre de pages | : | 104 |
| Responsable des travaux | : | Vincent LORIOT et Jean OLIVE |
| Validation | : | Responsables des travaux |
| Approbation | : | Conseil d'administration |
| Licence | : | |

Ce document a été réalisé par le Club EBIOS

Responsables des travaux :

- Vincent LORIOT (administrateur du Club EBIOS)
- Jean OLIVE (vice-président du Club EBIOS)
- Matthieu GRALL (IMINETI by NIJI)
- Charlène PROVOST (IMINETI by NIJI)

Contributeurs :

- Pierre BACQUET (THALES ALENIA SPACE)
- José-Patrick BOÉ (G-ECHO)
- Laurent CHOURAKI (SOGETI)
- Raphaël DROPSY (ORES)
- Rachid EL ALAOUI (AMN BRAINS)
- Matthieu GRALL & Charlène PROVOST (IMINETI by NIJI)
- Tony HÉDOUX (ALL4TEC)
- Jean OLIVE (CGI BUSINESS CONSULTING)
- Stéphane PAUL (THALES)
- Florent PETIT (AIRBUS/APSYS)
- Nicolas PIERRE (ADVENS)
- Fabien RENAUDIN (ANSSI)
- Jean-Victor SIE (SOPRA STERIA)
- Nicolas VAN CAUTER (THALES)
- Paul VARELA (EUSPA)

**Remerciements aux contributeurs**

**Le Conseil d'Administration du Club EBIOS tient à remercier tout d'abord les membres du Club EBIOS qui ont pris le temps de rédiger des commentaires et ses retours d'expérience riches et complets.**

**Nous remercions la société NIJI qui a piloté et compulsé un nombre important de retours et créé le présent document.**

**Une mention particulière aux membres du groupe d'édition qui ont analysé tous les retours des contributeurs et ont débattu pour apporter des compléments : Matthieu GRALL, Rachid EL ALAOUI, Jean OLIVE Florent PETIT, Nicolas PIERRE, Charlène PROVOST et Fabien RENAUDIN.**

# Historique des modifications

| Date | Objet de la modification | Auteur(s) | Statut |
|---|---|---|---|
| 01/12/2021 | Création du document | Charlène PROVOST<br>Matthieu GRALL | Document de travail |
| 07/12/2021 | Prétraitement des propositions pour l'atelier 1 | Charlène PROVOST<br>Matthieu GRALL | Document de travail |
| 08/12/2021 | Prétraitement des propositions pour l'atelier 2 | Charlène PROVOST<br>Matthieu GRALL | Document de travail |
| 14/12/2021 | Prétraitement des premiers retours d'expériences et de la première partie des propositions pour l'atelier 3 | Charlène PROVOST<br>Matthieu GRALL | Document de travail |
| 17/12/2021 | Finalisation du prétraitement des retours d'expériences et classement | Matthieu GRALL | Document de travail |
| 20/12/2021 | Analyse du prétraitement et corrections | Jean OLIVE | Document de travail |
| 21/12/2021 | Finalisation du prétraitement | Charlène PROVOST<br>Matthieu GRALL | Document de travail |
| 23/12/2021 | Analyse du prétraitement et corrections | Vincent LORIOT | Document de travail |
| 27/12/2021 | Acceptation des modifications apparentes, harmonisation des contributions, finalisation d'une version publiable au groupe d'édition | Matthieu GRALL | Document de travail |
| 12/01/2022 | Ajustement des décisions relatives aux propositions d'améliorations lors des réunions d'édition des 6 et 12/01/2022 | Groupe d'édition | Document de travail |
| 31/01/2022 | Intégration des contributions complémentaires | Matthieu GRALL | Soumis à l'approbation du CA |
| 4/05/2022 | Anonymisation du document transmis à l'ANSSI et suppression des remarques non prises en compte | Jean OLIVE | Document de travail |

# Sommaire

# Introduction : un entrant pour l'amélioration continue de la méthode

Ce document recense **les propositions d'amélioration des guides de la méthode EBIOS *Risk Manager et les retours d'expériences***, produits par le Club EBIOS en vue d'alimenter les réflexions de l'ANSSI dans le cadre de l'amélioration continue de sa méthode.

En complément, une évaluation des « Principales forces, faiblesses, opportunités et menaces (SWOT) » et une « Évaluation des travaux et référentiels » sont proposées en annexe.

# 1 Propositions d'améliorations

## 1.1 Propositions d'améliorations détaillées

Ce chapitre reprend toutes les propositions reçues par le Club et présente des compléments d'analyse réalisés par le groupe de travail en charge d'analyser les retours.

### 1.1.1 [Guide] et [Fiches] Général

| #[1] | Type | Localisation[2] | Constats[3] | Proposition[4] | Complément [5] |
|---|---|---|---|---|---|
| 1 | Forme | [Général] Structure et [Guide] 056 | L'atelier 1 rassemble des outils de natures très différentes, qui ne correspondent pas au sous-processus d'établissement du contexte de l'ISO/IEC 27005. | Sortir les événements redoutés et le socle de sécurité de l'étude du contexte (atelier 1), placer le socle dans un atelier dédié à l'approche par conformité, et les événements redoutés et les sources de risques dans un atelier dédié à l'approche par scénarios, conformément à l'annexe | L'atelier 1 doit mieux distinguer les différentes activités (cadrage, ER, socle), par exemple en illustrant comment les mettre en œuvre. |

[1] Référence incrémentale de la remarque.

[2] Localisation qui fait l'objet de chaque proposition d'amélioration : {[Général] / [Guide] / [Fiches]} [numéro(s) de ligne(s)].

[3] Explication qui justifie, et éventuellement explique, chaque proposition.

[4] Changements concrets proposés dans les documents de la méthode.

[5] Compléments apportés par le groupe éditorial lors de l'analyse des commentaires.

| #[1] | Type | Localisation[2] | Constats[3] | Proposition[4] | Complément [5] |
|---|---|---|---|---|---|
| | | | En effet, les événements redoutés relèvent du début de l'approche par scénarios, et l'évaluation du socle relève de l'approche par conformité.<br>En outre, l'appréciation (identification, analyse et estimation) liée aux sources de risques fait partie de l'appréciation des risques par scénarios | Reporter les changements dans l'ensemble des documents de manière cohérente.<br>NB : ceci ne change pas les « objets » de la méthode, mais uniquement leur présentation. | Attention, la correspondance avec l'ISO/IEC 27005 n'est aujourd'hui pas évidente. Celle-ci pourrait être ajoutée. |
| 2 | Forme | [Général] Structure et [Guide] 056 | Le schéma devrait se rapprocher davantage de celui des normes (ISO 31000 et ISO/IEC 27005), notamment afin de montrer que la méthode intègre également les autres sous-processus de la gestion des risques (ex : communication et consultation). | Changer le schéma par celui proposé dans l'annexe, ou au moins en ajouter un qui établisse la correspondance entre les ateliers et les sous-processus d'ISO/IEC 27005, et ajuster l'ensemble du texte en cohérence. | |
| 3 | Fond | [Général] Structure, [Guide] 056 et 122-124 | Je suis perplexe par le fait que le cycle opérationnel n'embarque pas aussi une revue du socle de sécurité, plus particulièrement du niveau de conformité ou de couverture du SI étudié par rapport au socle de sécurité sélectionné, car, entre les plans d'actions correctifs ou les évolutions fonctionnelles touchant le SI, la +/- mise en œuvre du MCS, les évolutions technologiques, etc. sont autant de facteurs impactant (en positif comme en négatif) le niveau de conformité au socle de sécurité tout au long de la vie du SI, y compris sur des temps relativement courts ! | Proposition pour la figure 2 :<br>- Représenter l'Atelier 1 comme 2 triangles au lieu d'un losange (comme la représentation des ateliers 3 & 4) avec pour le triangle du haut (p.ex. Atelier 1a) le « cadrage » et pour le triangle du bas (p.ex. Atelier 1b) le « socle de sécurité »<br>- De même représenter l'atelier 2 comme un triangle similaire aux ateliers 1a & 3, donc « pointe en haut » en lieu et place du losange actuel<br>- Décrire le cycle opérationnel comme un cycle passant par les triangles « pointe en bas », donc les ateliers 1b & 4<br>- Cette approche limiterait les changements structurels dans la description de la méthode (i.e. activités rattachées par ateliers)<br>Autre proposition pour la figure 2 :<br>- Ne garder que « cadrage » pour l'atelier 1<br>- Représenter l'atelier 2 en 2 triangles avec « sources de risque » pour le triangle supérieur et « socle de sécurité » pour le triangle inférieur, car en toute rigueur l'évaluation de la conformité au socle de sécurité participe à l'appréciation des risques et | Le socle pourrait toutefois être inclus dans le cycle opérationnel. |

| #[1] | Type | Localisation[2] | Constats[3] | Proposition[4] | Complément [5] |
|---|---|---|---|---|---|
| | | | | donc mériterait d'être intégrée dans le rectangle de l'appréciation des risques<br>- Décrire le cycle opérationnel comme un cycle passant par les triangles « pointe en bas », donc les ateliers 2b & 4<br>- Cette approche impacterait la structure du guide en déplaçant l'étude du socle de sécurité (i.e. de la conformité au socle) de l'atelier 1 vers l'atelier 2 (cependant le choix du socle en lui-même peut tout à fait être maintenu dans l'atelier 1)<br>Également, valable dans les deux cas, amender la phrase de la ligne 122 en :<br>« *Un cycle opérationnel revenant sur la conformité au socle de sécurité et sur les scénarios opérationnels à la lumière des incidents de sécurité survenus, de l'apparition de nouvelles vulnérabilités et de l'évolution des modes opératoires.* » | |
| 4 | Forme | [Fiches] 058 | L'élaboration des valeurs métiers et surtout la limite à respecter pour ne pas alourdir la méthode n'est pas toujours comprise. | Il pourrait être intéressant de donner des exemples de VM en expliquant dans quel cas il est intéressant d'avoir une VM de type Processus (qui peut porter des VM de type Information, sans besoin de démultiplier) ou de type Information directement (dans notre cas, quand la VM Information est transverse à plusieurs Processus et impactante en cas d'ER). | |
| 5 | Forme | [Général] Structure | L'usage d'EBIOS *Risk Manager* comme une boîte à outils devrait être davantage être mis en évidence. | Présenter les actions réalisables dans chaque atelier comme des « outils » (exemple : appeler chaque étape des ateliers « outil »). | Solution non décidée (changer « activité » en « outil » ? changer « atelier » en « ateliers » ?). |
| 6 | Forme | [Général] Structure | Le texte devrait mieux différencier ce qui est indispensable et ce qui ne l'est pas. | Présenter chaque atelier, de manière systématique et harmonisée, en distinguant :<br>- les objectifs ;<br>- les actions importantes ; | Travail ultérieur nécessaire. |

| #[1] | Type | Localisation[2] | Constats[3] | Proposition[4] | Complément [5] |
|---|---|---|---|---|---|
| | | | | - des éléments complémentaires (de manière non systématique), ex :<br>  ○ les possibles actions complémentaires ;<br>  ○ les conseils de mise en œuvre ;<br>  ○ les informations ;<br>  ○ les exemples ;<br>- des éléments pour « aller plus loin ». | |
| 7 | Fond | [Général] Structure | La méthode ne fait aujourd'hui apparaître explicitement la détermination de mesures que dans les ateliers 3 et 5. Or, les autres ateliers permettent également de nourrir le plan d'action (ex : mesures pour améliorer l'application du socle, mesures pour agir sur les sources de risques ou leur chemin, *etc*.). | Ajouter la détermination de mesures dans tous les ateliers qui permettent de les alimenter.<br><br>Deux solutions complémentaires :<br>1. structure :<br>  a. soit intégrer systématiquement une activité « Déterminer les mesures contribuant à traiter les éléments de cet atelier » dans tous les ateliers ;<br>  b. soit retirer l'activité en question de l'atelier 3 ;<br>2. phrase à ajouter dans chaque atelier : « Des mesures peuvent être déterminées dans cet atelier afin de contribuer au traitement » […]<br>  a. atelier 1 : « des défauts de conformité au socle de sécurité ou des événements redoutés. » ;<br>  b. atelier 2 : « des sources de risques ou de leurs objectifs visés. » ;<br>  c. atelier 3 : « de la dangerosité des parties prenantes ou des scénarios stratégiques. » ;<br>  d. atelier 4 : « des scénarios opérationnels » ;<br>  e. atelier 5 : « des risques de manière cohérente. ». | |

| #[1] | Type | Localisation[2] | Constats[3] | Proposition[4] | Complément [5] |
|---|---|---|---|---|---|
| | | | | | |
| 8 | Fond | [Général] Terminologie | Le terme « évaluer » est plusieurs fois employé de manière incompatible avec le concept normatif d'estimation. | Changer « évaluer » par « estimer » partout où c'est nécessaire. | |
| 9 | Fond | [Général] Terminologie | Le terme « valeur métier » n'est généralement pas compris. | Changer « valeurs métier » par « éléments à protéger » ou « données » (pouvant englober les processus informationnels). | Préciser que le métier peut être appliqué au support. Les valeurs métiers ne concernent pas que le cœur de métier… Le terme « éléments à protéger » (comme fin en soi, et non comme moyen) peut être ajouté à la définition. |
| 10 | Forme | [Général] Terminologie | Le terme valeur métier est souvent compliqué à comprendre pour les intervenants. | Nous tentons de leur expliquer ce qu'est une valeur métier. | |
| 11 | Fond | [Général] Terminologie | Le libellé « PACS » est trop utilisé par ailleurs (pacte civil de solidarité, prestataire d'accompagnement et de conseil en SSI). En outre, la norme ISO/IEC 27001 emploie le terme de « plan de traitement ». | Changer « PACS » en « Plan de traitement (des risques) ». | La notion d'amélioration continue devra être intégrée dans le paragraphe explicitant le plan de traitement.<br><br>Éventuellement, bien préciser que ce plan comprend des actions relatives à tous les ateliers. |
| 12 | Fond | [Général] Terminologie | L'exemple donné sur le libellé PACS est souvent remonté et nécessite des explications, sans parler de confusion selon les secteurs d'activité. | Bien que la notion d'amélioration continue soit intéressante (notamment dans le cadre des analyses ISO 27001), le terme mérite peut-être d'être changé/adapté. | |
| 13 | Fond | [Général] | La liste proposée pour les participants aux ateliers est très orientée pour un environnement SI d'entreprise. Il peut être compliqué de trouver des équivalences pour les autres environnements (ex. industriel, produit) | Proposer un rôle plus générique permettant d'identifier l'apport de ce rôle. Ex. : Direction > décideurs, RSSI > responsable(s) de la sécurité du périmètre de l'étude, DSI > responsable(s) informatique du périmètre de l'étude. | |

| #[1] | Type | Localisation[2] | Constats[3] | Proposition[4] | Complément [5] |
|---|---|---|---|---|---|
| | | | | "Direction" : "Responsable(s) décisionnel(s) du SI, en charge du budget",<br>"RSSI" : "Responsable(s) de la sécurité du périmètre de l'étude",<br>"DSI" : "Responsable(s) du périmètre de l'étude". | |
| 14 | Fond | [Général] (ex : Fiches 135) | Pourquoi privilégier des échelles de vraisemblance et de gravité avec un nombre de niveaux équivalents ? | Retirer la phrase | |

### 1.1.2 [Guide] Chapitres introductifs

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 15 | Fond | [Guide] 019 (note de bas de page 2) | Il conviendrait de pointer vers les productions du Club EBIOS qui regroupent la matière complémentaire sur la méthode. | Ajouter la phrase suivante : « des productions complémentaires (bases de connaissances, études de cas, techniques spécifiques, *etc*.) sont accessibles son site web ». | Une des ambitions de cette amélioration continue est aussi d'intégrer/référencer directement les productions du Club EBIOS dans le supplément. |
| 16 | Fond | [Guide] 045-050 | Clarification des deux approches cumulatives | Changer le texte par le suivant :<br>Avec EBIOS *Risk Manager*, l'ensemble des risques est donc considéré :<br>- d'une part *via* une approche par conformité pour les risques « standards », et notamment ceux liés à des événements accidentels et environnementaux, ou à des attaques classiques ;<br>- d'autre part *via* une approche par scénarios, pour les risques avancés, d'origine intentionnelle, et notamment les attaques particulièrement ciblées ou sophistiquées. | « Avec EBIOS *Risk Manager*, l'ensemble des risques est donc considéré :<br>- d'une part *via* une approche par conformité pour les risques triviaux ou connus, et notamment ceux liés à des événements accidentels et environnementaux, ou à des attaques classiques ;<br>- d'autre part *via* une approche par scénarios, pour les risques avancés, d'origine intentionnelle, et notamment les attaques particulièrement ciblées ou sophistiquées. »<br><br>Il serait possible d'ajouter un cas d'usage pour l'approche par scénarios : « ou pour les cas où l'analyse doit apporter des éléments contributifs/décisionnels au |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | choix de la stratégie de traitement du risque ». |
| 17 | Fond | [Guide] 064 | La définition des écarts n'est pas précise (constat, audit, recueil, acceptation, …)<br>À mon sens il faut : 1/ Définir le socle qui doit être appliqué dans le cadre de ce projet / produit. Ce qui doit être fait en amont. 2/ Identifier les écarts, qu'ils soient connus et arbitré de longue date, proviennent d'un problème technique ou de ressources, aient été constatés lors d'un audit. | Changer « Vous définissez également le socle de sécurité et les écarts. » en<br>« Vous définissez également le socle de sécurité à appliquer et prenez connaissance des écarts. » | « Vous évaluez également la conformité au socle de sécurité. » |
| 18 | Fond | [Guide] 114 | NOTE : chaque chemin d'attaque d'un scénario stratégique donne lieu à un scénario opérationnel.<br>Des regroupements de scénarios sont possibles ou des mesures de l'atelier 3 peuvent éliminer des scénarios opérationnels | Remplacer le mot « NOTE » par « Conseil : En général, »<br><br>Dans le cas de chemin d'attaque similaire à plusieurs scénarios stratégiques, les scénarios opérationnels peuvent être mutualisés dans un seul scénario de risque. | |
| 19 | Fond | [Guide] 142 (dans la note) | L'absence de croix dans la 3ème ligne crée une interrogation sur la capacité à apprécier la vraisemblance des risques. | Ajouter une note : « les croix figurant dans le tableau ne signifient pas qu'au moins une des activités de l'atelier ne doit pas être menée. Par exemple, l'étude préliminaire des risques peut nécessiter de rechercher une technique simple pour évaluer la vraisemblance des scénarios stratégiques. » | Ajout d'une note à partir de l'en-tête du tableau « Ateliers principaux » : « Il est souvent utile d'exploiter aussi certaines activités des ateliers non sélectionnés. Par exemple, l'étude préliminaire des risques peut nécessiter de rechercher une technique simple pour évaluer la vraisemblance des scénarios stratégiques. » |
| 20 | Fond | [Guide] 142 | Concernant l'objectif de l'étude "Réaliser une étude préliminaire de risque pour identifier les axes prioritaires | Changer le texte de la note 3 par : "PACS uniquement" | Ajout de « (PACS uniquement) » à la fin de la note 3. |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | d'amélioration de la sécurité", il est indiqué de ne faire que la partie b) de l'atelier 5. Cependant il n'est pas possible d'évaluer le niveau de risques avec les seuls éléments de l'atelier 3, puisqu'aucune vraisemblance n'y est calculée | | |
| 21 | Fond | [Guide] 170 | L'étape doit à mon sens être scindée en deux | Remplacer « d. déterminer le socle de sécurité. » par<br>« d. déterminer le socle de sécurité ;<br>e. identifier les écarts ». | « d. identifier le socle de sécurité et en évaluer la conformité ». |

### 1.1.3 [Guide] et [Fiches] Atelier 1

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 22 | Fond | [Guide] 145 | L'exercice d'analyse du socle n'est pas décrit dans l'objectif. Il est pourtant essentiel au traitement des risques non délibérés et non ciblés et à l'expression des hypothèses pour la suite de l'étude. | Ajouter : « La définition du contenu du socle de sécurité doit être vue comme : 1/ l'expression de mesures pour traiter les risques non délibérés ou non ciblés (souvent s'appuyant sur des référentiels standard. 2/ des mesures qui ne nécessitent pas d'arbitrage et qui donc n'ont pas besoin d'être justifiés par une approche par scénario (ateliers 3 et 4). En particulier, des mesures provenant de référentiels ou de législation dont l'application est obligatoire et sans interprétation. | |
| 23 | Fond | [Guide] 145 | Il manque l'objectif de formaliser des mesures complémentaires liées aux écarts au socle. | Ajouter un objectif : « A l'issue de cet atelier, des mesures de sécurité pourront être exprimées pour combler les écarts issus de l'analyse du socle. Ces mesures seront rappelées dans le PACS de l'atelier 5 ». | Dépend de la proposition de modification du terme PACS. |
| 24 | Forme | [Guide] 174-180 | L'objet de l'étude (pour Biovax) n'est pas indiqué alors que l'introduction précise que la méthode peut être appliquée pour différentes finalités. | Indiquer la finalité de l'étude (PSI, cahier des charges…) afin de préciser pourquoi il est nécessaire de réaliser tous les ateliers.<br><br>L'importance stratégique de la société Biovax pour la fabrication de vaccin ayant été mise en évidence du fait de la crise sanitaire subie par le pays, celle-ci a été déclarée Opérateur d'Importance Vitale (OIV). Cette décision impose à la société Biovax de réaliser une procédure d'homologation telle que l'impose la réglementation. La direction a convenu de réaliser une étude EBIOS RM pour, d'une part établir un bilan plus complet de son niveau de sécurité et d'autre part rédiger la Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS) nécessaire à la procédure d'homologation.<br><br>On peut utilement compléter cet exemple en indiquant comment composer une FEROS. Cette précision a été donnée par le club EBIOS dans la FAQ « Comment faire une FEROS avec EBIOS Risk manager ?» :<br><br>La FEROS est principalement le reflet des résultats de l'analyse de risque, elle est donc structurée comme telle. Par conséquent, vous pouvez adapter votre *template* en reprenant les grandes | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | séquences d'EBIOS Risk Manager. Par exemple, si l'on considère le *template* proposé par l'ANSSI<br>- §4 Besoins de sécurité ——> Socle de sécurité et événements redoutés (atelier 1)<br>- §5 Etude des menaces ——> Sources de risque (atelier 2)<br>- §6 Evénements redoutés ——> Menace liée à l'écosystème (atelier 3)<br>- §7 Risques ——> Scénarios de risque (ateliers 3 et 4)<br>- §8 Objectifs de sécurité ——> Stratégie de traitement du risque et mesures de sécurité (atelier 5)<br>- §9 Risques résiduels ——> Risques résiduels (atelier 5)<br>- §10 Compléments ——> Cadre de suivi des risques (atelier 5)<br>Pour le §8, nous vous recommandons fortement de structurer votre stratégie et vos mesures selon le cadre de référence suivant : protection, défense, résilience, gouvernance (voir fiche méthode n°9). | |
| 25 | Fond | [Guide] 174-183 | La définition des hypothèses et des contraintes n'est pas demandée dans l'atelier. Elles sont pourtant indispensables à l'analyse de risques. | Ajouter la nécessité de définir des hypothèses et des contraintes.<br><br>Ajouter le paragraphe suivant à la fin de la section "Définir le cadre de l'étude" : "Listez les hypothèses et les contraintes qui conditionnent la manière dont l'analyse sera menée, le niveau de détail qui pourra être considéré pour l'environnement, les parties de l'environnement qui ne seront pas considérées, les menaces qui doivent être privilégiées ou au contraire ne doivent pas être prises en compte...".<br>Note : pour plus de détails, il est possible de se référer à la section suivante de la méthode EBIOS 2010 : "Action 1.1.4. Identifier les paramètres à prendre en compte". | Elles peuvent être traitées dans le périmètre/cadre (ex : 187-189). |
| 26 | Fond | [Guide] 194+ | Il faudrait mettre en évidence la notion de valeur métier et la(les) raison(s) d'en définir une ou plusieurs. | Expliquer systématiquement avec des exemples la raison de diviser un processus métier en plusieurs valeurs métier (biens support différents, impacts différents, etc.).<br><br>Par exemple, un processus métier dans son entièreté peut être considéré soit comme une valeur métier à part entière soit | |

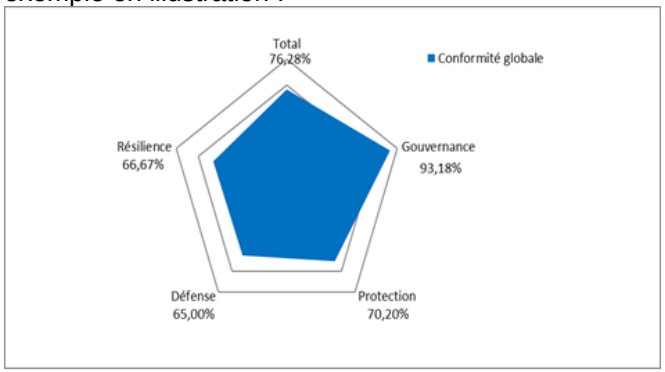
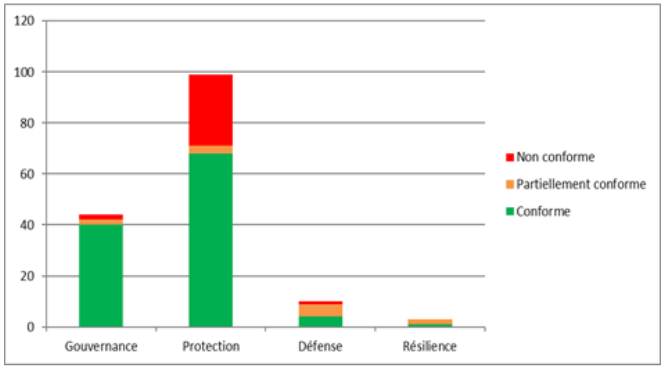
| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | découpée en plusieurs valeurs métiers. Cette découpe s'effectue selon que les sous-processus ou activités aient un niveau de criticité voire d'impact différent par rapport aux autres ou exploiter des biens supports sous-jacent bien distincts. Cela doit être fait de manière réfléchie, car elle va influencer la suite de l'analyse au risque de la compliquer voire même de la rendre impossible à conduire. | |
| 27 | Fond | [Guide] 223 | La question pour établir la liste des biens supports intègre les parties prenantes. Or, notre compréhension est qu'un bien est soit un bien support, soit une partie prenante. | "Il s'agit des éléments du système d'information sur lesquels les valeurs métier reposent." Si la sécurité de ces biens ne dépend pas directement du commanditaire du système étudié, ce sera des parties prenantes et non un bien support. | Ajouter seulement « lister les biens supports et les parties prenantes ».<br><br>Préciser (dans la définition des parties prenantes ou des biens supports, ou en note de bas de page) la distinction « Si la sécurité de ces biens ne dépend pas directement de l'objet de l'étude, ce seront des parties prenantes et non des biens supports. ». |
| 28 | Fond | [Guide] 288 (tableau de droite) | Les impacts identifiés dans le tableau ne permettent pas de justifier les niveaux de gravité. | Soit supprimer la colonne Impacts du guide, soit exprimer des conséquences qui justifient les gravités. | |
| 29 | Forme | [Guide] 288 | En cas de reprise (ou saisie dans des outils), ne pas connaître les niveaux d'impact par type peut être compliqué pour se rappeler ce qui avait été dit en atelier, surtout si cela n'est pas (ou mal) justifié. | Il serait préférable de conseiller d'évaluer tous les niveaux d'impact par type, en prenant le MAX pour établir la gravité. | Les types d'impacts pourraient disparaître du tableau. En outre, il est jugé préférable de formuler des impacts concrets (voir les événements redoutés du tableau) plutôt que d'estimer la gravité sur des impacts génériques. |
| 30 | Fond | [Guide] 289-317 | La « détermination du socle de sécurité » ne consiste pas uniquement en sa détermination, mais aussi, et plus justement, en | Changer le titre « Déterminer le socle de sécurité » par « Évaluer la conformité au socle de règles » et mieux décomposer la réflexion sur le socle, par exemple en ajoutant l'introduction suivante :<br>« Cette activité requiert de : | Le titre pourrait être « Déterminer et évaluer le socle de sécurité ».<br><br>Cette activité requiert de : |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | l'évaluation du respect / de l'application du socle. | 1. déterminer le socle de règles ;<br>2. évaluer le respect du socle ;<br>3. le cas échéant, déterminer les mesures complémentaires ;<br>4. décider de la manière de poursuivre l'étude. » | 1. identifier les exigences applicables composant le socle de sécurité ;<br>2. évaluer le respect du socle ;<br>3. le cas échéant, déterminer les mesures complémentaires ;<br>4. décider de la manière de poursuivre l'étude. » |
| 31 | Fond | [Guide] 302 | Introduire l'étape e | Ajouter « e. identifier les écarts » | Supprimer également « et les écarts » de la ligne 290. |
| 32 | Fond | [Guide] 301 | Ajouter une note sur l'importance de définir le socle de sécurité au plus tôt. | NOTE : Le socle de sécurité aura idéalement été défini avant la conception et intégré au cahier des charges. | « NOTE : le socle de sécurité aura idéalement été défini avant (ou pendant) la conception. Sa conformité peut également être traitée par ailleurs, par exemple dans le cadre d'un système de management de la sécurité de l'information (SMSI) ». |
| 33 | Fond | [Guide] 289-317 | Il faudrait conseiller sur la façon de traiter un socle de sécurité non mature et pouvant générer des risques non intentionnels.<br>Il faudrait conseiller sur la façon de gérer ces risques non intentionnels<br>Il nous arrive lors des ateliers d'identifier un scénario pour lequel l'erreur non intentionnelle serait plus vraisemblable qu'une action malintentionnée (perte d'un dispositif contenant des données | Nous avions commencé par identifier les écarts par rapport aux contrôles ISO27002 et générer un risque non intentionnel si aucun risque intentionnel ne venait couvrir ce risque. Et nous avons associé ce risque non intentionnel à un évènement redouté et un impact. Enfin nous évaluons la vraisemblance en mode express. | Reformuler comme suit : « En cas d'écarts au socle faisant émerger un risque non intentionnel, il est possible d'exprimer ce dernier de manière empirique ou en utilisant un évènement redouté et en évaluant la vraisemblance en mode express ». |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | confidentielles vs voler le dispositif afin de le divulguer) | | |
| 34 | Fond | [Guide] 289-317 | Cette activité est réduite dans le guide à sa plus simple expression alors même que, sur la base de la représentation graphique de la « pyramide du management du risque numérique » (cf. figure 1, ligne 51 du Guide), l'approche par « conformité » représente un objectif de couverture d'au bas mot 80% des menaces numériques (allant des menaces « simples » à « élaborées »), le chiffre de 80% n'étant pas donné par hasard puisqu'il correspond à une estimation du BSI allemand (i.e. *Bundesamt für Sicherheit in der Informationstechnik*) dans son « standard 100-2 » sur l'objectif maximum de couverture des menaces pouvant être traité par la seule approche par conformité à un socle de sécurité. Il y a donc un déséquilibre flagrant dans le Guide, qui peut s'expliquer dans la version 1 du Guide par la nouveauté de l'approche « mixte » Conformité + Scénarios dans la culture méthodologique française très imprégnée de l'approche par scénarios (cf. précédentes versions d'EBIOS). Maintenant, cette première révision du Guide de la méthode est l'opportunité de | En premier lieu, le choix (et/ou la constitution) d'un « bon » socle de sécurité n'est pas du tout trivial et mériterait d'être plus accompagné dans le Guide (ou à travers une Fiche méthode dédiée ?? J'ai des idées pour une telle fiche cependant pas encore assez formalisées pour donner ici un contenu complet de fiche méthode…).<br>- Il y a déjà eu des interventions intéressantes sur le sujet, qui pourraient être consolidées / capitalisées / synthétisées et/ou référencées pour enrichir cette activité sur le socle de sécurité.<br>- En complément une approche qu'il me semble intéressant de préconiser est d'avoir (ou de réorganiser) un socle de sécurité adoptant une structure selon les grands axes de défense en profondeur (cf. *Gouvernance – Protection – Défense – Résilience* pour l'approche ANSSI/UE ou *Identifier – Protéger – Détecter – Répondre – Reprendre* pour l'approche NIST, *etc*.)<br><br>Ensuite, si l'on est prêt à aller même encore un peu plus loin dans le « rééquilibrage », en écho à ma remarque de fond sur les chapitres introductifs, il pourrait être envisagé de faire de l'étude du socle de sécurité une Activité à part entière ou tout du moins une « demi-activité » (cf. proposition de passer le losange de l'Activité 2 en 2 triangles avec le triangle supérieur pour « Sources de risque » et le triangle inférieur pour « socle de sécurité »… à voir (pour cette révision ou pour une suivante 😄)<br><br>Également, sans vouloir faire peur, cette activité d'étude du socle de sécurité est chronophage si l'on veut la réaliser sérieusement … or il faut la réaliser sérieusement, car si la base (de la pyramide, et par transposition du SI étudié) n'est pas saine, cela a-t-il un sens d'étudier des scénarios avancés pour sortir des mesures de sécurité toutes aussi avancées … et potentiellement mises en défaut par des sous-jacents bancals… | (cf. , et autres propositions relatives au socle)<br><br>L'idée de développer la représentation graphique de la conformité au socle pourrait être ajoutée. |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | commencer à rééquilibrer les choses (progressivement)… | - Typiquement le nombre d'exigences grimpe assez vite au-delà de la centaine, voire potentiellement beaucoup plus (déjà au minimum 42 exigences avec le seul Guide d'Hygiène Informatique de l'ANSSI, ensuite p.ex. 188 exigences pour le DR (cf. II-901) même s'il est possible de rationaliser un peu, etc.)<br>- Et comme cela couvre tout le spectre de la sécurité cyber, il n'est pas trivial d'apporter toutes les réponses, cela demande généralement la contribution de plusieurs sachants de domaines différents…<br>- Ainsi, en retour d'expérience, cette activité réalisée à fond représente facilement entre la moitié et les deux tiers de la charge de l'analyse de risque … sans compter que lorsque l'on est en présence d'un SI (et d'un organisme) de faible maturité SSI, y a-t-il un sens à aller étudier des « scénarios avancés » alors que l'hygiène informatique de base n'est même pas réellement maitrisée ?!<br>○ Pour ne pas frustrer le commanditaire de ne pas avoir des « scénarios de risque » si l'on s'arrêtait à la seule étude de la conformité au socle de sécurité, une approche intermédiaire peut être de formaliser des scénarios se concentrant avant tout sur les écarts les plus problématiques au socle de sécurité pour les illustrer à travers des scénarios de risque dédiés, même si relativement « simples » dans leur mise en œuvre, dans une perspective de communication vers les commanditaires, les scénarios pouvant passer pour plus « tangibles » que les seuls constats des écarts de conformité au socle de sécurité… mais nous touchons ici à l'Atelier 4 😄<br>En complément, pour la façon de finir cette activité, tel que donné avec la phrase commençant en ligne 309, mettre plus en lumière cette activité d de l'Atelier 1 en précisant que le résultat de l'étude de la conformité au socle de sécurité est l'occasion d'une première intéressante communication (vis-à-vis des commanditaires et | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | autres parties-prenantes de l'analyse de risque) sur le niveau de sécurité cyber du SI par rapport à la cible fixée qu'est le socle de sécurité.<br>- Ainsi un rendu graphique synthétique sous forme de diagramme de Kiviat est très efficace pour exprimer la couverture au global et sur les axes de la défense en profondeur (cf. Gouvernance – Protection – Défense – Résilience pour l'approche ANSSI/UE ou Identifier – Protéger – Détecter – Répondre – Reprendre pour l'approche NIST, etc.) éventuellement complété d'un diagramme en bâtons pour exprimer les proportions d'exigences Conformes – Partiellement conformes – Non conformes, dont voici un | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | exemple en illustration :<br>  <br><br>Couverture consolidée<br>  <br><br>Couverture par exigences | |
| 35 | Fond | [Guide] 289-317 | Absence de lien explicite entre le socle de sécurité et l'appréciation des risques. | Le socle de sécurité traite implicitement les risques basiques et évidents.<br>La phase d'appréciation des risques s'intéresse aux risques non traités par le socle de sécurité. | Ajouter le texte proposé dans l'atelier 4. |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | La complémentarité entre les deux approches n'est pas claire. | Cela nécessite de déterminer les limites des protections assurées par les mesures du socle de sécurité et par la suite d'identifier les menaces qui vont au-delà de ces limites.<br>Concrètement, pour chaque mesure du socle de sécurité, il convient d'identifier les menaces qui exploitent ses limites.<br>On s'assurera de prendre en compte toutes ces menaces lors de la définition des scénarios opérationnels au cours de l'atelier 4.<br><br>Exemple :<br><br>**Mesures du socle** : mettre en place un verrouillage automatique des sessions Windows au bout d'un temps d'inactivité (mesure utile si l'utilisateur s'absente et oubli de verrouiller sa session)<br><br>**Menace exploitant les limites de cette mesure** : un attaquant qui accède au poste non verrouillé et non surveillé avant l'écoulement du temps d'inactivité qui déclenche le verrouillage. | |
| 36 | Fond | [Guide] 295-301 | Il manque dans la liste des référentiels les exigences des parties prenantes. Ceci est particulièrement applicable pour les systèmes industriels et les produits. Par exemple, les exigences de sécurité des clients lors de la conception d'un produit. | Ajouter à la liste des référentiels les exigences des parties prenantes. | Modifier le texte (293-301) comme suit :<br><br>*Ces référentiels peuvent être* **(**de manière illustrative et non limitative) :<br>■ des règles de sécurité internes à l'organisation (ex : PSSI) ;<br>■ des exigences de tiers que vous devez respecter (ex : exigences de clients pour la conception d'un produit) ;<br>■ *des règles d'hygiène informatique et bonnes pratiques de sécurité* (ex : *guides de recommandations de l'ANSSI~~, règles de sécurité internes à l'organisation, etc.~~*) ; |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | ■ *des normes* **(ex :** *famille ISO 27000***)**~~, etc~~. *;*<br>■ *des réglementations en vigueur : vous pouvez vous reporter au site de l'ANSSI qui dresse un panorama des textes réglementaires en matière de sécurité numérique*.<br>■ *des règles ou mesures spécifiques au SI concernés décidées au cours de la conception.* |
| 37 | Fond | [Guide] 302 à 312 | Cette section traite seulement le cas « si l'objet de l'étude est un système ou un produit déjà existant » et ne dit rien dans le cas où le système n'existe pas. | Proposition de mode opératoire pour élaborer un socle de sécurité dans le cas d'un système qui n'existe pas :<br>- Identifier le(s) référentiel(s) applicables(s)<br>- Décliner les exigences de ce(s) référentiel(s) en mesures concrètes pour le système objet de l'étude<br>- Parmi ces mesures, retenir dans le socle celles dont la nécessité est évidente ; celles qui relèvent de l'hygiène de base ou d'exigences obligatoires<br>- Reprendre les mesures non retenues dans l'appréciation des risques pour décider de leur mise en œuvre. | Ajouter le texte suivant (entre 301 et 302) :<br>Dans le cas où l'objet de l'étude est un système ou un produit à concevoir, déterminez les mesures à intégrer dans l'atelier 5. Parmi ces mesures, retenez notamment celles dont la nécessité est évidente, celles qui relèvent de l'hygiène de base ou d'exigences obligatoires, et celles qui ne nécessitent pas d'arbitrage. |
| 38 | Fond | [Guide] 303 | Évaluer l'état d'application par un audit est utile lorsque la finalité de l'étude est de montrer les risques qui pèsent actuellement sur la cible de l'étude. Néanmoins il peut y avoir d'autres finalités à l'analyse de risques comme de déterminer un référentiel de sécurité pour un projet, par exemple. | Remplacer en 302 « Si l'objet de l'étude est un système ou un produit déjà existant » par « Si l'objet de l'étude est un système ou un produit déjà existant et que l'objectif de l'étude est de fournir une vision des risques qui pèsent actuellement sur le SI à analyser ». | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 39 | Fond | [Guide] 309-312 | La manière de considérer les non-applications ou mauvaises applications du socle peut varier selon les études, et nécessite d'effectuer un choix pour la suite de l'étude. | Ajouter une action consistant à décider de la suite de l'étude, ex :<br>- ne pas poursuivre tant que le socle n'est pas respecté ;<br>- poursuivre en considérant que ce qui n'est pas appliqué le sera ;<br>- *etc*.<br>[à développer si ] | Remplacer le paragraphe 309-312 par le texte suivant :<br>Pour chaque écart, choisir comment poursuivre l'étude (plusieurs options possibles) :<br>- option 1 : ne pas poursuivre tant que l'élément du socle de sécurité qui n'est appliqué n'est pas correctement appliqué ;<br>- option 2 : poursuivre en considérant que l'élément est appliqué (vous tiendrez compte de celui dans les scénarios de risques) et en précisant les actions à mener (cf. reprises dans l'atelier 5) ;<br>- option 3 : poursuivre en considérant que l'élément n'est peut-être pas nécessaire (vous déterminerez s'il est utile au traitement de certains risques ou non). |
| 40 | Fond | [Guide] 310 | 1. Lorsque les risques sont liés à des sources non délibérées ou non ciblés, les écarts ne seront pas repris dans l'appréciation.<br>2. Si des écarts peuvent être comblés lors de l'atelier 1, pourquoi continuer à les considérer dans l'appréciation des risques par l'approche par scénario. Sauf si un | Les écarts observés vis-à-vis du socle seront soit repris dans l'appréciation des risques des ateliers suivants, soit comblés immédiatement par des mesures.<br>Dans le cas où ils sont comblés immédiatement, les mesures associées doivent être prises en compte dans l'appréciation des risques et repris dans le plan de traitement (atelier n°5). | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | arbitrage pour combler ces écarts est nécessaire. | | |
| 41 | Fond | [Guide] 309-312 | Lorsqu'il y a un écart vis-à-vis d'un référentiel, la conclusion considérée dans la méthode est nécessairement d'identifier les risques liés aux écarts. Or, d'autres possibilités devraient être considérées. Par exemple, il devrait être envisagé de ne pas continuer l'analyse de risques si les écarts sont trop importants. De plus certains écarts n'entraîneront pas nécessairement de risques dans l'analyse en cours, puisque l'objectif n'est pas d'avoir une liste exhaustive des risques. | Proposer plusieurs actions possibles en cas d'écart vis-à-vis d'un référentiel. Une proposition :<br>1. Les écarts sont tous inclus dans le plan d'action pour implémentation : l'activité peut se poursuivre avec l'identification des risques en partant du principe que les écarts sont couverts telle que définie dans le plan d'action<br>2. Certains écarts ne seront pas couverts dans le plan d'action :<br>a. Le besoin de sécurité lié à la couverture des écarts n'est pas clair : l'analyse est poursuivie avec identification des risques induits par les écarts aux exigences, ainsi que par les risques non couverts par les exigences,<br>b. Le nombre d'écarts n'est pas acceptable : l'analyse n'est pas menée à terme, car trop d'écarts ne seront pas couverts,<br>c. Le nombre d'écarts est acceptable : une action pour demande de dérogation/déviation doit être faite pour chaque exigence et l'analyse est poursuivie avec identification des risques induits par les écarts aux exigences, ainsi que par les risques non couverts par les exigences.<br>Pour les choix 2.a. et 2.c., une nouvelle décision doit être prise pour l'inclusion d'une remédiation dans le plan d'action. Dans le cas où la remédiation n'est pas choisie, il est nécessaire qu'une dérogation/déviation soit validée. | |
| 42 | Fond | [Guide] 303 | Le guide préconise lors de l'étude du socle de sécurité d'évaluer l'état d'application de référentiels de sécurité. L'évaluation de l'application requiert pratiquement un audit. Sur certains pans, le projet n'a pas d'information ou ne sait pas se prononcer. | Si l'état d'application des mesures est inconnu ou si le système est à concevoir ou si une étude des risques a déjà été réalisée, il peut être intéressant d'identifier les mesures pour lesquelles un arbitrage est nécessaire et qui devront être argumentées par l'approche par scénario. L'absence de ces mesures sera alors considérée comme des écarts et reprise dans l'appréciation des risques.<br>Dans le cas d'une étude déjà réalisée, les mesures qui nécessitent un arbitrage seront laissées en écart à l'issue de l'étude de sécurité et leur intérêt sera étudié par l'approche par scénario. | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 43 | Fond | [Guide] 306 | L'identification exhaustive des écarts est souvent impossible dans les budgets impartis pour les analyses de risque, et de plus sous exploitée dans la suite de la méthode. | Il faudrait expliquer comment concilier budget, temps et identification des écarts s'ils sont retenus comme obligatoire ou conseiller de faire une évaluation « grosse maille » et ajuster plutôt au niveau des AE où on rentre dans le détail des implémentations avec après coup une vérification des textes voir si tout est respecté (ou non). A contrario, si l'atelier 4 n'est pas réalisé dans le cadre de démarche simple, cette analyse d'écart est très importante, car structurante pour la suite. | C'est possible, mais au choix de chacun. |
| 44 | Fond | [Guide] 309 à 312 | Cette section dit que tous les écarts identifiés sont repris dans l'appréciation des risques et les mesures de remédiation sont définies au cours de l'atelier 5.<br><br>Cela est contraire à l'objectif du socle de sécurité qui est d'identifier des mesures de sécurité évidente à mettre en œuvre dans une approche par conformité, sans avoir à formaliser des risques. | Du moment qu'ils relèvent de l'hygiène de base ou d'exigences obligatoires, les mesures de correction des écarts observés doivent être définies dans le socle de sécurité, sans avoir à les traiter dans l'appréciation des risques. | |
| 45 | Forme | [Guide] 313 | Dans le cas de client mature sur la gestion des risques, il peut être nécessaire de réaliser des liens entre analyses (en héritage sur des périmètres en cascade par exemple) | Il pourrait être intéressant de créer une fiche méthode sur de possibles imbrications d'analyse et expliquer comment les lier. | Cette idée pourrait être développée dans le cadre soit des [Fiches] soit des travaux du Club EBIOS. |
| 46 | Fond | [Fiches] 061 | La notion d'« entité ou personne responsable » (pour les valeurs, métiers, biens supports, risques, mesures et risques résiduels) pourrait davantage converger vers la terminologie ISO 2700x. | Changer « entité », « personne responsable » et équivalents par « propriétaire ». | |

### 1.1.4 [Guide] et [Fiches] Atelier 2

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 47 | Fond | [Guide] Atelier 2 | L'atelier 2 est extrêmement utile et permet de discuter avec les représentants du métier de manière simple et efficace. C'est un bon moyen de conscientisation surtout si l'on dispose d'exemples concrets. | Aucune proposition. L'atelier pourrait être considéré comme superflu cependant il a son utilité. | Noté |
| 48 | Fond | [Guide] 351 | À ce stade de l'étude, il manque des mesures qui pourraient diminuer la pertinence des sources. | Il peut également être utile de proposer des mesures de sécurité pour diminuer la pertinence des SR/OV. Par exemple, des mesures de surveillance qui peuvent diminuer l'impunité des sources, restreindre la communication autour de l'importance du SI, retirer tout ou partie des valeurs métiers pour limiter l'objectif visé.<br>*À ajouter aussi aux données de sortie.* | |
| 49 | Fond | [Guide] 355 | La désignation des sources de risques comme type d'attaquant ou groupes d'attaquants peuvent être limitatifs dans certains cas où on préféra définir des profils très proches du système (administrateur technique, utilisateurs à privilèges avancés, usagers, etc.) | Ajouter « Une autre possibilité de caractérisation des sources pourrait être de s'appuyer sur les profils définis dans le SI ou dans l'écosystème. » | Ajouter la phrase suivante dans l'activité a) (après la ligne 375)<br><br>« Les exemples ci-après doivent être contextualisés. Il est possible de les affiner. |
| 50 | Fond | [Guide] 375 | Réfléchir sur les sources de risques dans l'absolu, de manière décorrélée du reste, est souvent difficile. En outre, cela fait perdre le fil de l'étude entamé par les événements redoutés. Enfin, l'estimation des motivations, ressources et activités peut dépendre de ces événements redoutés. | N'apprécier que les sources de risques susceptibles d'être à l'origine des événements redoutés. | Ajouter le texte suivant (après 375) :<br>« Il est également possible de n'apprécier que les couples SR/OV qui pourraient être à l'origine des événements redoutés retenus dans l'atelier 1. »<br><br>Attention toutefois, car analyser séparément les ER et les SR/OV permet ensuite de faire un rapprochement pour identifier s'il y a un ER qui n'intéressent aucune SR, ou |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | s'il y a un OV qui ne correspond à aucun ER.<br>Ce point de rapprochement croisé n'est pas explicite dans le guide et mériterait d'être décrit. |
| 51 | Fond | [Guide] 375 | Il faudrait mettre en évidence le fait qu'il est possible à ce stade-ci d'identifier un nouvel évènement redouté avec son impact. Lors des discussions, et c'est l'un des problèmes remontés au retour d'expérience « Difficulté à lier un scénario stratégique et un niveau de gravité dans certains cas ». On se rend compte que la source de risque qui peut atteindre son objectif en s'attaquant à un second système, mais que l'impact n'est pas équivalent à celui de l'évènement redouté (qui cible la première application) identifié à l'atelier 1. | Nous retournons dans l'atelier 1 et nous y définissons un nouvel ER avec son impact. Nous générons un nouveau couple SR/OV et donc un nouveau scénario stratégique.<br>Voir explication au retour d'expérience « Difficulté à lier un scénario stratégique et un niveau de gravité dans certains cas ». | |
| 52 | Fond | [Guide] 388 | L'appréciation sous forme de croix seules ne permet pas de comprendre l'évaluation à l'occasion d'une relecture. | Ajouter une colonne dans laquelle un argumentaire servira à rendre l'analyse reproductible (explication des appréciations). | |
| 53 | Forme | [Guide] 388 et [Fiches] 184-189 | Les « + » ne sont pas assez explicites. | Changer les « + » des niveaux de « ressources » et de « motivation » par l'échelle suivante :<br>1. Faibles<br>2. Significatives<br>3. Importantes<br>4. Maximales | Bien que 4 niveaux puissent être jugés comme un peu trop nombreux au regard de l'expérience, le niveau 4 permet de qualifier des moyens « illimités », par exemple d'un acteur étatique. Ceci permet aussi d'appliquer la bonne pratique des échelles paires. |
| 54 | Fond | [Guide 399] | Les valeurs de pertinence ne sont pas réutilisées dans la suite de l'analyse et pourtant elles devraient contribuer à l'estimation de la vraisemblance des risques. | Ajouter une note : "NOTE : la pertinence des couples SR/OV peut contribuer à l'évaluation de la vraisemblance des risques" | Par exemple, on pourrait proposer que, si la pertinence est significative, alors la vraisemblance ne puisse dépasser 2. Si elle est importante, la vraisemblance ne peut dépasser 3. |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | La proposition fait un raccourci, en fixant une note maximale en fonction du niveau de pertinence. Mais il y a bien une relation à faire entre la pertinence du couple SR/OV et le niveau de vraisemblance : le même mode opératoire évolué peut être très vraisemblable pour des acteurs très motivés et avec des moyens significatifs, et peu vraisemblables pour d'autres. Mais *a contrario*, si le mode opératoire est simple, alors il pourra avoir la vraisemblance maximale, quelle que soit la pertinence du couple SR/OV. |
| 55 | Fond | [Guide] 397-398 | Il est mentionné qu'il est important de ne pas laisser d'angle mort. Ce qui signifie qu'un certain nombre de couples SR/OV sont identifiés. Tous ne seront pas retenus. Cependant, trop sont peut-être retenus (en particulier s'il s'agit d'un premier cycle) afin de s'assurer d'une bonne couverture (menace externe/interne, couverture CID, Biens supports) | Étant donné qu'il s'agit de notre premier cycle stratégique, nous avons dû nous adapter d'un processus à l'autre.<br>Dans certains processus analysés, nous n'avons retenu que 3 à 5 couples. Dans des processus plus gros et pour ne pas avoir d'angles morts, nous avons retenu plus de 5 couples SR/OV | |
| 56 | Fond | [Fiches] 162 | L'exemple donné de collaboration entre sources est intéressant, mais n'explique pas comment il doit être matérialisé. | Donner un exemple concret d'utilisation avec la sélection des deux sources, mais identifié dans un couple SR/OV « spécial » | Une explication devrait en effet être apportée, mais la solution proposée n'est pas jugée comme appropriée.<br><br>Ajouter « (qui apparaîtra comme une unique source de risques) » à la fin de l'exemple de 162 |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 57 | Fond | [Fiches] 160-163 | Je suis perplexe par la présence du type « officine spécialisée » parmi les profils de Sources de Risque, car c'est le seul profil qui n'est pas (et même a priori jamais) commanditaire de l'attaque, mais plutôt contributeur (engagé par une « véritable » Source de Risque, au sens de l'entité ou la personne qui a la volonté initiale de nuire à une cible donnée…) et a contrario le profil « concurrent » n'apparaît pas en tant que tel dans le catalogue proposé dans la fiche méthode n°4, juste en exemple du type « malveillant pathologique » alors que ce type de profil est, de notoriété publique, à l'origine de beaucoup de (cyber) attaques… motivées par autre chose qu'une potentielle pathologie de la malveillance de leur dirigeant!! | Proposition de remplacer OFFICINE SPECIALISEE par CONCURRENT, avec le sous-titre suivant :<br>« Concurrents déloyaux, ils peuvent faire appel à des officines spécialisées en paravent. » | L'officine spécialisée pourrait, théoriquement, être une véritable source de risque agissant de son propre gré.<br><br>Changer :<br>- « officine » par « **cybermercenaire** » en 160 ;<br>- « officine spécialisée » par « **cybermercenaire** » en 162 et 163 ;<br>- « Étatique » par « **Organisme étatique** » (par cohérence avec les autres sources de risques) ;<br>- « Activiste idéologique » par « **Activiste** » (l'idéologie est plutôt une motivation) ;<br>- « Amateur vengeur » par « **Amateur** » (la vengeance est plutôt une motivation) ;<br>- « Malveillant pathologique » par « **Tiers opportuniste** ». |
| 58 | Forme | [Fiches] 163 | Le terme "officine spécialisée" est peu parlant et peu usité. La notion de "cybermercenaire" est bien plus commune. | Renommer la catégorie "officine spécialisée" en "cybermercenaire". | |
| 59 | Fond | [Fiches] 163 | Le terme « Malveillant pathologique » fait souvent peur et est incompris. | Nous privilégions plutôt le terme « Opportuniste » comme mentionné dans l'exemple. | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 60 | Fond | [Fiches] 163-164 | La liste des sources de risques ne distingue par une menace externe d'une menace interne (en particulier dans le contexte d'un vengeur, d'un malveillant pathologique ou d'un fraudeur) | Nous avons étoffé la liste avec les sources de risques suivantes :<br>- Vengeur, menace externe ;<br>- Vengeur, menace interne ;<br>- Fraudeur, menace externe ;<br>- Fraudeur, menace interne ;<br>- Malveillant pathologique, menace interne ;<br>- Malveillant pathologique, menace externe. | Ajouter la phrase suivante : « Les sources de risques peuvent être externes ou internes. » |
| 61 | Forme | [Fiches] 167 | Coquille sur le titre de la première colonne : « inalités poursuivies » | à corriger par « Finalités poursuivies ». | |
| 62 | Fond | [Fiches] 172 | Les tableaux d'appréciation sont difficiles à relire et les arguments justifiant l'évaluation de la pertinence d'un SR/OV manque. | Ajouter une colonne « argumentaire » dans le tableau pour assurer une reproductibilité de l'analyse. | |
| 63 | Fond | [Fiches] 172-175 | Le terme « ressources » est ambigu. | Changer « ressources » des sources de risque par « capacités d'attaque ». | |
| 64 | Fond | [Fiches] 185 | L'échelle avec des « + » a été un peu déroutante pour les clients. Elle est souvent préfixée et rarement remise en question. | Passer à une échelle en texte (faible, moyen, élevé) pourrait être intéressant bien que sur 3 niveaux (4 voire 5 étant compliqué pour aligner avec les autres échelles), ainsi les « + » pourraient être gardés, mais il serait intéressant de donner un exemple à chaque niveau et type (ressource et motivation a minima) afin de se positionner plus facilement. | |

### 1.1.5 [Guide] et [Fiches] Atelier 3

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 65 | Fond | [Guide] 421 | « Métier » - selon la finalité de l'étude les métiers ne sont pas les mieux placés dans cet atelier.<br>Des acteurs de la DSI dont les architectes techniques peuvent être nécessaires dans le cas de parties prenantes internes. | Ajouter : « Selon la finalité de l'étude, les métiers » au *bullet point* ;<br>Ajouter un *bullet point* : « Acteurs de la direction des SI – représentant les parties prenantes internes » | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | Ajouter un *bullet point* : « Acteurs ayant connaissance des engagements contractuels avec les parties prenantes » | |
| 66 | Fond | [Guide] 421-426 | Il faudrait inclure les responsables fournisseurs ou un rôle équivalent, ayant les informations sur les contrats passés avec les fournisseurs et ce qu'il est possible de leur demander | Ajouter "Responsable fournisseur" à la liste. | |
| 67 | Fond | [Guide] 422 | "Architectes fonctionnels" : une définition devrait être fournie sur la notion d'architecte fonctionnel, car elle est souvent comprise de manières différentes | Ajouter une définition pour "Architecte fonctionnel". Ex. : Architecte en charge de définir les fonctionnalités du système. Ces fonctions définissent ce qui est attendu en entrée et ce qui est attendu en sortie, mais sans présumer de la manière dont elles seront implémentées. | Ajouter une note de bas de page :<br>« Personne en charge de définir les fonctionnalités du système en fonction des besoins des usagers. Ces fonctions définissent ce qui est attendu en entrée et ce qui est attendu en sortie, mais sans présumer de la manière dont elles seront implémentées. » |
| 68 | Fond | [Guide] 430+ | Le terme « menace » est compris de manières extrêmement différentes, notamment en normalisation. Il est préférable de l'éviter le plus possible pour éviter toute ambiguïté. | Changer « cartographie de menace numérique » par « **estimation de la dangerosité des parties prenantes** » (qui peut, de manière optionnelle, faire l'objet d'une représentation visuelle pouvant être appelée « cartographie des parties prenantes »). | |
| 69 | Fond | [Guide] 430+ | Je partage l'ambiguïté du terme « menace », en particulier lors de son usage au sein de l'atelier 3 dans le cadre de l'étude de l'écosystème donc il me semble nécessaire de trouver un autre terme | Changer le terme « menace » (tel qu'utilisé dans l'atelier 3 et la fiche méthode 5) par « criticité », ce qui donnerait p.ex. « cartographie de la criticité des parties prenantes » (à la place de « cartographie de menace numérique »), sans compter que ceci fera de plus clairement écho à la notion de PPC (cf. Partie Prenante Critique) définie et utilisée au sein de l'atelier 3 et de la fiche méthode 5. | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 70 | Fond | [Guide] 445 | L'atelier 3 ne semble pas tenir compte des mesures déjà établies dans les ateliers précédents. | Ajouter : « l'analyse des scénarios stratégiques doit tenir compte déjà retenues dans les ateliers 1 et 2 ». | Ajouter le point suivant :<br>« l'analyse des scénarios stratégiques doit tenir compte des mesures déjà identifiées dans l'atelier 1 (socle de règles, mesures pour traiter les écarts, mesures pour traiter les événements redoutés) et l'atelier 2 (mesures pour traiter les sources de risques et leurs objectifs visés) ; » |
| 71 | Fond | [Guide] 455+ | Selon les exemples et les catégories des parties prenantes, celles-ci semblent être plutôt des entités organisationnelles.<br><br>Qu'en est-il des composants techniques qui sont impliqués dans les missions du système objet de l'étude, mais qui sont hors périmètre ?<br>Sont-ils des biens supports ? Ne font-ils pas plutôt partie de l'écosystème (et ainsi sont des parties prenantes) ?<br><br>Exemple :<br>- Application interne hors du périmètre, mais qui communique avec le système étudié et à qui des données sensibles sont envoyées.<br>Pour moi, cette application fait partie de l'écosystème et est ainsi une partie prenante.<br>- Le périmètre de l'étude est une application qui tourne sur une machine virtuelle, hébergée dans un cloud interne.<br>L'infrastructure du cloud interne n'est pas dans le périmètre de l'étude.<br>Dans ce cas, cette infrastructure fait partie de l'écosystème. | Proposition de définitions et distinction des parties prenantes et des biens supports :<br><br>- **Bien Supports** : un composant technique, physique ou organisationnel, qui fait partie du périmètre du système d'information objet de l'étude.<br>Un composant désigné comme bien support est étudié de manière « intrusive » (ou en boîte blanche) dans l'étude, particulièrement concernant les menaces qui lui sont appliquées et les mesures de sécurité qui lui sont associées.<br><br>- **Partie prenante** : un composant technique, physique ou organisationnel, impliqué dans la mission du système, mais ne fait pas partie de son périmètre.<br>Ce composant est traité en mode « boîte noire » ; l'étude se limite à la frontière et à ses interactions avec le système objet de l'étude.<br><br>Exemple : | Attention à la notion de périmètre qui peut être trompeur. L'administrateur technique peut être considéré dans le périmètre et pourtant il sera souvent pris comme une partie prenante lorsqu'il s'agit d'une cellule d'administration mutualisée.<br><br>Ajouter une note de bas de page derrière « partie prenante » (465) :<br>« Les parties prenantes sont des acteurs de l'écosystème (en dehors de l'objet de l'étude), composés d'éléments organisationnels, techniques et physiques dont les vulnérabilités ne pourront et ne seront pas être étudiées. » |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | Une analyse des risques porte sur une application interne (accessible depuis le réseau interne).<br><br>Cas 1 :<br>Le réseau de l'entreprise fait partie du périmètre de l'étude.<br>Dans ce cas, ce réseau ainsi que ses composants constituent des biens supports.<br>Un scénario opérationnel qui implique une attaque provenant d'internet et qui passe par ce réseau devra détailler étape par étape le mode opératoire d'intrusion dans ce réseau.<br>Ce scénario donnera lieu à l'identification de mesures de sécurité, appliquée aux composants de ce réseau, pour empêcher les étapes de cette intrusion.<br><br>Cas 2 :<br>Le réseau de l'entreprise ne fait pas partie du périmètre de l'étude.<br>Il est dans ce cas une partie prenante.<br>Contrairement au cas 1, un scénario opérationnel qui implique une attaque au travers de ce réseau ne détaillera pas le mode opératoire de l'intrusion.<br>Les acteurs du projet ne sont même censés connaître son architecture.<br>L'étude ne peut pas définir des mesures de sécurisation de ce réseau. Les mesures exprimées (atelier 3) se limitent à la frontière entre l'application objet de l'étude et le réseau (ex. isoler l'application au travers d'un pare-feu). | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 72 | Fond | [Guide] 466 | On a constaté que la menace de parties prenantes a été évaluée dans le cas de scénario de panne ou de sinistre. | Préciser : « Le niveau de menace doit être considéré uniquement dans le cas d'un scénario délibéré et ciblé provenant d'une SR/OV pertinent. » | |
| 73 | Fond | [Guide] 466-468 | Cette phrase pousse, à mon sens, à trop s'appuyer sur les critères et la formule de calcul et à négliger le jugement et le bon sens. Ces derniers sont cependant importants et même plus fiables qu'une approche robotique basée sur une formule de calcul. | Je propose de remplacer par une phrase dans ce sens :<br>« Dans l'évaluation du niveau de menace, il convient de combiner le jugement et le retour d'expérience avec une approche basée sur des critères… » | Attention toutefois, l'objectif est ici de privilégier l'usage de critères tangibles et objectifs pour rendre l'évaluation opposable. Le Jugé d'expert est bien évidemment important, mais ne doit pas occulter le besoin d'expliquer la notation donnée à chaque critère.<br><br>Il faut un « argument formel ». |
| 74 | Fond | [Guide] 468 | L'expérience a montré que les utilisateurs de la méthode indiquaient des évaluations chiffrées sans justifier. Les appréciations deviennent alors rapidement difficiles à relire et engendrant souvent des débats, car les points de vue d'analyse peuvent diverger. | Ajouter : "NOTE : Ajouter toutes les justifications à l'évaluation de la menace pour démontrer le point de vue utilisé par l'analyse et permettre une relecture aisée." | |
| 75 | Forme | [Guide] 469-471 | Pour une meilleure visibilité des parties prenantes et des dépendances, il serait utile d'apporter un graphique (optionnel) indiquant les liens directs et indirects entre les parties prenantes. Ce graphique est disponible dans le support du formateur, à la page 54. Cela permettra par ailleurs de faciliter la constitution des scénarios stratégiques. | Proposer l'ajout d'un graphique représentant les liens entre les parties prenantes et le système (voir le support du formateur, page 54). | Ajouter le schéma dans le [Guide].<br><br>Il est important de pouvoir visualiser les liens.<br><br>Discuter s'il est préférable d'insérer un tel graphique supplémentaire dans le cœur de la méthode ou dans une fiche supplément. |
| 76 | Fond | [Guide] 486+ | Par définition, le risque n'est évalué qu'à la sortie de l'atelier 4, puisque les vraisemblances sont calculées à l'atelier 4. Par conséquent, une analyse de haut | Une technique d'évaluation de vraisemblance partielle liée aux éléments calculés lors des ateliers 2 et 3 pourrait être utile. Cela reste | La réalisation d'un atelier 4 simplifié permet de répondre au commentaire avec une |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | niveau, préliminaire, ne comprenant pas l'atelier 4, ne permet donc pas d'afficher des risques communicables. | dangereux, car le risque évalué serait nécessairement incomplet. | technique « express » d'estimation de la vraisemblance (à dire d'expert et argumentée). Cet atelier 4 simplifié pourrait prendre la forme d'un paragraphe détaillant un mode opératoire simplifié tel que l'on peut le retrouver dans le bulletin de veille du CERT-FR.<br><br>Il faut que cela reste une possibilité. |
| 77 | Fond | [Guide] 503-505 | <u>Duplication des chemins d'attaques et des scénarios opérationnels entre différents scénarios stratégiques</u><br>Un scénario stratégique correspond à un couple SR/OV, pour lequel on formalise des chemins d'attaque qui sont, au cours de l'atelier 4, déclinés en scénarios opérationnels.<br>Si nous avons multiples sources de risques avec le même objectif visé, on finit souvent par dupliquer les chemins stratégiques et les scénarios opérationnels associés entre différents scénarii stratégiques (couples SR/OV).<br>La même situation peut se produire si différent Objectifs Visés sont atteignable au travers de la même valeur métier. | Ajouter la possibilité, voire recommander, de factoriser les couple SR/OV selon les objectifs visés et/ou les valeurs métier concernées, en tenant compte des capacités des sources de risque. | Ajouter une note après 534 : « L'objectif est ici de pouvoir distinguer et de présenter les différents cas possibles de manière intelligible. Ainsi, il peut être utile de regrouper les scénarios stratégiques (ex : factoriser les couples SR/OV selon les profils types d'attaque) ou les décomposer (ex : par événement redouté, voire par impact, ou par profil type d'attaque) ».<br><br>En amont, s'assurer que plusieurs SR n'ont pas été retenus pour le même OV. C'est la cause la plus fréquemment constatée de répétition des modes opératoires associés aux chemins d'attaque. De même, rappeler qu'il n'est pas |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | nécessaire de détailler en scénario opérationnel tous les chemins d'attaque d'un scénario stratégique. |
| 78 | Forme | [Guide] 517 | L'apport d'un complément à liste des ER de l'atelier 1, doit être plus explicite. | Remplacer « Le point de vue étant différent, la liste des ER est susceptible d'être mise à jour. » par<br>« La liste des ER validée dans l'atelier 1 peut être complétée. » | Remplacer « Le point de vue étant différent, la liste des ER est susceptible d'être mise à jour. » par<br>« Le point de vue étant différent, la liste des ER est susceptible d'être complétée ou modifiée. » |
| 79 | Fond | [Guide] 519+ | Il apparaît difficile de représenter des scénarios stratégiques qui pourraient entraîner de multiples impacts. En effet, actuellement nous ne considérons que des impacts unitaires, a fortiori l'impact le plus important. Or un impact à 4 peut être accompagné d'autres impacts à 3. | Considérer la possibilité de :<br>- soit dupliquer un scénario stratégique pour chaque impact, afin d'obtenir un risque spécifique ;<br>- soit faire ressortir les différents impacts pour le scénario stratégique avec, peut-être, une note d'impact augmentée.<br>Exemple à considérer : une attaque dont l'objectif visé est l'exfiltration de données entraîne les événements redoutés suivants, dont les impacts sont évalués à 3 sur 4 : diffusion d'un savoir-faire sensible (PSTN), diffusion de données personnelles (RGPD), diffusion de données clientes entraînant des pénalités financières majeures, diffusion de données stratégiques pour le développement de l'entreprise. L'atteinte de l'objectif visé pourrait entraîner un impact global à 4. | Rien n'interdit dans la méthode d'avoir un OV qui soit une combinaison d'impact. Un exemple plus précis permettrait de mieux apprécier le commentaire. |
| 80 | Fond | [Guide] 550 | Dans l'exemple qui est donné, les chemins d'attaque touchent des valeurs métiers que l'on peut comprendre comme de gravité différente. Ce qui peut poser une confusion dans l'appréciation de la gravité des scénarios opérationnels qui en découlent. | Ajouter une note pour attirer l'attention sur le fait que des chemins d'attaque à l'intérieur d'un même scénario stratégique peuvent toucher des valeurs métiers dont la sensibilité est différente, et qu'il faudra en tenir compte | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | dans l'évaluation de la gravité des scénarios opérationnels. | |
| 81 | Fond | [Guide] 531-532 | L'exercice de création des scénarios est un exercice difficile. Un guide d'aide à leur construction serait appréciable. | Généralement, la réflexion peut être menée en partant d'un SR/OV et en étudiant la pertinence de 3 types de chemin : 1/ l'attaque directe, 2/ l'attaque par rebond sur chaque partie prenante et 3/ l'attaque des parties prenantes. | Ajouter une parenthèse à la ligne 532 :<br>« (ex : attaque directe, attaque par rebond, attaque de parties prenantes uniquement) » |
| 82 | Fond | [Guide] 508-513 | Les événements redoutés ne peuvent pas constituer des attaques sur le SI. Par exemple, on ne peut pas réaliser une attaque "divulgation de données classifiées". Ils sont plutôt la conséquence d'une attaque, qui entraîne la perte de la valeur métier en disponibilité et/ou intégrité et/ou confidentialité...<br>Par ailleurs, les "Exemples d'événements (intermédiaires ou redoutés) d'un scénario stratégique" sont clairement des événements intermédiaires, qui sont des attaques ou des événements involontaires, plutôt que des événements redoutés. | Séparer la notion d'événement intermédiaire de celle d'événement redouté. Dans les schémas, les liens devraient être des événements intermédiaires uniquement. Ces événements intermédiaires devraient pointer vers un événement redouté (et non directement une valeur métier), qui à son tour pointera vers une valeur métier. | Préciser le type d'événement (intermédiaire ou redouté) dans les exemples lignes 508-513. |
| 83 | Fond | [Guide] 569-573 | La nécessité de définir des mesures de sécurité ici plutôt qu'à l'atelier 5 n'est pas claire. Si ces mesures doivent être intégrées dans le PACS, il semblerait qu'il faille les considérer directement dans l'atelier 5. | Déplacer la section "Définir les mesures de sécurité sur l'écosystème" en atelier 5 ou préciser que ces mesures doivent être reportées dans le PACS à l'atelier 5. | |
| 84 | Fond | [Guide] 569-573 | L'impact des mesures de sécurité définies dans cet atelier sur le suivant n'est pas clair. Si le fait d'ajouter des mesures permet d'exclure certaines parties prenantes, car elles sont désormais dans la zone de veille, il faudrait le préciser. | Décrire l'impact des mesures de sécurité sur l'écosystème proposées pour la suite de l'analyse. | Ajouter la phrase suivante après la ligne 573 :<br>« Il est utile de décrire l'effet attendu des mesures et de ré-estimer la dangerosité des parties prenantes. La suite de l'étude tiendra compte de ces mesures. »<br>À moduler toutefois : on ne peut réduire le niveau de danger d'une partie prenante que si la mesure est |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | effectivement mise en œuvre avant la suite de l'analyse. Dans le cas contraire elle n'aura pas d'effet immédiat pour la suite de l'analyse. Anticiper la prise en compte de mesures reviendrait à réduire de manière erronée le niveau de risque actuel pesant sur l'objet de l'étude. |
| 85 | Fond | [Guide] 569-573 | Il faudrait peut-être faire un lien plus clair entre les mesures de sécurité sur l'écosystème et le plan de traitement final. | Nous n'utilisons pas les mesures de sécurité des parties prenantes à l'atelier 3. Nous reportons, en particulier pour les parties prenantes critiques, les mesures de sécurité directement dans le plan de traitement (PACS). | |
| 86 | Forme | [Guide] 571 | "La dernière étape de l'atelier 3 porte sur la recherche de pistes de réduction de ces risques et leur traduction en mesures de sécurité." : il est parlé de risques ici alors qu'il n'y a pas de risques sur cet atelier. | "La dernière étape de l'atelier 3 porte sur la recherche de pistes de réduction de ces risques et leur traduction en mesures de sécurité." : remplacer le terme "risques" par "menaces". | Remplacer « réduction de ces risques et leur traduction en mesures de sécurité » par « traitement de ces scénarios stratégiques par des mesures permettant d'agir sur la menace représentée par les parties prenantes ». |
| 87 | Fond | [Guide] 575 | L'ajout de mesures de sécurité dès l'atelier 3 alourdit la méthode et perd souvent les clients, elle est souvent ignorée. | L'ajout des mesures est important si l'atelier 4 n'est pas réalisé, mais s'il l'est, nous suggérons de rendre cette étape conseillée, mais non obligatoire, quitte à lier les mesures du PACS aux PPC si elles sont concernées. | |
| 88 | Fond | [Fiches] 231 | La note est intéressante, mais son inverse l'aurait été tout autant. On est souvent questionné sur la volonté de mettre des PPC en SR. | Afin de limiter le nombre de couples SR/OV, nous indiquons que toute PPC malveillante est gérée au travers des SR Vengeur ou Opportuniste, une note pourrait être ajoutée en ce sens. | Ajouter une parenthèse à la fin de la ligne 235 : « (ex : opportuniste ou vengeur) ». |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 89 | Fond | [Fiches] 258-259 | L'estimation du niveau de menace des parties prenantes n'est pas facile du manque de clarté de la description des niveaux de dépendance et de pénétration. | Reformuler les échelles de dépendance et de pénétration (voir annexe). | Adopter l'échelle figurant en annexe « **Erreur ! Source du renvoi introuvable.** », afin de :<br>- séparer la dépendance fonctionnelle de la dépendance SSI, ;<br>- fusionner les descriptions proposées ;<br>- ajouter quelques exemples ;<br>- améliorer les questions posées.<br><br>Il conviendrait de bien distinguer et considérer les accès physiques et logiques dans l'échelle de pénétration.<br><br>Il pourrait être utile d'y intégrer les parties prenantes non humaines (interfaces, ex : système interconnecté).<br><br>Un complément est apporté en annexe. |
| 90 | Fond | [Fiches] 258 | L'échelle de pénétration fonctionne bien dans les cas où l'étude concerne un SI complet, mais ne fonctionne pas dans le cas d'une application. Par exemple, si une partie prenante contient des VM dont les ER associés sont de gravité forte, les utilisateurs de cette partie prenante exposent fortement la sécurité de mon SI. | Proposition d'échelles différentes en annexe | |
| 91 | Fond | [Fiches] 258 | La dépendance est vue ici uniquement comme une dépendance liée uniquement à la disponibilité, or par exemple l'impact d'une compromission d'une partie prenante qui assure une authentification externe | Proposition d'échelles différentes en annexe. | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | montre que le SI a une dépendance forte à la PP, et ce même si la PP est redondée. | | |
| 92 | Fond | [Fiches] 258 | L'échelle de pénétration fonctionne bien dans les cas où l'étude concerne un SI complet, mais ne fonctionne pas dans le cas d'une application. | Proposition d'échelles différentes en annexe. | |
| 93 | Fond | [Fiches] 258 | La définition des critères d'évaluation de la menace des parties prenantes pourrait être adaptée. En particulier le critère de pénétration qui dans sa définition actuelle ne reflète pas les aspects SaaS Cloud ou transfert de données vers l'extérieur. | Nous avons adapté la définition du critère de pénétration afin d'y inclure les aspects :<br>- Transfert de données<br>- Application cloud de type IaaS/PaaS/SaaS<br>Ex :<br>- niveau 4 -> fournisseur d'une solution de type IaaS/PaaS/SaaS (administration de l'application et de sa configuration, mais aussi de l'infrastructure sous-jacente)<br>- niveau 1 -> transfert de données agrégées à un prestataire | |
| 94 | Forme | [Fiches] 258 (tableau) | Il n'est pas évident pour les acteurs de l'atelier 3 d'avoir en tête en permanence la signification des 4x4 valeurs possibles, de même que lorsque l'on revient sur une évaluation d'une partie-prenante donc il a été trouvé intéressant de donner un titre expressif à chaque case de ce tableau pour en faciliter l'appropriation et la mémorisation. | Proposition de titre pour chacune des cases :<br>➢ DEPENDANCE<br>○ 1 – Non nécessaire<br>○ 2 – Utile<br>○ 3 – Indispensable<br>○ 4 – Unique<br>➢ PENETRATION<br>○ 1 – Niveau Utilisateur au plus<br>○ 2 – Niveau Administrateur local<br>○ 3 – Niveau Administrateur métier<br>○ 4 – Niveau Administrateur infrastructure<br>➢ MATURITE CYBER<br>○ 1 – Mode Ponctuel<br>○ 2 – Mode Hygiène<br>○ 3 – Mode Réactif<br>○ 4 – Mode Proactif | Les libellés courts pourraient être ajoutés au début de chaque cellule du tableau. |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | ➢ CONFIANCE<br>○ 1 – Intentions suspectes<br>○ 2 – Intentions Neutres<br>○ 3 – Intentions Positives<br>○ 4 – Intentions Communes | |
| 95 | Fond | [Fiches] 258 (tableau) | Pour le critère de CONFIANCE il n'est pas rare que l'on soit en mesure de dire que les intentions d'une partie prenante sont négatives ou suspectes et cela n'apparaît pas dans l'échelle actuelle, la « pire » note étant de dire que les intentions ne peuvent pas être évaluées, ce qui pourrait être aussi associé à un niveau « neutre »… | Mettre pour l'échelle de l'axe CONFIANCE :<br>➢ En niveau 1 : Les intentions de la partie prenante sont considérées comme suspectes<br>➢ En niveau 2 : les intentions de la partie prenante sont considérées comme neutres ou ne peuvent être évaluées<br>➢ pas de changement pour les niveaux 3 et 4. | « 1. Les intentions de la partie prenante ne peuvent être évaluées ou ne permettent pas d'avoir confiance »<br><br>Il y a une confusion dans le niveau 1 : la PP ne doit pas être considéré ici comme source de risque. Donc, le pire est que les intentions puissent être contraires aux missions de l'objet de l'étude. |
| 96 | Fond | [Fiches] 258 bis | Les tableaux d'appréciation sont difficiles à relire et les arguments justifiant l'évaluation de la menace d'une partie prenante manque. | Ajouter une colonne « argumentaire » dans le tableau pour assurer une reproductibilité de l'analyse. | |

### 1.1.6 [Guide] et [Fiches] Atelier 4

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 97 | Fond | [Guide] 594-597 | Il manque un architecte technique ou un administrateur. Il faut en effet une personne ayant suffisamment d'informations techniques afin d'être en mesure de donner une faisabilité sur les scénarios. | Ajouter "Architecte technique" ou "Administrateur" à la liste. | Ajouter une parenthèse à la ligne 595 :<br>« (ex : architecte technique ou administrateur) ». |
| 98 | Fond | [Guide] 633 | L'atelier 4 ne semble pas tenir compte des mesures établies dans les ateliers précédents. | Ajouter : « l'analyse des scénarios opérationnels doit tenir compte déjà retenu dans les ateliers 1, 2 et 3. Ainsi, certains chemins d'attaques identifiés dans l'atelier 3 traités par des mesures dans le même atelier ne seront plus détaillés dans l'atelier 4. ». | L'ANSSI considère que l'atelier 4 ne doit tenir compte que des mesures effectivement mises en place sur le SI.<br><br>Or, ceci peut aller à l'encontre de nombre de commentaires et propositions d'améliorations (ex : différentes tactiques pour poursuivre l'étude selon l'évaluation de la conformité au socle).<br><br>Par conséquent, il est préférable d'ajouter la phrase suivante après la ligne 633 :<br>« L'appréciation des scénarios opérationnels peut, dans certains cas, tenir compte des mesures déterminées dans les ateliers précédents. Ainsi, certains chemins d'attaques identifiés dans l'atelier 3 seront traités et ne seront plus détaillés dans l'atelier 4. ». |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | | Il conviendra de préciser les cas (ex : note dans le [Guide] ou les [Fiches]). |
| 99 | Fond | [Guide] 624 | Il est dommage de ne pas prendre en compte les éléments issus des précédents ateliers, notamment les mesures établies à l'issue de l'atelier 3 portant sur un PP ou sur SI étudié. | Ajouter "la construction des modes opératoires tient compte des mesures complémentaires établies lors de l'analyse du socle et lors de l'analyse de la menace résiduelle des parties prenantes (atelier 3)". | |
| 100 | Fond | [Guide] 641 | Pour les scénarios, il faudrait que l'on puisse voir les OU et les ET logiques dans l'enchaînement des actions :<br>- OU : l'une OU l'autre des actions en entrée permet de réaliser l'étape suivante,<br>- ET : l'une ET l'autre des actions en entrée sont nécessaires pour réaliser l'étape suivante. | Proposer l'ajout de connecteurs logiques OU et ET dans la représentation des scénarios. | Ajouter une nouvelle note sous la ligne 641 :<br>« Il est possible de compléter le schéma par des opérateurs entre les actions élémentaires :<br>- OU : l'une OU l'autre des actions en entrée permet de réaliser l'étape suivante ;<br>- ET: l'une ET l'autre des actions en entrée sont nécessaires pour réaliser l'étape suivante.». |
| 101 | Fond | [Guide] 641 | Les schémas en colonne reprenant les 4 tactiques sont un bon outil de réflexion. Néanmoins, il ne faut qu'elle engendre de blocage ou des représentations sans valeur ajoutée (ex: la tactique "Connaître" est souvent répétée et identique dans chaque scénario). | Ajouter une note : "la représentation en colonne par tactique n'est pas une obligation. Une représentation par enchaînement d'actions élémentaires - sans représentation des tactiques - peut parfois être plus claire. Ce qui est essentiel est que le mode opératoire soit compris sans interprétation par les destinataires de l'étude et que la présentation évite des redites qui nuisent à la lecture des scénarios." | |
| 102 | Fond | [Guide] 675-676 | Afin de donner plus de cohérence au calcul de la vraisemblance, les valeurs indiquées dans l'évaluation des couples SR/OV et des parties prenantes pourraient être prises en compte. En effet, le fait que la source de risque puisse avoir des ressources importantes va peser sur la vraisemblance. De même, le niveau de menace de la partie | Recommander de prendre en compte les évaluations réalisées en atelier 2 et 3 pour l'évaluation de la vraisemblance, afin que l'évaluation prenne en compte l'ensemble des éléments du scénario. | Ajouter la note suivante après la ligne 676 :<br>« L'estimation de la vraisemblance tient compte des éléments étudiés dans les ateliers précédents (pertinence des couples SR/OV, dangerosité des parties prenantes, *etc*.). ». |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | prenante va avoir une influence, tout comme le nombre de nœuds sur le chemin du chemin d'attaque en atelier 3. | | |
| 103 | Fond | [Fiches] 365+ | | Inclure, dans la fiche méthode N°7, ces critères de qualité d'un graphe d'attaque :<br>- Le point de départ doit correspondre à un point accessible par défaut pour l'attaquant ou à une partie prenante considérée dans le chemin d'attaque<br>- Le point d'arrivée doit avoir un lien clair avec l'Objectif Visé<br>- Toute action élémentaire du graphe doit remplir les conditions de réalisation de l'action d'après. | Ajouter une note avant la ligne 371 :<br>« Pour chaque chemin d'attaque, le graphe d'attaque devrait satisfaire les règles suivantes : ces critères de qualité d'un graphe d'attaque :<br>- le point de départ est accessible par défaut par la source de risque ou la partie prenante par laquelle elle passe ;<br>- le point d'arrivée a un lien clair avec l'objectif visé ;<br>- toute action élémentaire du graphe doit remplir les conditions de réalisation de l'action suivante. ». |
| 104 | Forme | [Fiches] 370 | Le visuel des scénarios opérationnels peut être alimenté par une légende caractérisant le type de menaces, la numérotation des actions élémentaires ou encore les biens supports utilisés. | Ajouter une phrase : « Un autre exemple visuel : » (voir annexe « Proposition d'un visuel légendé d'un scénario opérationnel »). | |
| 105 | Fond | [Fiches] 414 | La construction des scénarios opérationnels pourrait s'appuyer sur différents référentiels en accès libre. | Par exemple dans une sous-partie « pour aller plus loin », ajouter la phrase suivante : « il est également possible de s'appuyer sur le référentiel MITRE ». | Ajouter la phrase suivante :<br>« il est également possible de s'appuyer sur des référentiels d'attaques (MITRE ATT&CK®). » et, le cas échéant, pointer sur une fiche sur l'utilisation de MITRE pour réaliser l'atelier 4 (lien production du Club EBIOS). |
| 106 | Fond | [Fiches] 562-563 | Il semble un peu péremptoire d'annoncer qu'il y a « juste » trois approches pour coter | Reformulation, p.ex. en : | |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | la vraisemblance d'un scénario opérationnel. En effet, p.ex., les 3 approches présentées s'appuient sur des scénarios « statiques » et avec une approche avant tout « qualitative » cependant des praticiens expérimentés pourraient vouloir aller sur des approches quantitatives (ou au moins semi-quantitatives), relativement prisées dans le monde anglo-saxon, et nécessaires si l'on veut s'orienter sur des approches dynamiques des scénarios opérationnels (i.e. avec des interactions et des changements de posture dans le temps entre attaquant et défenseur, potentiellement typique d'une APT au long cours…) qui pourraient s'appuyer sur p.ex. la théorie des jeux, etc. | « Voici trois exemples d'approches types pour coter la vraisemblance du scénario opérationnel : » | Remplacer « Vous pouvez envisager trois approches pour coter la vraisemblance du scénario opérationnel » par « Voici trois approches proposées pour estimer la vraisemblance du scénario opérationnel ». |
| 107 | Fond | [Fiches] 592 | L'échelle de probabilité est intéressante pour les attaquants, mais ne reflète pas la source de risque de type vengeur. Un interne avec les bons droits est quasi certain de réussir, mais tous ne le feront pas. | Nous proposons de changer la description « Probabilité de succès … » par « Probabilité de succès ou motivation à passer à l'acte … » | |
| 108 | Forme | [Fiches] 629-635 | Cette notion d'expertise n'est pas toujours comprise par les clients, voire jugée suffisante. | Il pourrait être mentionné l'ajout de résultat d'audit technique pour corroborer (ou non) les résultats obtenus en ateliers, qui restent de niveau déclaratif. | Ajouter la phrase suivante entre les deux phrases (ligne 632) : « Ces estimations déclaratives peuvent utilement être justifiées par d'autres travaux (audits techniques, contrôle interne, *etc*.). ».<br>Il est même recommandé d'utiliser les scénarios opérationnels pour orienter un audit technique. |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 109 | Forme | [Fiches] 636-768 | Les nombreuses notes associées aux approches Standard et Avancée sont plus que des notes, ce sont des mises en garde vis-à-vis du risque de vouloir aller très (trop) loin dans l'automatisation de calculs de vraisemblance qui sont pourtant particulièrement délicats puisque devant exprimer, entre autre, une modélisation de la malveillance humaine… (cf. mise en garde sur les biais, etc.) cependant il n'y a nulle part la mise en garde sur le fait que ces approches sont à réserver aux praticiens aguerris qui ont une capacité de recul suffisante, et non aux débutants qui ne peuvent avoir cette capacité de recul…<br>Il paraît dangereux d'inciter à croire que la vraisemblance est (relativement) calculable alors même qu'en l'état actuel de l'état de l'art et en particulier avec les méthodes à base qualitative, l'évaluation de la vraisemblance ne se fait absolument pas sur une base rationnelle et démontrable (au sens mathématique du terme) ! La fiche méthode n°8 prend un certain nombre de précautions oratoires cependant est-ce suffisant ? Est-ce suffisamment explicite alors que cela se trouve précisé dans des « notes » qui peuvent être considérées comme +/-« facultatives » par certains lecteurs ? | Au minimum ajouter une mise en garde explicite en préambule de la fiche méthode 8 ou au niveau des parties 3 et/ou 4, précisant que :<br>« L'évaluation de la vraisemblance est tout sauf une activité triviale, cela n'est pas de simples enchaînements de calculs qui pourraient apparaître au premier abord « assez facilement automatisables », aussi les approches Standard et a fortiori Avancée, avec leur approche par consolidation des cotations des actions élémentaires, sont à réserver aux praticiens aguerris de l'analyse de risque. » | Ajouter une phrase d'introduction en 638 :<br>« L'objectif est ici de hiérarchiser la vraisemblance des scénarios opérationnels. De nombreuses techniques peuvent être employées. Ainsi, pour des études simples, il peut suffire de classer les scénarios opérationnels par ordre décroissant de vraisemblance, au jugé. Toutefois, pour des études plus riches, deux techniques sont proposées.<br>NOTE L'estimation de la vraisemblance n'est pas toujours triviale et facilement automatisable. Elle peut demander une véritable expertise afin de tenir compte des réalités techniques et d'assurer la cohérence méthodologique. ». |
| 110 | Forme | [Fiches] 647 | La formule mathématique est juste, mais a beaucoup de mal à être comprise. | Écrire en français ce qu'elle signifie : « L'arbre d'attaque doit être vu comme un automate. Les actions élémentaires sont les opérations de l'automate et les étapes d'attaque sont les états de l'automate. La vraisemblance de chaque étape est la | Ajouter l'explication suivante sous la formule de la ligne 647 :<br>« Le graphe d'attaque peut être vu comme un automate : les actions élémentaires |

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| | | | | vraisemblance maximum de chaque parcours possible de l'arbre d'attaque pour arriver à cette étape (tout mode opératoire possible) ». | représentent les opérations de l'automate et les étapes d'attaque représentent ses états : la vraisemblance de chaque étape est la vraisemblance maximale des différents parcours possibles au sein du graphe d'attaque pour y parvenir. ». |
| 111 | Forme | [Fiches] 665 | La méthode de calcul n'est pas aisée à comprendre et l'exemple donné peut être pas très clair (le chiffre entre parenthèses représente la probabilité héritée de la phase précédente ?) | Pour simplifier l'explication, nous parlons de goulot d'étranglement par phase et c'est lui qui influe sur la vraisemblance finale. Il faudrait peut-être davantage vulgariser cette partie qui n'est pas simple à comprendre (et visiblement appliquée différemment par tout le monde, solution labellisée comprise). | |

### 1.1.7 [Guide] et [Fiches] Atelier 5

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 112 | Fond | [Guide] 727 | La « synthèse des scénarios de risque » équivaut à l' « évaluation des risques » dans l'ISO/IEC 27005. | Changer « Réaliser une synthèse des scénarios de risque » par « Évaluer les risques ». | |
| 113 | Fond | [Guide] 737+ | Bien que pour une cohérence d'ensemble il puisse être nécessaire d'intituler cet atelier "Traitement du risque", nous pouvons nous retrouver dans des cas où il n'y a pas de "risque" à traiter, mais malgré tout réaliser cet atelier, essentiellement pour la réalisation du PACS. Ceci est valable pour toutes les analyses où l'atelier 4 n'a pas été réalisé. | Préciser dans l'atelier 5 qu'il est possible de ne pas avoir de risques à cette étape, et que dans ce cas-là, il faut uniquement appliquer le PACS. | En admettant qu'il est possible de définir un mode opératoire « haut niveau » lors de l'atelier 3 pour estimer une vraisemblance des risques dans le cadre d'une étude sans atelier 4. |
| 114 | Fond | [Guide] 744 | Attention si les risques sont exprimés en utilisant les scénarios opérationnels, l'objectif visé à la base du scénario peut impacter des valeurs métiers dont la gravité est différente. | Ajouter une note : « Si les risques sont exprimés en utilisant les scénarios opérationnels, l'objectif visé à la base du scénario peut impacter des valeurs métiers dont la gravité est différente. Veillez à vérifier que chemin d'attaque considéré vise la valeur métier dont l'ER correspondant à bien le bon niveau de gravité. » | « Si les risques sont exprimés en utilisant les scénarios opérationnels, l'objectif visé à la base du scénario peut engendrer des ER dont les gravités sont différentes. Veillez à vérifier que le chemin d'attaque considéré vise la valeur métier dont l'ER correspondant au bon niveau de gravité. »<br>Commentaire à clarifier : d'où sort la notion de gravité d'une valeur métier ? la gravité est liée à un ER et non à une VM. L'auteur veut-il parler de la criticité métier d'une VM ? |
| 115 | Fond | [Guide] 755 (note) | Attention certains utilisateurs oublient les risques non délibérés et non ciblés | Ajouter : les ER liés à des risques non délibérés ou non ciblés devront également | Il ne s'agit pas d'un « oubli », mais d'une |

| | | | | | |
|---|---|---|---|---|---|
| | | | | être analysés pour vérifier que les moyens de traitement répondent aux besoins.<br><br>Les risques (atelier 1) non traités dans l'approche par scénario peuvent être rappelés à des fins de communication et de sensibilisation. Ils permettront également de vérifier que les mesures de traitement sont adaptées.<br>Ils peuvent par exemple être exprimés sous la forme d'évènements redoutés. L'évaluation de ces risques peut s'appuyer sur l'évaluation de la gravité et sur une estimation de vraisemblance à dire d'expert | volonté affichée de traiter les risques non intentionnels et non ciblés dans le socle de sécurité et non par scénarios. La définition de scénarios pour illustrer ce type de risques peut être pertinente à des fins pédagogiques, mais ne doit pas être pour autant encouragée dans la méthode. |
| 116 | Fond | [Guide] 755 | Les utilisateurs ont du mal à trouver des méthodes pour représenter les risques | Ajouter : « l'expression des risques peut être basée sur les évènements redoutés, les scénarios stratégiques ou les scénarios opérationnels, selon la granularité et finalité de l'étude. | L'esprit de la méthode est que les risques soient décrits par les scénarios stratégiques. Ce point est à préciser, car effectivement non mentionné de manière explicite dans le guide.<br><br>Ajouter la phrase suivante après la ligne 755 :<br>« De manière générale, les risques sont décrits par scénarios stratégiques. Toutefois, il peut être envisagé de les identifier et exprimer de différentes manières selon l'objectif de l'étude et ses destinataires : par événements redoutés, par sources de risques, par scénarios stratégiques, par |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | scénarios opérationnels, ou autres. ». |
| 117 | Forme | [Guide] 762 | En pratique, les mesures sont identifiées hors de l'atelier 5. | La remarque ici est de ne pas confondre la stratégie d'acceptation des risques résiduels (vu dans les étapes suivantes) et ici le choix de traitement pour définir ou non des mesures.<br>Peut être faut-il simplement changer les termes « acceptabilité », « tolérable sous contrôle » et « inacceptable » dans le tableau, profit respectivement de « décision de traitement du risque », « niveau de sécurité à renforcer à moyen ou long terme » et « niveau de sécurité à renforcer à court terme | |
| 118 | Fond | [Guide] 762+ | Dans un nombre important de situations, il n'est pas possible au moment de l'analyse de risques de donner une échéance pour la mise en place des mesures de sécurité, même de manière approximative. Ceci est dû au fait que des investigations supplémentaires sont nécessaires pour réaliser ces estimations vis-à-vis du projet ou que les personnes aptes à valider l'échéance proposée ne sont pas présentes, puisqu'il peut y avoir des impacts budgétaires sur d'autres projets. | Dans le PACS, proposer 2 méthodes de gestion des mesures de sécurité :<br>- gestion à l'échéance : c'est ce qui est actuellement proposé. Il s'agit de la colonne "Échéance"<br>- gestion par priorité : définir plusieurs niveaux de priorité et donner une estimation de la charge nécessaire à la réalisation de la mesure de sécurité. Créer 2 nouvelles colonnes "Priorité" et "Charge estimée". Pour cette dernière, préciser qu'il s'agit d'une estimation qui ne tient pas compte des contraintes projet actuelles. | |
| 119 | Fond | [Guide] 787-790 | Le travail d'identification des mesures associées aux actions élémentaires (des scénarios opérationnels) est dans la pratique réalisé lors de l'élaboration de ces scénarios au cours de l'atelier 4.<br>Dans l'atelier 5, il s'agit de réaliser des arbitrages selon les décisions de traitement des risques associés à ces scénarios. | Remettre dans l'atelier 4 l'activité d'identification des mesures associée aux scénarios opérationnels. | |

| | | | | | |
|---|---|---|---|---|---|
| 120 | Fond | [Guide] 789-790 | "diminuer sa **probabilité** de réussite" : le terme "probabilité" ne nous paraît pas adapté, car cela sous-entend une évaluation quantitative. Or, nous devons généralement faire appel à des métriques qualitatives pour calculer la vraisemblance. | Remplacer le terme "probabilité" par "potentialité". | |
| 121 | Fond | [Guide] 795 | Il est souvent reproché de ne pas pouvoir constater la réelle influence d'une mesure sur le niveau des risques. Le dire d'expert ayant parfois ses limites. | Afin d'apporter plus de précision, nous lions nos mesures aux AE afin d'apporter plus de finesse sur les vraisemblances résiduelles, mais le travail pourrait aller plus loin, avec une notion de poids à donner aux mesures par exemple, voire de liens entre elles.<br><br>À chaque mesure sont associés […] ainsi que l'action élémentaire afin d'identifier rapidement sur quel risque l'action vient peser. Une notion de poids peut également être donnée afin de distinguer l'importance de la mesure dans la réduction du niveau du risque | Toutefois, le commentaire est également valable pour d'autres composants des risques (écarts au socle de règles, sources de risques, événements redoutés, impacts, *etc*.). |
| 122 | Fond | [Guide] 795-800 | Il apparaît qu'il y a souvent un amalgame entre la notion de mesure de sécurité et d'action. Le PACS devrait contenir uniquement les mesures de sécurité et un plan d'action devrait être établi à la suite, avec les actions qui permettront la mise en place des mesures de sécurité. Le plan d'action est à réaliser à la suite et non pendant l'analyse de risques. | Ajouter une précision sur la différence entre un PACS et un plan d'action. Indiquer que le plan d'action est à réaliser en dehors de l'analyse de risques. | Remplacer « Documentez l'ensemble de ces mesures de traitement dans un plan d'amélioration continue de la sécurité (PACS) » par « Pour chaque mesure issue de chaque atelier, formaliser la/les action(s) permettant de la mettre en œuvre au sein d'un plan d'amélioration continue de la sécurité (PACS) / plan de traitement des risques » dans la ligne 795. |

| | | | | | |
|---|---|---|---|---|---|
| 123 | Fond | [Guide] 797 | Il n'est pas clairement dit de quoi est composé le PACS. | Le PACS étant composé des mesures issues de l'atelier 1, de l'atelier 2, de l'atelier 3 et de l'atelier 4 et des mesures précédemment citées dans l'atelier 5.<br>Le niveau du risque résiduel évoluera principalement au niveau de la vraisemblance suite à la mise en œuvre des actions du PACS. Néanmoins la gravité résiduelle peut diminuer dans le cas où les événements redoutés associés ne se réaliseraient pas dans leur totalité. | |
| 124 | Fond | [Guide] 804+ | Il y a souvent débat (et désaccord) sur la gravité résiduelle, savoir si elle peut être diminuée ou non vis-à-vis du net. | À voir si le Club EBIOS et l'ANSSI veulent se positionner sur ce débat, mais une note au niveau de la fiche pourrait être intéressante. Côté ADVENS, nous pensons qu'une gravité résiduelle peut être diminuée dans des cas extrêmement précis et dans la seule condition où l'évaluation initiale des ER ne serait pas réalisée dans sa totalité. | |
| 125 | Fond | [Guide] 813 (note) | Les risques résiduels sont souvent exprimés par les utilisateurs de la méthode de manière identique aux risques bruts précédents. Ainsi, les décisions d'acceptation ou non du risque résiduel ne se font que sur l'appréciation du niveau de risque et donc sans argument concret. | Ajouter dans la note : « N'hésitez à reformuler le risque pour faire clairement apparaître le risque résiduel persistant dans l'expression du risque ». | |
| 126 | Forme | [Guide] 828 | Le commentaire ne fait pas référence au risque lié à la menace bioterroriste, de plus la source n'est pas rappelée dans les formulations des risques. | Rappeler le numéro du risque qui correspond pour faciliter la lecture : R4 et R5. | |
| 127 | Forme | [Guide] 833 | Les indicateurs de pilotage ne sont pas définis ni dans le guide, ni dans les fiches, ni dans les définitions | Ajouter : « Reprendre chaque mesure (socle et mesures complémentaires issues de l'analyse) et indiquer des fréquences et moyens de contrôle, ainsi que des preuves à collecter. ». | |

### 1.1.8 [Guide] et [Fiches] Termes, définitions et bibliographie

| # | Type | Localisation | Constats | Proposition | Complément |
|---|---|---|---|---|---|
| 128 | Fond | [Guide] 870+ | Certains termes définis ne correspondent pas à des concepts importants de la méthode EBIOS *Risk Manager*. Ils ne devraient pas être définis de la même manière que les concepts de la méthode. | Supprimer les termes qui ne correspondent pas à des concepts d'EBIOS *Risk Manager* :<br>- correctif de sécurité ;<br>- déni de service ;<br>- ingénierie sociale ;<br>- point d'eau ;<br>- surface d'attaque ;<br>- test ou audit d'intrusion.<br>Éventuellement, les décrire en notes de bas de page là où ils sont employés. | |
| 129 | Fond | [Guide] 989 | La notion de « menace » n'est pas toujours bien appréciée quand on parle des parties prenantes. | Changer « niveau de menace » par « niveau de dangerosité ». | |
| 130 | Fond | [Guide] 1017 | | Ajouter dans la définition de la partie prenante :<br>Un élément doit être considéré comme une partie prenante ou un bien support selon la propriété.<br>Un bien est partie prenante si le commanditaire du périmètre de l'étude n'en est pas responsable. Si le bien est sous la responsabilité du commanditaire, c'est un bien support. | |
| 131 | Fond | [Guide] 1077-1086 | La définition de « stratégie de traitement du risque » ne correspond pas à une définition, mais à une explication | Déplacer la « définition » en note de bas de page à l'endroit où le terme est employé. | |

# 2 Retours d'expérience

L'objectif de ce chapitre est d'illustrer les retours d'expérience des praticiens de la méthode et les opportunités d'améliorations de la méthode EBIOS *Risk Manager* à partir de plusieurs cas d'usages concrets.

**L'ensemble de ces contributions et propositions d'actions n'ont pas été analysées ou évaluées par le Club EBIOS. Elles sont présentées ici telles que reçues par les contributeurs.**

**Elles feront éventuellement l'objet de travaux complémentaires au sein des groupes de travail du Club.**

## 2.1 Atelier 1

### 2.1.1 Cadrage de la réalisation d'une étude (3)

#### ORGANISATION DE LA CONDUITE D'UNE ETUDE : CAS D'UNE ANALYSE SIMPLE

Contexte

Cadre de la conduite d'une étude dont les finalités sont simplifiées (étude préliminaire ou étude du socle).

Difficulté(s) / intérêt(s) et solution(s)

Les utilisateurs ont beaucoup de mal à comprendre la grille pour la sélection des ateliers à mener. Notamment :

- ils ont du mal à comprendre comment il est possible de mener une étude préliminaire des risques sans avoir mené d'atelier 4, et donc sans avoir de technique dans l'atelier 3 pour apprécier la vraisemblance. Il manque une technique pour apprécier un niveau de risque des scénarios stratégiques (peut-être dans les fiches) ;
- ils ont du mal à comprendre comment l'approche par conformité – si on se limite à ça - peut conduire à une identification des risques. Il manque une technique pour aider à construire des risques.

#### NOTE D'ORIENTATION

Contexte

EBIOS *Risk Manager* propose de dérouler différents ateliers en fonction du besoin.
Le formalisme de ce cadrage initial doit être plus formalisé pour définir les documents à produire, le niveau de sécurité attendu, *etc*.

Difficulté(s) / intérêt(s)

Formaliser les attendus pour une étude de sécurité (e.g. : Homologation d'un système, phase d'appel d'offres, *etc*.).

Solution(s)

Proposer une note d'orientation ou le point de contact projet est défini, les documents à produire, les ateliers à dérouler, le niveau de sécurité nécessaire et le socle de sécurité associé (voir référentiel de socle).

#### PERTINENCE DE LA SPECIFICATION DU RYTHME DES MISES A JOUR (CYCLES STRATEGIQUES ET OPERATIONNELS)

Contexte

Analyse de risque sur projet.

Difficulté(s) / intérêt(s)

D'une part, le chapitre sur les différents usages d'EBIOS *Risk Manager* prévoit plusieurs usages très différents de la méthode. D'autre part, l'atelier 1 requiert la définition du rythme des mises à jour (cycles stratégiques et opérationnels). Cette spécification est pertinente lorsqu'on déroule les 5 ateliers. Elle devient beaucoup moins claire lorsque l'étude ne prévoit qu'une sélection réduite d'ateliers, e.g., ateliers 1 et 5.

Solution(s)

Le guide pourrait être plus explicite sur la façon de procéder dans la durée pour les mises à jour et la pertinence des cycles selon les usages de la méthode.

### 2.1.2 Évaluation de la conformité au socle de règles (9)

LA DETERMINATION DU SOCLE EST UN SUJET DIFFICILE

Contexte

Lors d'une analyse de risques sur un projet, le socle est l'une des réflexions majeures.
Lorsqu'aucun résultat d'audit n'est disponible, que doit-on faire ?

Difficulté(s) / intérêt(s)

Beaucoup se retrouvent bloqués à ce niveau :

- quelle portée du socle : sur la partie prenante ? sur les biens supports uniquement ?
- en l'absence d'audit ou de contrôle, comment considérer les écarts ?

Solution(s)

Nous suggérons de considérer le socle selon plusieurs approches combinées :

- le socle pour répondre aux évènements redoutés préalablement identifiés. Il s'agit là de choisir les mesures, cohérentes avec les besoins de sécurité exprimés, qui ne nécessitent aucun arbitrage ou pour lesquels la suite de l'étude n'apporte pas d'éléments de décision supplémentaires ;
- les écarts au socle, issus d'un audit et pour lesquels des mesures peuvent être envisagées dès cette étape et qui seront reprises à la fin de l'étude ;
- le socle comme exigence législative ou réglementaire, où dans l'analyse il s'agit de produire des mesures (soit complémentaires liés à un résultat d'audit, soit adaptées au contexte de l'étude). Là encore ces mesures seront reprises à la fin de l'étude.

IDENTIFICATION DE RISQUES NON DELIBERES (OU NON CIBLES)

Difficulté(s) / intérêt(s)

La direction générale souhaite avoir une vision complète des risques SSI pesants sur son organisation ou son projet. La direction veut être informée, dans une analyse des risques, des risques pesant sur leur SI qu'ils soient d'origine délibérée (et/ou non ciblés) ou non.

L'approche EBIOS *Risk Manager* est vécue comme très complète, notamment la partie des scénarios est très parlante et rencontre une forte satisfaction.

Les utilisateurs comprennent que ces risques non délibérés et non ciblés ne nécessitent pas une analyse par scénario, mais souhaiteraient qu'ils soient intégrés dans la cartographie des risques (par exemple, les risques de panne ou de sinistre).

Solution(s)

Il manque peut-être une fiche technique pour fabriquer simplement des risques d'origine non délibérée à partir des écarts du socle (l'absence de mesures étant un risque ou comme dans EBIOS 2010 à partir des vulnérabilités des biens supports). Ils pourraient alors se retrouver dans la matrice de risques finale.

### DIFFICULTE DE CHOIX DU SOCLE DE SECURITE

Contexte

Analyse de risque (atelier 1) dans le cadre de prestations.

Difficulté(s) / intérêt(s)

Faire un bilan de la conformité peut être compliqué (voire fastidieux) si le système étudié est soumis à plusieurs référentiels dont les règles se recoupent, ou se complètent. Par exemple un système peut être soumis à la réglementation sur le DR (II 901) et doit être conforme à la PSI définie pour le Groupe.

Solution(s)

S'accorder sur une structure unique de référentiel. Mais cela nécessite de faire la synthèse de tous les référentiels applicables selon cette structure. Ce travail est loin d'être négligeable, mais il permet de faire un bilan global de la conformité.

### METHODE D'ANALYSE DU SOCLE DE SECURITE PAS ASSEZ DETAILLEE

Contexte

Toute analyse EBIOS *Risk Manager* qui comprend l'analyse du socle de sécurité.

Difficulté(s) / intérêt(s)

Comment et à quel niveau de granularité faire l'analyse du socle de sécurité ?
Les recommandations de l'ANSSI sont un peu floues à ce sujet.

Si on demande directement au client de se positionner sur un niveau de conformité pour chaque référentiel, il ne sait pas comment répondre dans la majorité des cas. Il est le plus souvent capable de citer une ou deux non-conformités dont il se rappelle, mais ça va rarement plus loin.

Si on balaye chaque référentiel exigence par exigence, ça passe si le socle est constitué des 42 mesures d'hygiène de l'ANSSI, mais ça devient impossible si le nombre d'exigences est trop élevé. Par ailleurs c'est extrêmement rébarbatif à faire en atelier.

Solution(s)

À la place de demander au client de se positionner sur un niveau de conformité pour chaque référentiel, on lui demande de nous donner des éléments pour nous donner confiance dans la mise en application de ce référentiel sur le SI cible : organisation définie pour y répondre, budget alloué, activités mises en œuvre : support sécurité projet, Audit interne/externe, contrôle permanent, tableau de bord et KPI, *etc*.

Lorsque le client a beaucoup d'éléments à nous donner, on se rend compte dans la majorité des cas que les non-conformités/vulnérabilités sont déjà identifiées ailleurs, dans d'autres documents qu'il suffit de récupérer.
Lorsque le client a peu d'éléments à communiquer, on juge le niveau de conformité au référentiel « non conforme » et on ne cherche même pas à identifier les vulnérabilités détaillées.

Cette approche permet d'analyse le socle de sécurité de façon rapide en atelier tout en amenant des discussions entre les différents acteurs très intéressantes. « *Au lieu de nous dire ce qui ne va pas essayer de nous rassurer sur ce que vous faite pour que ça aille bien…* ».

En revanche, à elle seule, cette approche ne suffit pas pour récupérer l'ensemble des informations sur la sécurité du système cible. C'est la raison pour laquelle nous la complétons par la description des mécanismes de sécurité existants qui sont utiles à l'évaluation des scénarii de risque de niveau opérationnel.
Cela permet de nous concentrer uniquement sur le plus important et de définir un niveau de granularité pour ces mesures adaptées à la nécessité de les associer à nos risques. (il est très difficile d'associer de façon cohérente, 250 exigences de sécurité sur chaque action élémentaire, alors que cela reste possible avec 30 mesures de sécurité de plus haut niveau).

## ÉTUDE DU SOCLE DE SECURITE

Contexte

Lors de missions d'analyse de risque dans des organismes avec une faible maturité cyber.

Difficulté(s) / intérêt(s)

Chez des clients manquant de maturité, la PSSI n'est pas appliquée, ni certaines bonnes pratiques basiques.
Lors de l'atelier 1, l'équipe découvre des mesures de sécurité et des référentiels à appliquer alors que le produit est quasi-fini. Par exemple :

- on demande au consultant de justifier de l'utilité de l'application des correctifs de sécurité (en général, pas uniquement pour une exception) ;
- hébergement non conforme aux exigences du référentiel (étranger, mutualisation, accès en administration depuis internet, *etc*.) ;
- prestataire ou sous-traitant ne pouvant respecter le socle de sécurité ;
- des écarts tellement importants que les ateliers suivants ne sont pas utiles.

Solution(s)

Suivant le contexte et les missions, plusieurs stratégies ont été possibles :

- NO-GO les besoins de sécurité basiques n'ont pas été pris en compte dans le cahier des charges, même les bonnes pratiques basiques ne sont pas respectées. L'analyse de risque déclenche une reprise de la phase conception du projet. (EBIOS *Risk Manager* a bien fonctionné, mais d'un point de vue client la mission est un échec) ;
- réaliser un mini audit « en bonne intelligence » pour lister les écarts et s'accorder sur un plan d'action ; ensuite l'analyse considère les écarts résiduels prévus.

Il faut noter que ces « solutions » impliquent des coûts et des délais et sont toujours une source de friction.
Il faudrait une fiche consacrée au socle de sécurité :

- sa définition au plus tôt et son intégration au cahier des charges ;
- l'étude des écarts qui ne doit pas se transformer en audit et plan de mise en conformité. Il s'agit d'avoir une vision de l'état d'application du socle. EBIOS *Risk Manager* n'est pas là pour définir et faire appliquer un socle de sécurité.

## REFERENTIELS COMMUNS DE SOCLE

Contexte

L'atelier 1 ne donne que très peu d'outils sur la constitution d'un socle de sécurité.
Traiter les *non-compliances* du socle.

Difficulté(s) / intérêt(s)

Tout le monde réinvente la roue dans son coin et définit ses référentiels à partir de différents documents de référence.
Difficulté d'avoir des socles homogènes et leur constitution est très chronophage.
Comment traiter les *non-compliance* du socle dans les scénarii ?

Solution(s)

Mise à disposition de référentiels de socle de sécurité (intégration des guides ANSSI).
Utilisation du formalisme OSCAL (comme le NIST).
Faire référence à l'ISO 27002 qui devrait utiliser ce formalisme prochainement.
Identifier une non-compliance du socle comme une vulnérabilité sur un bien support à traiter dans l'atelier 4.
Proposer différent niveau de mesure de sécurité en fonction du niveau de protection recherché (voir note d'orientation) :

| SRs and REs | | SL 1 | SL 2 | SL 3 | SL 4 |
|---|---|---|---|---|---|
| **FR 1 – Identification and authentication control (IAC)** | | | | | |
| SR 1.1 – Human user identification and authentication | 5.3 | ✓ | ✓ | ✓ | ✓ |
| SR 1.1 RE 1 – Unique identification and authentication | 5.3.3.1 | | ✓ | ✓ | ✓ |
| SR 1.1 RE 2 – Multifactor authentication for untrusted networks | 5.3.3.2 | | | ✓ | ✓ |
| SR 1.1 RE 3 – Multifactor authentication for all networks | 5.3.3.3 | | | | ✓ |
| SR 1.2 – Software process and device identification and authentication | 5.4 | | ✓ | ✓ | ✓ |
| SR 1.2 RE 1 – Unique identification and authentication | 5.4.3.1 | | | ✓ | ✓ |

ISA/CEI 62443 *example*

## CHOIX DE L'APPROCHE DANS LE TRAITEMENT DES RISQUES NON INTENTIONNELS SI LE SOCLE DE SECURITE N'EST PAS MATURE

Contexte

Lors d'une analyse de risque d'un processus métier.

Difficulté(s) / intérêt(s)

La méthode se concentre sur des cas d'études précis, en l'occurrence des actions malintentionnées. La méthode mentionne également le besoin d'établir un socle de sécurité qui servira entre autres lors de l'atelier 4.
Par contre la méthode ne mentionne rien du ne niveau de maturité du socle de sécurité. Elle part du principe qu'avec un socle mature, les risques non intentionnels et/ou environnementaux sont traités.
Cependant, aucune approche n'est faite dans le cas d'un socle non mature et donc rien n'explique comment gérer les risques non intentionnels.

Solution(s)

Nous avons hésité sur l'approche à adopter lorsque nous avons commencé à utiliser la méthode en 2019. Nous hésitions à seulement remonter une non-conformité par rapport à un standard de sécurité (en l'occurrence ISO27002) ou aller plus loin. C'est cette dernière approche que nous avons choisie en identifiant une non-conformité et en faisant découler un risque non intentionnel que nous évaluons (en termes d'impact/gravité) à l'aide d'un évènement redouté.
Enfin, nous évaluons un niveau de vraisemblance en méthode express (à la grosse louche).
Depuis qu'ORES a acheté l'outil Agile *Risk Manager*, nous avons encore fait évoluer notre approche.
Nous créons un couple SR/OV de type « Erreur non intentionnelle » que nous lions à l'évènement redouté adéquat. Et nous évaluons en méthode express le niveau de vraisemblance du scénario.

## L'EVALUATION DE LA CONFORMITE EST FLOUE ET A TROP GROS GRAIN

Contexte

Analyse de risque projet ou système (ateliers 1 et 3).

Difficulté(s) / intérêt(s)

EBIOS *Risk Manager* ne détaille guère comment doit être faite l'évaluation de conformité au socle de sécurité. On devine qu'elle est globale. L'IEC 62443 prévoit le découpage du système étudié en zones et conduits. L'évaluation de la conformité se fait par zone et conduit. Il est très bien possible qu'une mesure soit correctement appliquée sur une zone, partiellement appliquée sur une autre, et non appliquée sur une troisième. Ceci est très important pour évaluer la vraisemblance des scénarios opérationnels, et pour la définition du plan d'action.

Solution(s)

Il n'est pas forcément nécessaire de reprendre les notions de zones et conduits, mais il faudrait quelque chose d'équivalent, en termes de partitions, et/ou de biens supports (si la granularité des biens supports est grosse).

UTILISATION DU SOCLE DE SECURITE

Difficulté(s) / intérêt(s)

L'usage (et la compréhension générale) du socle de sécurité mènent à penser qu'un niveau de maturité insuffisant (mauvaise couverture du socle) doit amener à ne pas réaliser les ateliers 2/3/4.Cette pratique a pour effet négatif de réduire la démarche à une simple phase d'audit/correction, ce qui réduit la valeur ajoutée de l'analyse de risques.

Solution(s)

Proposition : Expliciter dans la méthode la possibilité de poursuivre l'analyse même en présence d'un niveau de maturité faible, mais en considérant le socle comme complété. Il faudrait aussi pouvoir différencier les risques issus du socle de ceux issus des étapes suivantes de l'analyse.

### 2.1.3 Identification des missions et valeurs métier (2)

LIEN ENTRE MISSION ET VALEUR METIERS

Contexte

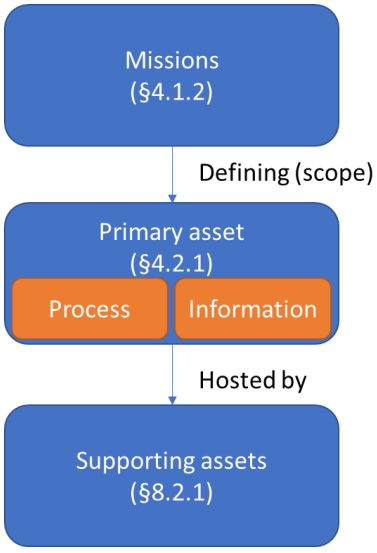
Bien cadrer son analyse et faire le tri dans les VM.

Difficulté(s) / intérêt(s)

Dans le guide et les supports de formation il ne transparait pas assez comment choisir les valeurs métiers. E.g. : dois-je intégrer la fonction RH, paie, *etc*. dans mon analyse ?

Solution(s)

Seules les VM qui ont un lien direct avec la mission sont à identifier :




### 2.1.4 Valeur métier : Intégration de l'information au processus ?

Contexte

Une valeur métier peut être une information ou un processus.

Difficulté(s) / intérêt(s)

Faut-il traiter le processus séparément de l'information que le processus traite ou intégrer cette dernière au processus. Il est nécessaire d'avoir une aide à la décision.

Solution(s)

Séparer les 2 quand les besoins de sécurité sont différents et quand il y a vraiment un intérêt à les dissocier.

### POSITIONNEMENT DE L'ATELIER 1

Contexte

Lors de missions ponctuelles d'analyse de risque en vue d'une d'homologation.

Difficulté(s) / intérêt(s)

Chez des clients manquant de maturité, la sécurité n'est pas prise en compte dès la conception du produit, l'Atelier 1 est réalisé alors que le produit est quasi-fini et soulève des questions importantes qui n'avaient pas été tranchées.

On en arrive à des contradictions :

- besoins fonctionnels incompatibles avec la sécurité (ex : permettre à un utilisateur de consulter des informations sensibles depuis un poste non maîtrisé) ;
- prestataire ou sous-traitant ne pouvant respecter le niveau de sécurité demandé.

Cette difficulté n'est pas liée directement à EBIOS *Risk Manager* mais à des projets avec des enjeux de sécurité importants qui n'ont pas été traités en amont et à un client qui « achète un rapport » et n'est pas dans une logique de maîtrise des risques de son organisme.

Solution(s)

Il est possible de réaliser une mission EBIOS *Risk Manager* pour « valider » la sécurité d'un projet lorsque celui-ci ne présente pas d'enjeu particulier (autres projets du même type déjà réalisés, maturité cyber de l'organisme et de l'équipe projet, *etc*.), mais la bonne pratique est de réaliser les ateliers 1, 2 et 3 avant d'investir dans la réalisation.

### L'EXERCICE DU BIA DANS L'ATELIER 1

Contexte

Lors d'analyses de risque dans le cadre d'homologations de SI.

Difficulté(s) / intérêt(s)

La lecture en première approche des activités b et c de l'Atelier 1 peut, pour un praticien débutant, les faire apparaître comme plus ou moins informelles et amener les acteurs de l'atelier à les réaliser sans forcément beaucoup de formalisme, amenant potentiellement de l'hétérogénéité d'une étude à l'autre…
*A contrario*, pour des acteurs plus aguerris, ces 2 activités leur font penser au BIA (i.e. *Business Impact Assessment*) que l'on déroule habituellement dans le cadre des plans de continuité et de reprise d'activité (cf. PCA/PRA). Cela leur donne l'impression de faire doublon (même si des critères de sécurité comme l'intégrité, voire la confidentialité, n'y sont pas toujours étudiés au même titre que le critère de disponibilité…) et surtout que l'approche est mieux cadrée/structurée côté gestion de la continuité…
Pour une bonne appropriation et acceptation de ces activités, il serait donc peut-être intéressant de structurer un peu plus ces activités, p.ex. en capitalisant sur l'état de l'art des BIA (y compris orientés « disponibilité », quitte à les généraliser aux autres critères de sécurité retenus telles l'intégrité, la confidentialité, *etc*.).

Solution(s)

Proposer de s'appuyer sur un exemple de trame un peu structuré pour mener les activités b & c de l'Atelier A, comme p.ex. en renvoyant à l'Annexe 1 du Guide de l'homologation de sécurité en 9 étapes simples (intitulée « Estimation rapide du besoin de sécurité d'un système d'information).
Également signaler la similitude avec l'exercice du BIA tel qu'habituellement mené par les équipes en charge de la gestion de la continuité d'activité et par là-même suggérer de se rapprocher d'eux pour capitaliser sur leurs pratiques du BIA (qui auront l'avantage d'être déjà connu des métiers), quitte à les compléter/enrichir pour répondre à tous les attendus au titre des activités b & c de l'Atelier 1.

## 2.2 Atelier 2

### 2.2.1 Appréciation des sources de risques et objectifs visés (5)

DETERMINATION DES SOURCES DE RISQUES ET OBJECTIFS VISES

Contexte

Cadre de l'intégration de la sécurité dans un projet.

Difficulté(s) / intérêt(s)

La réflexion sur les sources de risques est délicate.

Beaucoup utilisent les sources présentées dans les exemples du guide et l'adaptation au contexte est faible. Beaucoup également n'ont pas de connaissance des motivations de ces sources.

On constate souvent que les sources sont exprimées selon sa nature et sa motivation (terroriste, hacktiviste, *etc*.). De ce fait, les scénarios stratégiques et opérationnels sont répétés et souvent identiques.

Solution(s)

Selon la focale de l'étude, nous avons l'habitude de décrire et de dissocier les sources de risque selon les privilèges dont elle dispose (sans oublier leur motivation). L'avantage est que les scénarios opérationnels seront du coup bien différenciés.

DIFFICULTE D'ELABORATION DES SCENARIOS STRATEGIQUES

Contexte

Analyse de risque dans le cadre de prestations

Difficulté(s) / intérêt(s)

Le guide n'est pas clair concernant l'association des ER avec les couples SR/OV pour élaborer les scénarios stratégiques. Il semble possible qu'un scénario stratégique contienne plusieurs ER. Dans ce cas quelle est la règle pour estimer la gravité et finalement quel est l'intérêt de définir des ER ?

Solution(s)

Associer systématiquement un seul ER à un seul couple SR/OV :
Le scénario stratégique qui en découle est davantage cohérent et la valeur de la gravité s'en déduit automatiquement
De plus, lors de la phase de restitution, il est important de montrer aux responsables métier qui se sont exprimés sur les ER comment cette vision a été effectivement prise en compte dans la suite de l'étude.

SR/OV DES ISO

Contexte

Pour un couple SR/OV donné, le SR peut avoir plusieurs objectifs. Court, moyens et long terme.

Difficulté(s) / intérêt(s)

Difficulté de savoir si on doit identifier le OV court, moyen ou long terme, e.g. : je veux compromettre la BDD de FERRERO pour pouvoir obtenir la recette du Nutella et ainsi produire une copie pour récupérer des parts de marché.

Solution(s)

Dans la version DIS 27005 il y a la notion de DES (*Desired end state*) État final recherché qui vient compléter la notion d'objectif visé qui peut être un objectif intermédiaire.

#### PERTINENCE DES COUPLES SR/OV : AIDE INSUFFISANTE DANS LE GUIDE

Contexte

Atelier 2.

Difficulté(s) / intérêt(s)

Il est demandé à l'issue de l'atelier 2 de retenir les SR/OV les plus pertinents. La pertinence ne dépend pas que de la cotation Motivation x Ressources x Activité. Il faut aussi, entre autres, une bonne couverture des valeurs métier, et notamment de leurs événements redoutés les plus graves. Pour cela, il serait intéressant, à l'issue de l'atelier n°2, de connaître la couverture des valeurs métier et/ou des événements redoutés par les couples SR/OV, pour savoir si l'on a retenu le bon jeu de couples SR/OV. Actuellement c'est impossible, car l'association avec les événements redoutés se fait lors de l'atelier n°3, à travers les scénarios stratégiques.

Solution(s)

Établir une traçabilité entre SR/OV et VM/ER lors de la sélection des SR/OV les plus pertinents (atelier 2).
Note : cette traçabilité pourrait aussi être utile pour construire un argumentaire solide dans la méthode démontrant qu'EBIOS *Risk Manager* est apte à supporter un processus d'homologation / certification (cf. RETEX sur homologation / certification ci-dessus, §4.5).

#### IDENTIFICATION DES COUPLES SR/OV

Difficulté(s) / intérêt(s)

La phase d'identification des sources de risques fonctionne très bien avec les métiers, une fois exposées les catégories les plus connues. Par contre, la phase d'évaluation de la pertinence et la sélection en résultant sont beaucoup plus laborieuses et subjectives à réaliser : on va à la fois identifier ceux ayant le plus de ressources, de motivation, mais aussi essayer de conserver un panel représentatif. Or la méthode n'apporte pas de précision sur l'association des deux : comment évalue-t-on la représentativité d'un couple SR/OV ?

Solution(s)

Proposition : ajouter un critère explicite en sus de la pertinence permettant d'évaluer la représentativité (par exemple la *catégorie* de la source de risque), et utiliser la combinaison pertinence/représentativité explicitement pour réaliser ce filtrage.

### 2.2.2 Lien entre points de vue du défenseur et de l'attaquant (1)

#### LIENS ER/VM

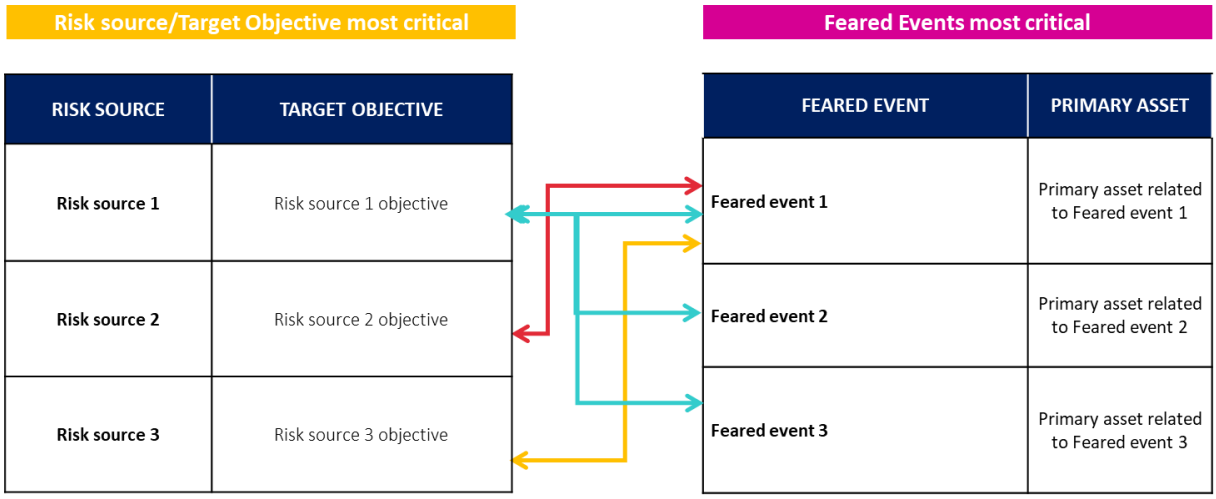
Contexte

Le livret de formation EBIOS propose des outils non présents dans le guide EBIOS *Risk Manager*, par exemple les liens entre VM et ER

Difficulté(s) / intérêt(s)

Visualiser les liens entre VM et ER.

Solution(s)




## 2.3 Atelier 3

### 2.3.1 Appréciation des parties prenantes (3)

CALCUL DU NIVEAU DE MENACE DES PARTIES PRENANTES

Contexte

Toute analyse avec des parties prenantes.

Difficulté(s) / intérêt(s)

Il n'est pas rare d'obtenir des incohérences dans le niveau de menace des parties prenantes et de devoir en sélectionner une avec un faible niveau pour la suite de l'analyse parce que le calcul ne reflète pas bien le niveau de menace ressenti par les acteurs.

Je ne suis pas mathématicien, donc je ne sais pas si la formule est la bonne, mais à un niveau opérationnel, ce qui semble poser problème sont les points suivants :

- le niveau de **confiance** n'est pas simple à évaluer et, il me semble qu'il a trop de poids dans le calcul. Cela reste quelque chose de très subjectif comme critère et cela a autant de poids que la **maturité** qui peut être évaluée de façon bien plus objective ;
- le niveau de **pénétration** n'est pas toujours facile à évaluer non plus et il ne prend pas en compte le fait de confier ou de recevoir des données sensibles en confidentialité /intégrité avec un tiers ;
- le niveau de **dépendance** est simple à évaluer, mais Il ne considère que la disponibilité des services fournis par un tiers. (à Par conséquent, ni la **dépendance**, ni la **pénétration** ne considère les besoins de confidentialité/intégrité des données qu'on confie à ou qu'on reçoit d'un tiers) ;
- le niveau de **maturité** est le critère sur lequel le client peut le plus agir, mais il n'a pas assez de poids dans le calcul. Par ailleurs il faudrait que la méthode guide beaucoup plus pour l'évaluation de ce critère. J'ai vu des analyses avec des maturités de parties prenantes externes évaluées au niveau 3-4 sur la base d'une interview avec le tiers et sans les moindres garanties contractuelles…. Ce qui peut avoir du sens au pays de Candy voir éventuellement au moyen Age. Mais de nos jours, que vaut un engagement oral fait au détour d'une réunion *Teams* dans le cadre de l'analyse de risque. Même si c'est tracé dans l'analyse ça n'aura une valeur que si éventuellement, l'analyse est annexée au contrat, ce qui n'est jamais le cas…

Solution(s)

Pour obtenir de meilleurs résultats en conservant la formule de calcul actuelle :

- on n'évalue le niveau de **confiance** que sur 2 niveaux : 1-Faible confiance ; 2-Confiance neutre ;

- pour la **pénétration** on précise un peu l'échelle en l'occurrence, le niveau de pénétration peut aussi être égal :
    - au niveau de classification I/C des données confiées au tiers ;
    - à 2 si on reçoit des données d'un tiers que l'on « *parse* » ou que l'on « *execute* » ;
- pour la **maturité** on itère encore sur des questionnaires ciblés qui cherchent avant tout à récupérer des « preuves » sur les niveaux d'engagement de la PP en termes de sécurité : Engagements contractuels en adéquation avec les besoins, Annexes de sécurité, certification de sécurité sur périmètre adéquat, résultats d'audit externe, pénalités, *etc*.

C'est un peu du bricolage, mais on est plus en phase avec les résultats que cela produit dans la majorité des cas.

### INTEGRATION DES PP DANS L'ECOSYSTEME

Contexte

Dans l'écosystème, toutes les parties prenantes ne sont pas liées à l'ensemble des Valeurs métiers. Quand l'écosystème devient trop complexe/dense on se perd dans les parties prenantes.

Difficulté(s) / intérêt(s)

Il est difficile d'utiliser la partie visuelle de l'écosystème pour réfléchir aux scénarii stratégiques. Il manque une identification visuelle de chaque PP et le lien qu'il a avec une ou plusieurs VMs.

Les scénarii stratégiques qui ne passent pas par une PP, mais en direct sur mon système n'ont pas un outil d'aide la visualisation.

Solution(s)

Filtrer l'écosystème par VM pour ne visualiser que les PP associées.

Utiliser l'outil de l'écosystème pour visualiser le système en lui-même permettrait d'utiliser la même boîte à outils pour définir le scénario stratégique interne au système et ceux externes (écosystème).

### MODELISATION DE L'ECOSYSTEME IMPLICITEMENT SUBORDONNEE A L'ATELIER 2

Contexte

Analyse de l'écosystème.

Difficulté(s) / intérêt(s)

Les sources de risque et objectifs visés retenus (atelier 2) sont cités comme une entrée de l'atelier 3. Or la modélisation de l'écosystème ne nécessite pas la connaissance des sources de risque et objectifs visés retenus. Cette connaissance n'est nécessaire que pour la modélisation des scénarios stratégiques, au même titre que la connaissance des valeurs métier.
Ce point est bien mis en avant dans le chapitre sur les différents usages d'EBIOS *Risk Manager*, en distinguant : (i) Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude ; et (ii) Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème. Cette distinction bien utile n'apparaît plus dans l'introduction de l'atelier 3.
Le schéma sur l'articulation des ateliers renforce cette dépendance.

Solution(s)

Reprendre l'introduction de l'atelier 3 pour bien ré-évoquer ce qui a été rapidement explicité dans le chapitre sur les différents usages d'EBIOS *Risk Manager*. Il ne s'agit pas de nier la dépendance, mais de laisser la porte ouverte à la simple évaluation de la criticité des parties prenantes.

### 2.3.2 Appréciation des scénarios stratégiques (4)

#### COMMENT MODELISER DES RISQUES PESANT SUR L'ECOSYSTEME

Contexte

Par exemple le cas d'une analyse de risque d'une application Web de sensibilité faible, mais exposant le reste du SI à des menaces provenant de l'Internet.

Difficulté(s) / intérêt(s)

L'analyse de l'écosystème (atelier 3) relèvera la menace que cette écosystème (environnement Internet) fait peser sur le projet. Par contre, il ne permettra pas de modéliser le risque que fait peser ce site Web à son écosystème (ici le SI environnant).

Solution(s)

Pour résoudre cette difficulté, nous avons l'habite d'ajouter une mission et une valeur métier qui est de protéger l'écosystème dans lequel le SI est placé. Ainsi, un évènement redouté sera défini comme la compromission possible du SI environnant par attaque par rebond de la cible de l'étude.

#### DIFFICULTE A DEFINIR, ECHANGER ET REPRESENTER LES SCENARIOS STRATEGIQUES

Contexte

Lors d'analyse de risque projet/homologation ou sur une organisation (type SMSI).

Difficulté(s) / intérêt(s)

L'atelier 3 au niveau des scénarios stratégiques comme définis est très complexe à réaliser. S'il est réalisé avec le Métier, ils n'ont généralement que très peu d'avis sur le sujet et renvoient vers l'IT. S'il est réalisé avec l'IT, il ne rentre pas suffisamment dans le détail et est plus intéressé par les scénarios opérationnels.
Il reste néanmoins intéressant à notre niveau pour se focaliser précisément sur les intentions des sources de risques avec les bons liens des événements redoutés, mais cela reste plus de l'avis d'expert que de réels échanges constructifs avec les clients.

De plus la représentation graphique n'apporte que très peu d'intérêt étant donné sa simplicité. Elle pourrait être passée en conseillée dans une note.

Solution(s)

Cet atelier est souvent réalisé de notre côté, avec envoi pour avis, mais souvent sans réponse.
De plus, nous privilégions la factorisation des SS par OV et surtout chemin d'attaque, pour éviter de les démultiplier et lire plusieurs fois le même chemin (toutes les sources externes emploient souvent le même chemin, avec plus ou moins de facilité, mais les démultiplier n'apportent pas grand-chose, si ce n'est de perdre le lecteur).

Cet atelier est le seul qui n'a pas de fiche méthode associée, alors qu'il est bien différenciant avec l'ancienne méthode.

Cette étape pourrait être facultative si la méthode est réalisée dans sa globalité (atelier 4 principalement), mais obligatoire dans le cas contraire.

#### [PBA] CALCUL DE LA GRAVITE DES RISQUES LORS DE LA DEFINITION DES SCENARIOS STRATEGIQUES (SS)

Contexte

Étude en phase amont d'un système dual.

Difficulté(s) / intérêt(s)

Le fait que la méthode mette la gravité des risques associés à des événements redoutés (ER) au maximum de la gravité des ER est réellement contre-intuitif.

Solution(s)

Calculer la gravité d'un risque associé à un ER indépendamment de celle du SS qui doit rester au maximum des gravités.

#### SCENARIOS STRATEGIQUES & GRAVITE

Difficulté(s) / intérêt(s)

La méthode définit que la gravité d'un scénario stratégique est celle de l'événement redouté le plus grave présent sur ce scénario stratégique. Cette même gravité sera ensuite partagée pour l'ensemble des risques (un par chemin d'attaque) liés à ce scénario stratégique. Cette approche a pour effet de décorréler le niveau de gravité du risque de celui de son événement redouté. Ce phénomène est renforcé par le choix réalisé dans l'exemple sur lequel s'appuie la méthode (BIOTECH) : au sein de chaque scénario stratégique, tous les ER ont un niveau de gravité équivalent (et donc identique à celui du scénario stratégique).

Solution(s)

Proposition : Faire disparaître la notion de gravité de scénario stratégique (pour lequel nous n'avons pas trouvé d'usage concret), ou dissocier la gravité d'un chemin d'attaque (réutilisée dans l'atelier 4 pour le scénario de risque), et la gravité d'un scénario stratégique.

## 2.4 Atelier 4

### 2.4.1 Analyse des scénarios opérationnels (8)

#### DIFFICULTE DE CONSTRUIRE LES SCENARIOS OPERATIONNELS

Contexte

Lors d'une analyse de risque projet.

Difficulté(s) / intérêt(s)

Les utilisateurs ont du mal à construire les scénarios opérationnels. Ils sont souvent trop génériques et n'apportent pas suffisamment d'éléments pour faire les choix de mesures de traitement des risques optimums et adaptés.

Certains utilisateurs font intervenir des auditeurs techniques dans une logique de *Red Team* pour aider à la construction des scénarios. Cette pratique fonctionne bien à condition que le niveau de granularité de l'étude le permette.

D'autres utilisent la matrice ATT@CK du MITRE, mais les actions élémentaires sont rarement retravaillées et le scénario présenté devient difficile à lire pour des non-initiés.

Enfin, beaucoup se trouvent bloqués par le choix des 4 tactiques proposées par la *kill chain* ou se retrouvent obligés d'écrire des techniques d'attaque sans réelle pertinence et avec de nombreuses répétitions dans les scénarios opérationnels.

Solution(s)

Notre vision est de ne pas systématiser toutes les étapes de la *kill chain*. Ainsi, on construit des chemins d'attaque, avec la réflexion de la *kill chain* en toile de fond, mais sans forcément l'afficher afin de ne pas alourdir le visuel et d'éviter des redites systématiques.

#### DIFFICULTE(S) / INTERET(S) ET SOLUTION(S) - COMPLEMENTS

Nous partageons pleinement ce constat donné en exemple, sans apport de réelle solution. Est-ce parce que le socle de sécurité est rarement respecté et par conséquent il ne nous est pas nécessaire de « creuser » davantage ? Est-ce que cette étape ne peut être réalisée sur du déclaratif et nécessiterait systématiquement un audit technique pour trouver les « vrais » problèmes et éviter cet aspect générique (alourdissant considérablement le budget lié à une analyse) ?

Nous regrettons également qu'il est trop complexe dans les temps (et budget) impartis pour descendre finement au niveau de tous les biens supports. Nous nous arrêtons généralement à la catégorie de bien (matériel, logiciel, …) et déclinons l'action élémentaire si les mesures sont très différentes pour différents biens supports appartenant à la même catégorie. Cette approche renforce le côté « générique ».

Dernière difficulté rencontrée sur les scénarios opérationnels, c'est la difficulté à mieux représenter les parties prenantes critiques et leurs rôles. Ils interviennent souvent soit au début de la *kill chain* sur de l'usurpation, soit à la fin sur de l'abus de droit, mais cela ne ressort pas clairement. Faudrait-il lier les biens supports aux parties prenantes pour connaître leur vrai pouvoir de nuisance ?

## VULNERABILITES DANS LES SCENARII OPERATIONNELS

Contexte

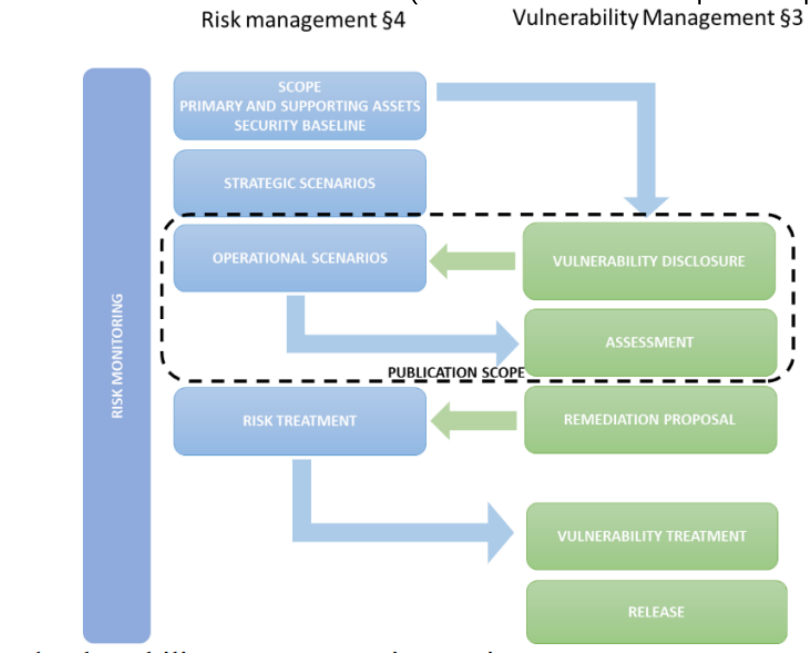
Les appréciations de risques sont souvent vues comme étant d'un point de vue au niveau sans lien avec la réalité technique.
Il est nécessaire que les vulnérabilités apportent une réalité technique aux appréciations des risques et qu'à l'inverse la vision risques apporte du contexte a la gestion des vulnérabilités pour permettre la priorisation de la remédiation.

Difficulté(s) / intérêt(s)

Avoir un niveau de granularité suffisant dans la description des biens supports pour pouvoir y rattacher une vulnérabilité.
Faire un lien entre les paramètres CVSS et les paramètres de scénarii opérationnels.

Solution(s)

Avoir un mapping vulnérabilité et tactique/technique pour pouvoir rattacher la vulnérabilité a un support métier et ses mesures de sécurité (utilisation de la CMDB quand disponible).




## CONCEPT DE VULNERABILITE MANQUANT

Contexte

Atelier 4.

Difficulté(s) / intérêt(s)

La notion de vulnérabilité n'appartient pas à EBIOS *Risk Manager* alors que c'était un élément majeur d'EBIOS-2010. Le suivi et le contrôle des vulnérabilités est une partie importante du management des risques. Sans notion de vulnérabilité, les scénarios opérationnels restent assez abstraits. Actuellement il est aussi difficile d'établir des liens entre l'analyse de risque EBIOS *Risk Manager* et les CVE, CVSS, *etc*.
Je connais plusieurs personnes qui ont refusé d'adopter EBIOS *Risk Manager* à cause de la « zone blanche » côté vulnérabilités.

Solution(s)

Réintroduire la notion de vulnérabilité dans le vocabulaire d'EBIOS *Risk Manager*, et *a minima* au niveau de l'atelier 4, mais potentiellement aussi ailleurs, e.g., lors de l'étude de conformité de l'atelier 1.

## INTEGRATION DE ATT&CK DANS L'ATELIER 4

Contexte

Avec l'arrivée du MITRE *engenuity*, ATTA7CK du MITRE est de plus en plus utilisé. Intégré à MISP, projet de maj du CVSS pour intégrer les techniques/tactiques, *Threat landscape* 2021 Annex A de l'ENISA.

Solution(s)

Faire vivre une version anglaise de la production du collège du Club EBIOS sur le lien entre la *kill chain* simplifiée et ATT&CK.

Utilisation de *ATT&CK workbench* pour proposer des techniques personnalisées. Annex 6.3.

## REGISTRE DE SCENARII OPERATIONNELS GENERIQUES

Contexte

La description des scénarii opérationnels est très souvent haut niveau, car la description des systèmes analysés l'est également.
On a rarement un niveau de détails suffisant pour faire une définition suffisamment détaillée des scénarii opérationnels (retour d'expérience au cercle des formateurs- seulement 30% des analyses dont un A4).

Difficulté(s) / intérêt(s)

Avoir un référentiel de menaces élémentaires génériques suffisamment détaillé.
Prendre en compte les attaques récentes.

Solution(s)

Utilisation de l'annexe A du *Threat Lanscape report* 2021 ENISA pour définir des catalogues de scénarii opérationnels génériques en fonction des types d'attaques actuelles (e.g. *Ransomware, etc*.).
Voir https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

## DIFFICULTE A CONSTRUIRE DES SCENARIOS OPERATIONNELS

Contexte

Lors d'une analyse de risque d'un processus métier.

Difficulté(s) / intérêt(s)

La difficulté est de construire des scénarios opérationnels avec différents modes opératoires sans que cela ne devienne un véritable spaghetti de chemins, d'autant plus s'il y a deux, voire trois, applications derrière le même scénario stratégique.

Solution(s)

Nous avons délibérément choisi l'approche suivante :
Pour les applications simples ou celles pour lesquelles il y a peu de chemins, nous les conservons dans le même scénario opérationnel et nous identifions facilement 5 voire 6 ou 7 chemins d'attaques.
Pour les applications plus complexes (SAP, SAP BO, *etc*.), nous construisons (derrière un scénario stratégique) un scénario opérationnel par application. Chaque scénario montrant facilement 8 ou 9 chemins différents
N'ayant aucune donnée concrète en notre possession, nous supposons qu'une attaque débutant par du *phishing* et une attaque débutant par du *spear phishing* n'aurons pas le même niveau de vraisemblance -> cela nous donnera déjà deux chemins différents.
De même, nous n'écartons pas les attaques sur les services internes exposés sur l'internet.
Une fois ces points d'entrée passés, il y a plusieurs possibilités de trouver les données/systèmes avec plus ou moins les mêmes vraisemblances (cela étant dû au faible niveau de maturité du socle). Cela est la raison pour laquelle, nous avons vite 8 à 10 chemins différents dans un scénario opérationnel.

### COMMENT MODELISER UNE ATTAQUE AVEC REBOND SUR L'ECOSYSTEME ?

Contexte

Atelier 4.

Difficulté(s) / intérêt(s)

Certains scénarios stratégiques représentent des attaques avec rebonds sur l'écosystème. L'attaque d'une partie prenante peut être assez complexe. Dans l'atelier 4, il peut être intéressant de la modéliser plus finement que lors de l'atelier 3, pour évaluer la vraisemblance de scénario opérationnel au global, et/ou pour en discuter avec la partie prenante afin de la convaincre d'adopter certaines mesures de sécurité. Une attaque sur l'écosystème n'appartient ni à la phase « connaitre » ni à la phase « rentrer ».

Solution(s)

Expliciter le fait que la modélisation d'une attaque dans le scénario opérationnel ne se limite pas à la seule partie de l'attaque sur l'objet de l'étude, mais peut aussi concerner l'écosystème, et illustrer cela avec un exemple concert.

## 2.4.2 Estimation de la vraisemblance (4)

### COMPLEXITE DU CALCUL DE VRAISEMBLANCE

Contexte

Méthodes d'évaluation des vraisemblances et indicateurs.

Difficulté(s) / intérêt(s)

Les moyens d'évaluer les vraisemblances sont aujourd'hui assez léger notamment s'il s'agit de fiabilité (appréciation individuelle de l'évaluateur) ou de reproduction des résultats (nuance d'évaluation d'un interlocuteur à un autre). Les préconisations du guide sont finalement fondées sur du jugement d'ingénieurs/expert sécurité et donc sur des indicateurs qualitatifs pour l'essentiel.

Des méthodes et listes d'indicateurs types permettant de combiner des éléments quantitatifs afin de consolider les vraisemblances seraient un réel plus pour les évaluations. Typiquement, 2 exemples :

- l'intégration de statistiques provenant des SOC/CERT pour les incidents sécurités déjà rencontrés sur le périmètre de l'étude serait un plus (ex. : sur un contexte donné, on sait que l'on a 1 attaque par an de type ransomware, comment cela se répercute-t-il sur la vraisemblance ?) ;

- l'intégration de statistiques provenant de NVD ou autres sources de CVE montrant les tendances sur les découvertes de vulnérabilités sur les biens supports de l'étude serait un plus.

Solution(s)

Proposer des méthodes d'évaluation supplémentaires, intégrant des formules quand nécessaire ainsi que des indicateurs types.

## ÉVALUATION DE LA VRAISEMBLANCE D'UN SCENARIO OPERATIONNEL SANS PRENDRE EN COMPTE LA PERTINENCE DES COUPLES SR/OV (ET L'ANALYSE DE LA MENACE DES PARTIES PRENANTES)

Contexte

Lors d'une analyse de risque projet.

Difficulté(s) / intérêt(s)

Les utilisateurs évaluent en général la vraisemblance d'un chemin en fonction de la vraisemblance de chaque action élémentaire.

La pertinence de source ou la menace des parties prenantes n'est pas prise en compte, ce qui aboutit parfois à des résultats non pertinents.
Par exemple, si la source de risque est un administrateur technique, les chemins auront en général une vraisemblance maximum. Or si on a considéré l'administrateur comme une source de risque de pertinence faible ou moyenne (car faiblement motivé), il faudrait pouvoir intégrer cette appréciation dans l'appréciation de la vraisemblance finale du risque.

Solution(s)

Notre suggestion est d'ajouter à l'appréciation de la vraisemblance la pertinence des SR/OV, et de tenir compte de l'évaluation du niveau de menace des parties prenantes éventuellement impliquées dans le scénario de risque.

## CALCUL DE LA VRAISEMBLANCE CUMULEE D'UN CHEMIN D'ATTAQUE (MODE OPERATOIRE) OPERATIONNEL

Contexte

Pour toutes les analyses qui descendent au niveau opérationnel (Atelier 4) et quel que soit le mode de calcul. Même si, pour ce retour d'expérience je vais me focaliser sur le mode de calcul standard.

Difficulté(s) / intérêt(s)

Ce mode de calcul nie totalement le principe de défense en profondeur. Il suffit d'une action élémentaire a 1 sur le chemin pour que la vraisemblance cumulée soit à 1.

Au-delà du fait que j'ai des doutes sur la justesse de la vraisemblance considérée, cela engendre par effet de bord, de gros problèmes dans la justification des plan d'action.
Il est assez fréquent qu'il soit impossible de montrer l'effet d'une préconisation dans la réduction des risques résiduels. Un bon exemple vaut mieux qu'un long discours :

Imaginons un chemin simple avec 2 actions élémentaires. La première action est évaluée avec une vraisemblance de 1 (bon niveau de protection), la seconde avec une vraisemblance 4 (grosse vulnérabilité). La vraisemblance cumulée du chemin est donc de 1.
On propose une préconisation pour couvrir la grosse vulnérabilité (action 2), le client demande quel effet cela a sur les niveaux de risque résiduel et cela en a aucun… La vraisemblance du risque étant déjà à 1, corriger la vulnérabilité n'a aucun effet sur le niveau de risque résiduel.

Plus les années passent et plus je suis convaincu que l'analyse de risque est outil de communication/aide à la prise de décision avant d'être un outil de mesure précis et infaillible des niveaux

de risque. C'est la raison pour laquelle ce problème me semble particulièrement gênant, voire même contre-productif.

Solution(s)

Malheureusement je n'ai pas de solution miracle même si nous en avons testé plusieurs :

- la moyenne règle le problème dans certains cas, mais amène d'autres incohérences (par ex : un chemin avec 2 actions 1-4 va être jugé moins vraisemblance qu'un autre chemin avec 4 actions 1-4-4-4…) ;
- évaluer la vraisemblance directement au niveaux du chemin, ça marche, mais cela fait perdre une bonne partie de l'intérêt de le faire au niveau de chaque action, voire même de dessiner un arbre d'attaque…Il me semble que cela va à contre-courant de la philosophie EBIOS *Risk Manager* ;
- Egérie propose un mode de calcul « propriétaire », qui ne semble pas trop mal, mais qui a le défaut d'être obscur… Il me semble extrêmement gênant qu'un analyste ne soit pas en mesure d'expliquer ses évaluations de vraisemblances… ;
- j'ai fait quelques recherches et je n'ai rien trouvé qui m'a convaincu, ni de modèle qui semble naturellement faire consensus… Mais je ne suis pas en veille très active sur le sujet, donc j'espère que ces REX permettront de trouver LA Solution.

Assez naturellement, la longueur d'un chemin semble avoir une importance dans le calcul de sa vraisemblance cumulé. Maintenant la vraie question c'est, quel poids cela doit-il vraiment avoir ?
Sachant que dans un contexte d'analyse de risque :

- la longueur d'un chemin et aussi fortement dépendante du niveau de granularité de l'analyse. Si on utilise le référentiel des techniques MITRE en tant que base d'actions élémentaires, on obtiendra des chemins plus longs que si on s'appuie sur les exemples donnés dans la méthode. Récemment, nous avons fait une EBIOS *Risk Manager* sur un SI de SoC PDIS. SI par définition extrêmement cloisonné, nous pensions avoir des arbres d'attaques simples… Grosse erreur ! le fait de devoir définir des actions « d'initial accès » très précises pour illustrer les façons de contourner l'étanchéité du cloisonnement nous a contraint à conserver ce même niveau de granularité pour la suite de l'arbre d'attaque…. Au final nous avons eu des arbres d'attaque bien plus touffus que ce que l'on peut avoir dans une analyse de type « cartographie des risques sur l'ensemble d'un SI » ;
- la longueur d'un chemin opérationnel est aussi potentiellement dépendante de la façon dont on définit les parties prenantes…. ;
- si 2 actions élémentaires demandent exactement le même type de compétences/outils/ressources, jusqu'à quel point, le fait de faire les 2 est plus difficile pour l'attaquant ?

## CALCUL DE VRAISEMBLANCE AVANCE

Contexte

Analyse de risque de niveau opérationnel avec le mode de calcul de vraisemblance avancé.

Difficulté(s) / intérêt(s)

J'ai constaté qu'avec ce mode de calcul, on obtenait des résultats bien moins homogènes entre différents analystes. J'ai constaté qu'il y avait au moins 2 façons cohérentes d'évaluer ce couple de critères de vraisemblance :

- il y a la façon de l'ANSSI qui manque un peu de précision, mais qui a du sens et qui doit être la bonne… ;
- il y a une autre façon qui me semble avoir beaucoup de sens aussi, mais qui diffère de celle de l'ANSSI, elle consiste à :
    - évaluer en premier la difficulté de l'attaque au regard des mesures de sécurité existantes de tous types (prévention, protection, détection, réaction) ;
    - puis en fonction de la source de risque et de ses ressources, d'évaluer la chance de succès. Ainsi, pour un même niveau de difficulté, on peut juger qui aura plus ou moins de chance d'y arriver.

Bref, quand les analystes me demandent comment faire, je recommande la méthode de l'ANSSI, mais quand ils contre-argumentent avec la seconde approche j'ai du mal à leur dire où ils se trompent. ;)

Solution(s)

Utiliser le calcul de vraisemblance standard, ce qui est regrettable.

## 2.5 Atelier 5

### 2.5.1 Évaluation des risques (2)

L'ETUDE DES RISQUES DU CLUB EBIOS : DES PISTES POUR AMELIORER LA METHODE

Contexte

L'étude des risques du Club EBIOS a été réalisée de façon à tester une application courte, explicite, et ce, en intégrant sécurité de l'information et protection de la vie privée. Cette application a permis de croiser les points de vue et l'expérience de plusieurs membres experts en la méthode.

Solution(s)

Plusieurs techniques et manières de présenter les résultats ont ainsi été tentées, avec succès :

- **le détail de l'étude des risques est renvoyé en annexes** de façon à avoir un corps de texte clair et concis ;
- **les scénarios stratégiques sont déclinés en scénarios opérationnels dans une même section**, de façon à visualiser directement les actions élémentaires à mettre en œuvre par l'attaquant pour exploiter le mode opératoire choisi ;
- **le traitement des risques est spécifié au regard des scénarios stratégiques et opérationnels, tous formulés pour mettre leur spécificité distinctive en évidence**, afin d'une part de pouvoir traiter les scénarios stratégiques et/ou opérationnels (et pas uniquement les scénarios opérationnels), d'autre part d'assurer et vérifier la cohérence de la gravité et de la vraisemblance, et enfin de bien se rendre compte de l'action attendue des mesures :

| Risque | Gravité | Vraisemblance | Mesures |
|---|---|---|---|
| Scénario stratégique n°1. La source de risque abuse des fonctionnalités d'un site web pour atteindre son objectif.<br>Scénario opérationnel n°1 – Risque n°1. La source de risque exploite une vulnérabilité du site web pour atteindre son objectif.<br>Scénario opérationnel n°1 – Risque n°2. La source de risque bloque volontairement les publications sur le site web dans le but d'atteindre son objectif. | | | |

PRISE EN COMPTE DE LA PERTINENCE DANS L'EVALUATION DES RISQUES

Difficulté(s) / intérêt(s)

La pertinence proposée à l'atelier 2 peut être perçue comme une vraisemblance de passage à l'acte. Pour des raisons de représentativité, un couple SR/OV faiblement pertinent peut cependant être conservé, et exploité dans l'identification de risques sur les ateliers suivants. Le problème majeur est que cette pertinence disparaît ensuite complètement de l'évaluation du risque : on se retrouve avec des risques potentiellement très élevé, alors qu'en réalité la probabilité d'occurrence est très faible.

Solution(s)

Proposition : réintégrer le niveau de pertinence à l'évaluation des risques, en impactant directement le calcul de la vraisemblance lors de l'atelier 4, ou de manière autonome (apparition d'une matrice complémentaire).

### 2.5.2 Détermination des mesures (4)

APPLICATION A UN GRAND SYSTEME D'UN MINISTERE : UNE ERREUR A EVITER

Contexte

L'application de la méthode d'EBIOS *Risk Manager* à la création d'un vaste système d'information d'un ministère régalien a perdu en efficacité du fait d'un manque de compréhension de certains acteurs du projet.

Difficulté(s) / intérêt(s)

Une fois le socle de sécurité défini et l'appréciation des risques effectuée, **les mesures de sécurité ont été scolairement reprise de l'ISO/IEC 27002**.

Ainsi, toute l'efficacité d'avoir mené l'évaluation du socle, qui couvre déjà tous les thèmes de la sécurité de l'information, puis apprécié des risques précis, ciblés et sophistiqués, a été complètement perdue ! Les risques n'ont donc pas été réellement traités et des incohérences ont été engendrées.

Solution(s)

Les mesures auraient pu et dû être déterminées de la même manière : de façon précise, ciblée, et non générique, afin de compléter utilement l'étude.

Ce retour d'expérience met en évidence le **besoin de clarifier l'esprit de la méthode et la manière de la mettre en œuvre**.

NE PAS CONFONDRE LISTE DES MESURES ET PLAN D'ACTION

Contexte

Sur un projet, une analyse de risques est demandée et des audits sont prévus.

Difficulté(s) / intérêt(s)

Souvent la distinction entre analyse des risques et audit est difficile à appréhender pour les utilisateurs, surtout quand le guide précise que le socle peut être alimenté par un résultat d'audit.

Solution(s)

Nous avons l'habitude de dire que les mesures issues de l'analyse de risque (et les référentiels du socle) doivent servir de référentiel à l'audit. Les écarts constatés correspondent à la dette sécurité. Ils sont censés être couverts à terme.

À l'inverse, les risques résiduels sortant de l'analyse de risque, eux sont intrinsèques au projet.

Ainsi, lors d'une homologation, par exemple, il est présenté à l'autorité, la liste des risques résiduels issus de l'analyse des risques, mais également la liste des risques issue des écarts de l'audit.
Le problème est qu'il n'existe pas de technique pour apprécier ces écarts provenant des résultats de l'audit par rapport aux risques, surtout quand les écarts proviennent de mesures issues du socle ou de l'atelier 3, et ne sont donc pas liés dans l'étude à des risques.

DIFFICULTE D'UTILISATION DU SOCLE DE SECURITE

Contexte

Analyse de risque dans le cadre de prestations.

Difficulté(s) / intérêt(s)

Faire le bilan de la conformité avant d'analyser les risques est un point fort de la méthode qui permet de concilier le point de vue « conformité » avec le résultat de l'analyse des risques. Toutefois il n'est

pas aisé de faire le lien entre les mesures issues du socle et celles nécessaires pour contrer les risques. Le guide ne propose pas de manière de procéder.

Solution(s)

Structurer les mesures de traitement du risque de manière identique au référentiel du socle de sécurité utilisé.
Par exemple si le référentiel est une PSI modèle ISO 27002 et que la mesure envisagée porte sur du chiffrement elle sera référencée en 10.1 et pourra ainsi compléter les mesures du chapitre 10 « cryptographie » de la politique (dans la mesure où elles ne seraient pas suffisantes).

#### MESURES DE SECURITE SELON L'ATELIER

Contexte

Les mesures de sécurité sont à plusieurs niveaux et elles n'ont pas une influence au même niveau

Difficulté(s) / intérêt(s)

Il n'est pas compréhensible à l'heure actuelle de savoir sur quelle mesure agir en fonction de l'objectif.

Solution(s)

Proposer un chapitre dédie aux mesures de sécurité pour définir leur niveau d'application :

- socle : applicable au système étudié ;
- écosystème / A3 : mesures sur les PP,
    - dans le cas d'une étude de haut niveau (sans A4) la seule façon de proposer des mesures à ce niveau est de préconiser une maj du socle de sécurité ;
- scénarii opérationnels : Mesures sur les biens supports.

### 2.5.3 Autres (3)

#### SCENARIOS DE SURVEILLANCE DANS L'ATELIER 5

Contexte

Assurer le lien entre SIEM et RM.

Difficulté(s) / intérêt(s)

S'assurer qu'une fois un scénario de risque identifié et traite A4 ce dernier soit surveillé

Solution(s)

Utiliser la notion de scénarii de surveillance dans l'atelier 5 pour permettre de traduire un scénario de risque en éléments de détection pour le SIEM.
Comment détecter ce scénario ? Traduction scénario stratégique/ope en indicateur de compromission
Sommes-nous capables de le détecter ? Si non que faut-il mettre en place
*Etc*.

Référence à l'ISO 27005 DIS qui intègre cette notion.

#### DIFFICULTE A EVALUER A CONSTRUIRE LE PLAN DE TRAITEMENT ET EVALUER L'EFFICACITE DES MESURES DE *MITIGATION*

Contexte

Lors d'une analyse de risque d'un processus métier.

Difficulté(s) / intérêt(s)

La méthode n'apporte pas beaucoup d'aide sur la façon d'évaluer l'efficacité des mesures de *mitigation* et d'évaluer les risques résiduels. Plusieurs mesures de *mitigation* peuvent s'appliquer sur un scénario de risque. Dès lors comment calculer le niveau de risque résiduel ?
Appliquer un % d'efficacité par mesure et définir si ce % équivaut à un palier du niveau d'impact/gravité ou vraisemblance ?
Réduire d'un palier le niveau d'impact/de gravité ou de vraisemblance pour chacune des mesures considérées comme très efficace ? Mais quid des mesures moins efficaces ?
Est-ce qu'un audit fournisseur est tout aussi efficace que l'implémentation d'un DLP ?

Exemple : implémentation d'un DLP, implémentation d'un CASB, Conscientisation du personnel.
Est-ce que le cumul de ces 3 mesures permet de passer d'un niveau de vraisemblance de 4/5 à 3/5 voire 2/5 ?
Est-ce que ces mesures prises séparément permettent de réduire d'un niveau le risque (de 4/5 à 3/5 pour le DLP puis de 3/5 à 2/5 pour le CASB puis de 2/5 à 1/5 pour la conscientisation ?)
Est-ce qu'une de ces mesures permet de réduire le niveau de 2 (passer de 4/5 à 2/5)

Solution(s)

Nous sommes partis du principe que les mesures de *mitigation* s'appliquent sur le chemin d'attaque du scénario et non sur une technique d'attaque. Nous sommes également partis du principe et vu le faible niveau de maturité du socle, qu'il fallait identifier plusieurs mesures de *mitigation* afin de parer au fait qu'un chemin secondaire prendrait le dessus dès le moment pour les mesures de mitigation s'appliquant sur le chemin principal sont appliquées.
Dès lors, nous identifions plusieurs mesures de *mitigation* s'appliquant sur un scénario de risque. Parfois 5 ou 6 mesures différentes.
Nous avons estimé un % d'efficacité pour chacun de ces mesures et nous calculons le risque résiduel par un cumul de ces %.

#### MESURES DE SECURITE DEFINIES A L'ATELIER 1 & 3

Difficulté(s) / intérêt(s)

Il est possible en sortie d'atelier 1 d'identifier des mesures de sécurité, ainsi qu'en sortie d'atelier 3. Dans les deux cas ces mesures ne sont pas rattachées explicitement par la méthode à un risque particulier. De plus, la matrice de choix des ateliers donne l'impression que ces activités peuvent être autonomes, rendant de facto les mesures encore plus orphelines.

Solution(s)

Proposition : si des mesures sont identifiées comme étant à mettre en œuvre à ce stade, elles devraient servir à alimenter un PACS, et les ateliers 1 & 3 ne devraient donc pas être autonomes.

## 2.6 Transverse

### 2.6.1 Général (7)

#### AUDITS ET EXAMENS DE CERTIFICATION : UNE INTERPRETATION « A LA LETTRE »

Contexte

Cadre d'audits (ex : renouvellement de certification ISO/IEC 27001), dans le matériel d'évaluation de certificateurs de compétences, voire dans les logiciels permettant de mettre la méthode en œuvre.

Difficulté(s) / intérêt(s)

Ceux qui doivent juger de la « conformité » à la méthode EBIOS *Risk Manager* (auditeurs, évaluateurs, *etc*.) ou figer la manière de la mettre en œuvre ont besoin de référentiels qu'ils vont exploiter « à la lettre » pour assurer que leur évaluation est impartiale et reproductible.

Or, puisque les guides d'EBIOS *Risk Manager* comportent autant des actions précises que des exemples de techniques ou des explications, **tous les éléments du texte peuvent être repris de manière « scolaire », et ce, sans distinction entre ce qui est indispensable et ce qui ne l'est pas**. On peut ainsi constater que des exemples de techniques et de valeurs possibles, des concepts rapidement évoqués, ou des éléments pas toujours utiles (exemples de critères et d'échelles, manière d'analyser et d'estimer les sources de risques, les parties prenantes ou les scénarios opérationnels, distinction entre événement redouté et impact, notion de mode opératoire, etc.), deviennent « obligatoires » ou peuvent être mal interprétés.

Solution(s)

**Une attention particulière devrait donc être portée à la manière de formuler les choses, notamment en distinguant explicitement ce qui est impératif de ce qui est adaptable ou illustratif**.

### DIFFICULTES SUR DES ANALYSES TRES DETAILLEES

Contexte

Analyse pour conception de produit embarqué.

Difficulté(s) / intérêt(s)

Le cas d'usage d'une analyse de risque pour conception de produit complexe (afin d'ajuster les mesures de sécurité pour atteindre un risque acceptable) n'existe pas. Il manquerait une ou des techniques de calcul de vraisemblance plus robuste.

Solution(s)

Intégration des techniques d'analyse de risques validées pour la conformité à l'ED-203A (norme aéronautique). Il s'agit de la méthode RIME.

### ABSENCE DE PRISE EN COMPTE DES MESURES D'UNE ETAPE SUR L'AUTRE

Contexte

Lors de la conduite d'une analyse de risques projet, par exemple en phase de conception.

Difficulté(s) / intérêt(s) et solution(s)

Les utilisateurs produisent des mesures à chaque atelier de la méthode. Certains ne les prennent pas en compte d'un atelier sur l'autre.

Notre suggestion est de rappeler à chaque atelier de la méthode que les mesures évoquées dans l'atelier N-1 doivent être prises en compte dans l'analyse de l'atelier N.

Lorsque les mesures issues de l'atelier 3 sont prises en compte dans l'atelier 4, des chemins peuvent devenir sans intérêt et donc ne justifient pas la création de scénarios opérationnels dans l'atelier 4. Certains s'étonnent qu'il n'existe plus de bijection entre les chemins d'attaque de l'atelier 3 et les scénarios opérationnels de l'atelier 4.

Notre suggestion est de rappeler que les ateliers doivent prendre en compte les mesures issues des ateliers précédents et donc que certaines menaces ou certains risques peuvent disparaître de la suite de l'analyse, car traités par des mesures précédemment imaginées.

### APPROCHE TROP FOCALISEE SUR LA NOTION « D'ATELIER »

Contexte

La majorité des contextes d'analyse de risque.

Difficulté(s) / intérêt(s)

Réaliser le nombre d'ateliers recommandés par l'ANSSI dans la méthode semble inadapté dans la majorité des contextes d'analyse.
La raison principale est que ça mobilise beaucoup trop les ressources du client. Nous n'avons jamais réussi à vendre à nos clients une telle approche alors que le coût global de la prestation était inférieur à une approche avec moins d'ateliers, mais plus de préparation/entretien ciblée en amont.
Par ailleurs les ateliers sont extrêmement complexes à organiser, ils sont longs, et même en si prenant à l'avance c'est compliqué de bloquer un directeur la moitié de son après-midi.

L'autre raison c'est qu'un atelier n'est pas toujours la meilleure façon de récupérer de l'information. Parfois la lecture d'un document peut-être plus efficace, parfois un entretien ciblé sera plus adapté pour faire parler les gens sans qu'ils aient peur d'être jugés.

Enfin, l'animation d'un atelier n'est pas quelque chose de facile… Cela impose quasiment l'implication d'un analyste senior, ce qui n'est pas toujours adapté au contexte des analyses de risque à instruire. Même si, paradoxalement, les juniors ont souvent l'impression qu'une EBIOS *Risk Manager* est « plus facile à faire » qu'une EBIOS 2010.

Solution(s)

Réduire le nombre d'ateliers au strict minimum (4 à 5 pour une AR de niveau opérationnel).

Cela impose de bien plus préparer les ateliers en amont afin de n'utiliser ces moments d'échanges en groupe que pour préciser, valider et sélectionner les résultats de chaque étape.

Les ateliers supprimés sont remplacés par de l'analyse documentaire et des entretiens ciblés de courte durée (45min-1h) Dont on adapte le nombre en fonction de la complexité de l'analyse.

Au-delà du nombre d'ateliers, sur les AR EBIOS *Risk Manager* importante nous privilégions systématiquement un binôme d'analystes.

## SYNTHESE DES RESULTATS D'UNE ANALYSE EBIOS RISK MANAGER ET CONSTRUCTION ET PRIORISATION DES PLANS D'ACTION

Contexte

Toute analyse dans laquelle il faut produire des résultats de synthèses et des plans d'action.

Difficulté(s) / intérêt(s)

Les schémas c'est très bien pour « construire en atelier », mais ça marche mal lorsqu'il faut synthétiser :

- les risques stratégiques par exemple, Il faudrait les avoir sur 1 seul schéma, quand on en a 5 à présenter ça marche moins bien ;
- les arbres d'attaque opérationnelle, on arrive à en montrer 1 seul en général, pour « montrer comme on a bien bossé », mais personne n'a envie d'en voir plus au moment de la restitution des résultats ;
- les schémas des SR/OV sont jolis, mais ils ne disent pas grand-chose.

De plus, ce que EBIOS *Risk Manager* définit en tant « qu'objet risque » n'aide pas même s'il y a 2 niveaux :

- le risque stratégique est trop haut niveau (SR/OV) même pour des dirigeants, il est trop détaché du métier ;
- le risque opérationnel (ou chemin d'un risque stratégique) est au bon niveau pour le métier. Ce n'est ni plus ni moins que des évènements redoutés scindés par source de risque.

Le problème, c'est qu'il n'y a pas « d'objet risque » adapté au niveau des acteurs plus techniques d'une analyse. Le niveau action élémentaire qui pourrait éventuellement convenir n'est jamais un « objet risque » vu qu'on ne sait pas y attacher un impact…

Cela engendre aussi des difficultés pour la définition des plans d'action.

Comme les risques sont à un trop haut niveau d'abstraction, un grand nombre de préconisations est associé à chaque risque. Ça reste juste d'un point de vue théorique, mais :

- ça n'aide pas pour prioriser le plan d'action ;
- l'effet d'une préconisation a du mal engendrer une réduction des risques résiduels ce qui n'aide pas pour la justifier ;
- ça rend plus difficiles les calculs de risques résiduels.

Solution(s)

Nous n'avons pas de solution miracle. En général on fait la synthèse « à la main » en réutilisant très peu des schémas produits par la méthode.

Pour les risques stratégiques, l'idéal semble être de faire 1 seul schéma. Il peut aussi être intéressant d'ajouter les vecteurs d'entrée sur la cible sur ce premier schéma pour lui donner encore plus d'intérêt.

Pour parler aux acteurs techniques, on fait un top10-20 des actions élémentaires à couvrir en priorité (celles qui sont de vraisemblance 4-3 et celle a 2 sur des chemins critiques). On n'a pas de niveau de risque, mais on se sert de la vraisemblance unitaire pour prioriser les plans d'action.

On n'a pas encore trouvé de solution vraiment fonctionnelle pour régler les problèmes liés à l'affichage des effets de réduction et aux calculs des niveaux de risque résiduels… Ça reste un vrai problème, car les effets de réduction des risques résiduels ont toujours été un bon indicateur pour faciliter les prises de décisions.

## UN BEL OUTIL D'ANALYSE DE RISQUE ET DE COMMUNICATION

Contexte

Tout le temps 😊

Difficulté(s) / intérêt(s)

La méthode EBIOS *Risk Manager* est géniale lors des analyses de risques car :

- elle est légitime, soutenue par l'ANSSI ;
- elle met en avant le métier qui dans de trop nombreux cas était gardé à l'écart d'un « exercice d'expert » ;
- elle pose le socle de sécurité qu'il n'est plus nécessaire d'expliquer, de justifier, de négocier. On ne regarde que les écarts ;
- elle propose une démarche adaptable à de petits projets comme à des gros ;
- …

On arrive à des analyses de risques pertinentes qui sont comprises par tous les participants.

Solution(s)

Sans objet.

## [REA] METHODE VUE PAR UN NOMBRE DE PRATICIENS COMME LOURDE ET CONTRAIGNANTE

Contexte

Échanges avec la communauté : collaborateurs, clients, membres du Club EBIOS.

Difficulté(s) / intérêt(s)

Une bonne partie des praticiens qui débute avec la méthode (si ce n'est la majorité) la voit comme lourde et contraignante, alors c'est l'inverse qui est vrai.

Le problème provient, à mon sens, du focus du praticien sur le déroulé de la méthode et de sa volonté de s'y conformer, au point de perdre le recul et le bon sens.

Solution(s)

Pour une pratique saine de la méthode, il est important de :

- connaître l'esprit de la méthode et le "pourquoi" de chacune de ses activités ;
- maintenir le focus sur les attendus de l'étude : Que dois-je protéger ? Pourquoi ? Contre qui ? et Comment ?
- maintenir un recul par rapport à la méthode et faire constamment appel au bon sens.

Concrètement, et avant d'entamer les ateliers de la méthode, j'invite le praticien ou le groupe de travail à réfléchir dans un premier temps, avec du simple bon sens, aux risques qui pèsent sur le système objet de l'étude. Il formalise ces risques sous forme de paragraphe non structuré, avec son propre vocabulaire.

Dans un deuxième temps, ces risques identifiés sont structurés selon les notions de la méthode. Cela permet une meilleure appréhension de ces notions et de leurs utilités et aussi d'acquérir un recul par rapport à la méthode.

### 2.6.2 Interactions avec d'autres processus (2)

UNE ETUDE POUR UN GRAND GROUPE : UNE CENTRALISATION COHERENTE

Contexte et solution(s)

EBIOS *Risk Manager* a été employée pour bâtir l'étude globale d'un grand groupe du secteur de l'assurance, sous la forme **d'une étude unique, centralisée, en lieu et place de multiples études dont la cohérence ne pouvait être assurée**.

En outre, on note que :

- les valeurs métier sont directement issues des processus identifiés par le système qualité ;
- les biens supports sont directement issus d'un inventaire centralisé des biens ;
- **les nouveaux systèmes ne font que développer l'étude globale ;**
- **l'étude vit donc en permanence**.

Ainsi :

- l'étude de nouveaux systèmes repose sur de nombreux éléments communs : politique, socle, mesures, *etc*. ;
- les bases de connaissances étant communes, elles peuvent être mises à jour et directement répercutées pour toutes les micro-études ;
- les interactions entre les équipes métier et celles en charge de la sécurité se multiplient ;
- les risques estimés sont devenus des entrants pour les audits ;
- les résultats des audits alimentent l'étude des risques (socle, scénarios opérationnels, risques, risques résiduels, mesures de sécurité) ;
- le contrôle interne alimente le socle de sécurité et réciproquement.

**En conséquence, non seulement les études produites sont homogènes, mais en plus, les différentes fonctions traitant de sécurité de l'information et les métiers se retrouvent autour d'un même outil, parlent le même langage et interagissent en continu.**

ASSISTANCE A LA PREPARATION DE *PENTESTS*

Contexte

EBIOS *Risk Manager* peut aider à la préparation d'un *pentest* (définition du scope, échelles, scénarii en fonction du type de *pentest* (*white box*, *etc*.).

Difficulté(s) / intérêt(s)

Cadrer un audit/*pentest* en utilisant la connaissance liée à la gestion des risques par EBIOS *Risk Manager*.

Solution(s)

Proposer les scénarios à dérouler pour préparer un *pentest*.

### 2.6.3 Autres (19)

UNE FORMATION DISPENSEE : DES DIFFICULTES RENCONTREES

Contexte

Dans le cadre de formations à la méthode EBIOS *Risk Manager*, en utilisant un kit de formation amendé.

Difficulté(s) / intérêt(s) et solution(s)

Les échanges entre formateurs et apprenants ont permis de mettre plusieurs points en évidence :

- **certains termes ne sont pas naturellement compris** :
  - la notion de « valeurs métier » pose souvent des difficultés, alors que « données » ou « informations » sont immédiatement comprises ;
  - le terme de « menace » apparaît comme ambigu, car utilisé de différentes manières, dans les anciennes versions de la méthode, la version actuelle, dans certaines normes et selon la culture des apprenants ;
- **les apprenants « se noient » systématiquement dans l'estimation de la dangerosité des parties prenantes et leur représentation sous forme de radar**, non seulement car ils ne comprennent pas les critères et valeurs proposées, mais aussi du fait de la complexité de construction des schémas proposés ;
- l'esprit collaboratif et itératif de la méthode est bien compris lorsque des **jeux de rôles** sont mis en place ;
- **le suivi des risques (atelier 5) apparaît comme insuffisamment expliqué** ;
- l'identification des scénarios opérationnels (atelier 4) à l'aide de **la séquence d'attaque type (connaître, trouver, rentrer, exploiter) oriente tant les réflexions qu'elle peut brider ou bloquer les participants**. À l'inverse, lancer les réflexions à partir des chemins d'attaques des scénarios stratégiques, en montrant éventuellement des exemples de *kill chains*, laisse un plus libre recours à l'imagination ;
- il est souvent demandé si EBIOS *Risk Manager* sera **toujours compatible avec la future version d'ISO/IEC 27005**.

USAGE DANS LE CADRE D'UN SMSI : DES TECHNIQUES UTILES

Contexte

Pour mener l'étude globale du SMSI d'une PME, intégrant sécurité de l'information et protection de la vie privée :

- un document interne a été créé pour expliquer comment utiliser EBIOS *Risk Manager* dans le cadre du SMSI, conformément aux exigences de l'ISO/IEC 27001 et de manière compatible avec la méthode (procédure « Gérer les risques ») ;
- dans ce cadre, le socle était constitué de la PSSI, qui fait l'objet de contrôles internes et externes, le parti pris pour réaliser la suite de l'étude étant qu'elle est donc bien appliquée ;
- les valeurs métier considérées étaient les traitements issus du registre des traitements dont l'organisme est responsable ;
- les impacts considérés étaient non seulement ceux qui portent sur l'organisme, mais aussi ceux sur les personnes concernées.

Solution(s)

L'étude, qui n'a pas été menée « de façon scolaire », a pu faire émerger plusieurs améliorations potentielles et points à souligner :

- **la démarche mise en œuvre a consisté à réaliser des filtres successifs**, ce qui a permis d'avancer rapidement et de se focaliser sur l'essentiel : on part de 3 événements redoutés par valeur métier (atteinte en disponibilité, intégrité et confidentialité), mais on ne garde que ceux dont la gravité est la plus importante, et ainsi de suite tout au long de l'étude (sources de risques,

scénarios stratégiques, scénarios opérationnels), afin de pouvoir disposer d'une étude qui peut tenir en un onglet de tableur lisible !

- **la démarche mise en œuvre n'a pas séparé le point de l'attaquant et le point de vue du défenseur** (les sources de risques n'étaient identifiées que pour les événements redoutés retenus), ce qui a permis d'éviter une rupture en cours d'étude, et d'assurer la continuité entre les événements redoutés, les couples SR/OV et les scénarios ;
- **des scénarios opérationnels très simples (sous forme de liste d'actions numérotées, sans imposer de décrire des actions pour connaître/rentrer/trouver/exploiter), mais très parlants** pour les parties prenantes ont permis d'envisager rapidement des cas bien différents sans perdre les participants dans des scénarios trop compliqués ou trop détaillés pour en percevoir les différences ;
- **les bases de connaissances existantes ont été jugées trop génériques**, car elles ne permettaient pas d'impliquer facilement les parties prenantes et de les faire adhérer aux scénarios : elles ont donc été systématiquement affinées ou illustrées de manière très appliquée au contexte étudié, sans chercher l'exhaustivité, mais plutôt des exemples les plus variés possibles afin de couvrir le plus de cas possibles.

## SUPPORT DES ORGANISMES DE SECURITE

Contexte

Analyse de risques grands systèmes.

Difficulté(s) / intérêt(s)

Afin de légitimer l'évaluation il serait peut-être intéressant pour les grands systèmes qui le peuvent de faire valider l'évaluation de cet atelier par des équipes de *Cyber Threat Intelligence*, CERT ou SOC. Cela éviterait notamment la remise en cause de la légitimité de certains scénarios à différents moments de l'analyse (lors de restitutions par exemple) et permettrait de consolider cet atelier à des échelles plus larges pour la gestion de risques d'entreprise.

Solution(s)

Ajouter une recommandation à l'attention de personnes en charge de la sécurité de grands systèmes ayant des départements dédiés à la gestion d'incident.

## ORGANISATION DES REUNIONS DANS UNE ETUDE D'INTEGRATION DE LA SECURITE DANS UN PROJET

Contexte

Cadre d'une analyse de risques dans un projet.

Difficulté(s) / intérêt(s) et solution(s)

Il est recommandé d'organiser dès le début les réunions à planifier et les acteurs à mobiliser.

- dans l'atelier 1, il faut à la fois 1/ traiter des valeurs métiers et de leur analyse et également 2/ traiter des socles applicables, des biens supports et des écarts. Nous avons l'habitude de dissocier ces 2 sujets avec les acteurs adaptés ;
- dans l'atelier 1, pour l'analyse du socle, il y a 2 activités différentes qui font appel souvent à des acteurs différents :
    - activités de conformité législative et réglementaire ;
    - activités de conformité aux règles d'hygiène ou une politique ou aux mesures répondant aux évènements redoutés issus d'actions non malveillantes ou non ciblées (par exemple, mesures liées au PCI) ;
- il manque dans l'organisation de l'étude, la désignation du chef de projet qui doit assister à toutes les réunions ;
- la réflexion sur les sources de risques, prise de manière autonome dans une réunion est parfois peu productive. Nous avons plus l'habitude de traiter le sujet des sources de risques au travers des ateliers 1 et 3 de manière à illustrer de manière plus évidente les SR/OV.

## APPLICATION DE LA METHODE DANS DES CONTEXTES D'ANALYSE PROJET AU NIVEAU OPERATIONNEL

Contexte

Analyse de risque projet classique dans le cadre d'accompagnement sécurité sur les projets d'évolution du SI. Et en particulier pour les clients qui réalisent de nombreuses AR sur leur SI.

Difficulté(s) / intérêt(s)

La représentation d'un arbre d'attaque opérationnel avec EBIOS *Risk Manager* impose de partir de la source de risque jusqu'à l'atteinte de la valeur métier. Dans un contexte où on fait de nombreuses AR sur une petite partie d'un même SI, cela a tendance à engendrer énormément de redondance au niveau des arbres d'attaque opérationnelle et la mise en avant de vulnérabilité en dehors du périmètre de responsabilité du projet.

L'exemple classique : Quelle que soit l'application analysée, à partir du moment où j'ai une source de risque externe il y a de fortes chances que je retrouve dans mes arbres d'attaque l'action élémentaire « infection *malware via phishing mail* » ….

De façon plus générale, toutes les actions élémentaires de type « *discovery, initial compromission* » (voir de « latéralisation » jusqu'à un certain point) vont se retrouver dans de très nombreux arbres d'attaques, et dans toutes les analyses…

Cela pose plusieurs problèmes :

- perte de temps et maintien de cohérence sur l'ensemble des analyses (répétitions inutiles, complexification des arbres d'attaques) ;
- remonte des problèmes de sécurité qui sont totalement hors de périmètre de responsabilité du projet ;
- rends plus difficile le fait de détailler l'arbre d'attaque sur le cœur de cible :
    - si la base de l'arbre est déjà compliquée, le fait de détailler les branches fait exploser le nombre de chemins ;
    - certains outils (ex : EGERIE) considèrent dans leur calcul de vraisemblance la longueur du chemin. Donc, même problème, si on part d'un arbre déjà compliqué et qu'on détaille plus les fins de branches on obtient des niveaux de vraisemblance qui n'ont plus de sens…

Solution(s)

Nous avons envisagé et testé plusieurs solutions :

- définir une base de connaissances d'actions élémentaires pré-évaluées qui peuvent être reprises dans les différentes Analyses. Cela permet de gérer une partie du premier problème (la cohérence entre différentes Analyses), mais ne gère pas du tout le reste des problèmes ;
- faire une première phase d'analyse de type « initial compromission » sur l'ensemble du SI dont les résultats pourront être directement repris dans les analyses projets. Par exemple, dans ce type d'analyse : on définit des évènements redoutés d'ordre plus technique comme « compromission et prise en main d'un poste de travail », « compromission et prise en main d'un serveur en zone Front Web » « intrusion via les accès VPN », etc… et les arbres d'attaques détaillés associés. Puis, on considère ces « évènements redoutés » comme des « actions élémentaires » dans les AR projets de plus bas niveau (en reprenant leur niveau de vraisemblance global). Cette solution permet de gérer l'ensemble des problèmes, mais elle n'est pas simple à mettre en œuvre les premières fois ;
- s'appuyer sur le concept de partie prenante pour écarter du niveau opérationnel des analyses projet tous les débuts de chemin d'attaque redondants. Par exemple on peut considérer « la sécurité d'un poste de travail » comme une PP interne. On fait une analyse sur la « compromission des postes de » travail dont les résultats pourront être directement repris dans les analyses projets. De la même façon que dans la solution précédente, mais avec :

- un découpage d'analyse différent qui est plus adapté dans le cas où le client gère son SI en mode « catalogue de service ». Chaque brique de service peut être vu comme une PP ;
- une réutilisation un peu détournée du concept EBIOS *Risk Manager* de base qu'est celui des parties prenantes. Ça reste cohérent en termes de « périmètre de responsabilité différent », mais la formule de calcul du niveau de menace des PP ne colle plus trop…

### ABSENCE D'EXHAUSTIVITE POUR LES ANALYSES DANS DES CONTEXTES D'HOMOLOGATION/CERTIFICATION.

Contexte

L'agilité a été prise en compte « *by design* » dans la méthode EBIOS *Risk Manager*. C'est génial dans la plupart des cas (DEVOPS par ex.), mais, dans un contexte d'AR d'homologation ça pose problème. En effet, il est difficile d'expliquer au client que son analyse ne sera pas « exhaustive ».

Difficulté(s) / intérêt(s)

Nous sommes bien conscients qu'aucune méthode ne garantit l'exhaustivité d'une démarche d'analyse… Mais, EBIOS *Risk Manager* le fait bien ressentir au client : à chaque étape de l'approche il faut sélectionner et écarter des éléments de l'analyse. À l'inverse de EBIOS 2010 qui, au contraire, pouvait donner au client un faux sentiment d'exhaustivité : *« Si cette analyse comporte 250 scénarii, c'est forcément qu'ils ont tout vu ! »*

Dans un contexte d'homologation, il est très difficile pour le client de vraiment écarter un élément. Le plus souvent, il préfère le garder et que l'analyse affiche un risque « vert » pour bien tracer que le cas a été pris en compte et qu'il ne présente pas de risque…

EBIOS *Risk Manager* permet de n'écarter aucun élément si on le souhaite, mais, le problème c'est qu'elle n'est pas pensée pour ça ! Si on garde tout, le nombre de risques stratégiques et opérationnels explose avec beaucoup de redondance.
Comme dans EBIOS 2010, mais à la différence que, cette fois, un scénario supplémentaire n'est pas une ligne de plus dans un tableau Excel, mais un arbre d'attaque à dessiner… Ce qui rend a priori ce type d'approche « opérationnellement impossible ».

Solution(s)

Il me semble que, comme dans EBIOS 2010, une partie de la solution doit se trouver dans le fait de « regrouper les éléments » (Actifs, ER, Source de risque).
D'un point de vue de la perception client, il est plus facile d'accepter le fait de regrouper 2 éléments plutôt que d'avoir à faire le choix d'en écarter 1.

La difficulté dans le cas d'une EBIOS *Risk Manager* c'est que tout n'est pas forcément pertinent à regrouper, par ex :

- regrouper des objectifs visés (ex : vol de donnée dans un but lucratif et paralysie du système dans un but lucratif/rançon)) va réduire le nombre de risques stratégiques, mais n'aura aucun impact au niveau des scénarii opérationnels ;
- regrouper les parties prenantes n'est pas forcément évident/pertinent ;
- regrouper les sources de risque a le plus souvent du sens même si ça peut engendrer des incompréhensions dans les couples SR/OV.

Ce qui pourrait aider, c'est que la méthode donne des guides pour adapter les niveaux de sélection en fonction du contexte de l'AR et des besoins d'exhaustivité (pour la première itération).

### VALORISER L'AGILITE DE LA METHODE

Contexte

Lors de mission longue intégrée aux équipes client.

Difficulté(s) / intérêt(s)

La présentation d'EBIOS *Risk Manager* est principalement séquentielle. Il est aussi possible de l'utiliser de façon dynamique et agile.
On se permet alors de revenir dans les différents ateliers lorsque c'est nécessaire pour compléter et ajuster. Voici quelques principes :

- la validation d'une homologation se fait sur une version validée de l'étude ;
- EBIOS *Risk Manager* doit être utilisé lors des phases projet pour :
    - les « sources de risque et scénarios stratégiques » lors de l'« initialisation du projet » (intrusion via ce nouveau partenaire, ouverture sur internet du SI X, dépendance à la technologie Y) ;
    - le « cadrage et socle de sécurité » lors du « cadrage du projet » (ex : niveau SI Industriel sensible, niveau bureautique, Accès interne avec authentification forte uniquement, signature numérique des documents) ;
    - la prise en compte du RGPD et des mesures de sécurités demandées par le DPO ;
    - les scénarios opérationnels lors de conception et de choix technologique (ex : intrusion sur le wifi, vulnérabilité sur l'hyperviseur, collaborateur sous contrainte) ;
    - le traitement du risque avec la définition et mise en place de mesures de sécurité (ex : séparation des fronts intranet et internet, chiffrement en BDD, sous-traitance à un prestataire de paiement) ;
- lors d'une modification d'un atelier, il faut vérifier les impacts sur les autres ateliers ;
- la nécessité d'une bonne communication entre les acteurs.

La méthode est déroulée en entier rapidement dès le lancement du projet. Elle est ensuite complétée et mise à jour. Elle est utilisée aussi pour :

- arbitrer des choix coût / sécurité (écart socle de sécurité, mutualisation ou non d'équipement, secours à chaud, *etc*.) ;
- justifier des choix d'architecture (non-chiffrement des flux en zone back, positionnement d'un IPS, *etc*.) ;
- expliquer des impossibilités fonctionnelles avec les besoins de sécurité (impossible de permettre un accès à un tiers depuis un matériel non maîtrisé depuis internet et limiter les fuites d'informations).

Tout ceci dépend beaucoup du projet et de l'environnement.

Solution(s)

Ajouter une fiche méthode sur l'utilisation de la méthode en mode agile/dynamique/itératif.
Présenter les ateliers comme des lieux avec des outils pour travailler sur des problématiques plutôt que comme des étapes méthodologies séquentielles.

### INCOMPREHENSION SUR LA REPRESENTATION DES RISQUES

Contexte

Lors d'analyse de risque projet/homologation ou sur une organisation (type SMSI).

Difficulté(s) / intérêt(s)

Le schéma page 10 laisse penser qu'il y a autant de risque que de scénarios opérationnels - sachant que si on ne factorise pas au niveau des scénarios stratégiques (point ci-dessus), on démultiplie les risques, qui à la lecture sont pour beaucoup très semblable (seule la source change). C'est notamment l'approche prise par les solutions labélisées.

De plus, la représentation des risques page 76 du guide ne fait apparaître que les événements redoutés liés aux risques, sans mention des scénarios stratégiques ou opérationnels.

Solution(s)

Il est pourtant bien indiqué page 71 du guide qu'il faut affiner les risques, approche que nous préconisons également, mais cela n'est pas toujours réalisé. Une fiche méthode pourrait éventuellement aider sur ce point.

Quant au rattachement des scénarios, afin de trouver une utilité aux scénarios stratégiques, qui portent la gravité, nous les rattachons aux risques ainsi que les scénarios opérationnels pour la vraisemblance. Les liens pourraient être davantage explicites dans le guide ou dans une fiche.

### [PBA] DIFFICULTE A JUSTIFIER DES MESURES DE SECURITE DIFFERENCIEES DU FAIT DE LA METHODE DE CALCUL DE LA GRAVITE D'UN RISQUE

Contexte

Nous avons un système dual, d'un côté grand public et gouvernemental de l'autre. Le client nous a demandé de monter une panoplie de mesures de sécurité qu'il espère moins fortes côté grand public que côté gouvernemental qui sera soumis à une homologation de sécurité.

Difficulté(s) / intérêt(s)

Pour cela, nous pensions faire plusieurs SS avec des impacts sur des services grand public d'une part et des services gouvernementaux d'autre part (le même type de scénario pouvant aboutir aux mêmes attaques, mais sur des services différents, mais //) et nous nous attendions à des gravités différentes pour les risques afférents, car les gravités des ER étaient différentes (évidemment, impacts plus forts sur les services gouvernementaux). Patatras :

| | | | | | | |
|---|---|---|---|---|---|---|
| RO4 - Crime | TO9 - Hijacking resources for personal use | ☑ | R22 | Hijack Mobile user data communications telecom services | 3. Serious | 3. Serious |
| | | ☑ | R23 | Hijack Business communications telecom services | | |
| | | ☑ | R24 | Hijack [redacted] service | | |
| | | ☑ | R37 | Hijack [redacted] telecom services | | |

Ici, les gravités des 2 premières lignes (R22 et R23) seraient plutôt 2 (impact sur des services grand public) et celles de R24 et R37 sont bien 3 (impact sur des services gouvernementaux).

Le fait que l'outil utilisé prenne le max est d'ailleurs ce qui est prévu par la méthode EBIOS est indiqué dans les supports de cours EBIOS (en début d'atelier 4 « Ce que nous avons vu précédemment » : gravité des impacts identiques pour le SS et tous ses chemins d'attaque).

Avec l'outil, pour calculer la matrice d'aversion au risque, nous faisons un mini-atelier 4, juste pour pouvoir mettre une vraisemblance (avant mesures de sécurité) un peu au doigt mouillé (un scénario opérationnel où nous mettons juste la dernière étape et en forçant une vraisemblance retenue). Ce à quoi nous nous attendions, c'est de voir R22 et R23 sur la ligne d'en-dessous de R24 et R37 vu que leur gravité n'est pas la même ; or, R22, R23, R24 et R37 se trouvent dans la même case.


Le résultat est contre-intuitif. En effet, que le SS retienne le maximum des gravités est tout à fait entendable ; par contre, que les risques prennent tous la gravité du SS qui les contient n'est pas très intuitif et n'aide pas à justifier des mesures plus légères pour contrer des risques moindres sur les services ayant un besoin de sécurité plus faible.

Nous nous en sommes tirés en créant deux SS similaires, chacun portant sur des ER de niveau homogène :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| RO4 - Crime | TO9a - Hijacking MassMarket resources for personal use | ☑ | R22a | Hijack Mobile user data communications telecom services | | 2. Significant | 2. Significant |
| | | ☑ | R23a | Hijack Business communications telecom services | | | |
| RO4 - Crime | TO9b - Hijacking GovSatCom resources for personal use | ☑ | R22b | Hijack [redacted] telecom services | | 3. Serious | 3. Serious |
| | | ☑ | R23b | Hijack [redacted] telecom services | | | |

Mais cela implique de faire deux fois le même travail.

Solution(s)

Il serait appréciable que les risques gardent leur niveau de gravité et ne prennent pas le maximum des risques du SS qui les contient.

## REPRESENTATION DES RISQUES D'UN SYSTEME COMPLEXE

Contexte

Dans le cas d'une analyse sur un système global il est nécessaire d'avoir une analyse globale haut niveau (analyse système) et des analyses spécifiques bas niveaux (systèmes de systèmes).
Il est nécessaire d'avoir des liens entre ces analyses afin d'apporter une cohérence globale.

Difficulté(s) / intérêt(s)

**Type d'analyse :**
Comment lier ces analyses systèmes de systèmes à l'analyse globale et comment la modéliser, notamment dans les outils ?

- faut-il traiter chaque sous analyse comment une nouvelle analyse en soi avec l'ensemble des ateliers à dérouler ?
- avoir une seule et même grosse analyse à laquelle on vient tout rattacher et mettre à jour régulièrement ?

**Lien :** Pour assurer le lien entre les analyses cela se fait-il avec :

- des déclinaisons de valeurs métiers en sous valeurs métiers et sous évènement redoutés associés ?
- échelle absolue ou relative ou les calculs (un risque très grave sur une plateforme de développement une fois rapporté a l'importance de cette plateforme dans le système dans sa globalité peut-être très faible. Comment assurer cette pondération ?

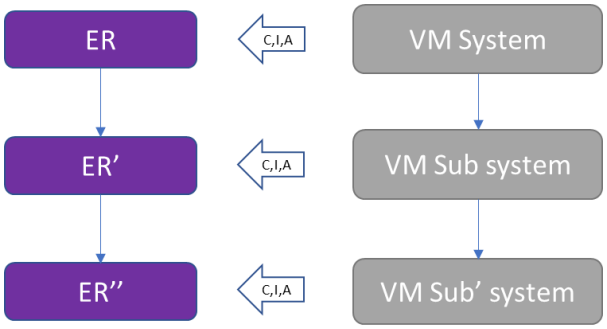
**Visualisation :** Comment visualiser la vue globale du système et de ses risques vs la vue spécifique sous-systèmes.

**Sous-traitance :** Comment un maître d'œuvre peut-il sous-traiter une partie de son analyse sans dévoiler à son sous-traitant la vision sur ses risques ?

Solution(s)

Les solutions proposées sont une proposition de choix qui a été effectué sur des projets :
**Type d'analyse et lien :**

- pour chaque analyse dériver les Valeurs métiers de plus haut niveau et en déduire des ER dérivés également :




**Visualisation :**

- utiliser l'écosystème comme un outil de visualisation pour modéliser son système, les interactions entre ses différents sous-systèmes et leur état de menaces basé sur :
  - exposition : dépendance/pénétration *business* ;
  - cyber :
    - niveau de *compliance* au socle de sécurité système ;
    - confiance : composante de 1er niveau, 2ème niveau, *etc*. (interne/externe à mon périmètre).

**Sous-traitance :**

Seule la définition des scénarii opérationnels est confiée au sous-traitant en fonction d'un scénario stratégique spécifique fourni en donnée d'entrée. Le fournisseur va ainsi définir le scénario en fonction de son architecture.

## LEXIQUE ISO

Contexte

L'ISO 27005 est en cours de révision (DIS). De nombreuses notions sont compatibles entre EBIOS et ISO.

Difficulté(s) / intérêt(s)

Beaucoup de projets EU/internationaux font références à l'ISO seulement. Pour percer, EBIOS doit mettre en avant cette comptabilité.

Solution(s)

Proposer une matrice de comptabilité ISO/EBIOS en FR/EN (DIS 27005 en cours de traduction), ex :

| EBIOS Risk Manager | ISO 27005 (CD3) |
|---|---|
| Source de risque/Objectifs visés (SR/OV) | *Risk source and desired end state/Target objectives* |
| Ecosystème | *Ecosystem* |
| Parties Prenantes | *Interested parties* |
| Scénarios stratégiques | *event based approach / strategic scenarios* |
| Scénarios opérationnels | *asset based approach / operational scenarios* |
| Cycles stratégiques/opérationnels | *Risk management cycles (operational/strategic)* |
| Impacts | *Consequences* |
| Valeur métier / Bien support | *Primary asset (info/process) / Supporting asset* |
| Scenarios de surveillance (college des practiciens) | *Monitoring risk related events* |

## PROBABILITE D'OCCURRENCE DANS LES SCENARII STRATEGIQUES

Contexte

Dans le cas d'une analyse de haut niveau (A1/A2/A3/A5) les scénarii opérationnels ne sont pas définis. Par définition un risque = probabilité d'occurrence * conséquence/Impact (selon le référentiel).

Difficulté(s) / intérêt(s)

En l'absence de scénarii opérationnels il manque la composante probabilité d'occurrence.
On a donc en théorie *risk level* = gravité de l'ER.

Solution(s)

Intégrer la notion de vraisemblance au niveau de l'atelier 3 si jamais on ne fait pas l'atelier 4.

### DIFFICULTE A LIER UN SCENARIO STRATEGIQUE ET UN NIVEAU DE GRAVITE DANS CERTAINS CAS

Contexte

Lors d'une analyse de risque d'un processus métier.

Difficulté(s) / intérêt(s)

La réalité d'un système d'information au sein d'une organisation nous montre qu'il peut s'avérer très complexe simplement par la multitude d'applications (biens supports) exploitée au sein d'un même processus.
Lorsque nous déroulons une analyse de risques sur un processus métier, nous avons pris pour habitude, dans les cas complexes (et à cause des scénarios opérationnels), de définir un scénario stratégique lié à un évènement redouté et d'y définir un scénario opérationnel (R1, R2, R3, *etc*.) par application (bien support).
De ce fait, s'il y a au moins deux applications, elles seront liées au même évènement redouté et donc au même impact.
Ce qui peut dans certains cas d'avérer incorrect (l'impact de l'évènement redouté sur le second bien support n'est peut-être pas aussi élevé par rapport au premier bien support, ce qui oblige à affiner les évènements redoutés).

Ex : Crime Organisé / Divulgation massive et publique des données Finance dans le but de nuire à la réputation d'ORES, avec un impact de niveau 4/5. Les données Finance se trouvent dans 2 applications différentes (App1 et App2).
Nous aurons donc un scénario stratégique et deux scénarios de risques (R1 ciblant App1 et R2 ciblant App2).
Selon la méthode, ce scénario stratégique est lié à une valeur métier et donc à un niveau d'impact/de gravité.
Nous devrions donc avoir un niveau d'impact identique (4/5) pour une divulgation que ce soit de l'App1 ou l'App2).
Les discussions en atelier et hors atelier (établissement du socle) nous montrent que le volume de données dans l'App1 est important, mais il l'est moins dans l'App2.
Ces discussions nous montre également qu'il y a dès lors un impact d'une divulgation des données Finance issues de l'App2, mais moindre que si la cible est l'App1.

Solution(s)

Nous avons pris pour habitude de revenir sur l'atelier 1, d'y définir un nouvel évènement redouté (ex : divulgation publique et isolée) avec un autre niveau d'impact/de gravité (3/5). Nous repassons lors de l'atelier 2 pour y définir un nouveau couple SR/OV.
Dès lors nous pouvons définir un nouveau scénario stratégique qui générera un scénario opérationnel (R2), ciblant App2.
Le premier scénario stratégique, lui, générant un scénario opérationnel R1 ciblant App1, mais avec l'impact de l'évènement redouté initial 4/5.
Les deux systèmes étant différents, il est aussi possible que les niveaux de vraisemblance des modes opératoires ne soient pas identiques.

### DIFFICULTE A CONDUIRE UNE ANALYSE LORSQU'IL S'AGIT DU PREMIER CYCLE

Contexte

Lors d'une analyse de risque d'un processus métier.

Difficulté(s) / intérêt(s)

La méthode mentionne de se concentrer sur ce qui est le plus évident, le plus critiques (parties prenantes, biens supports), le plus pertinent (couple SR/OV, chemin d'attaque), de faire une évaluation du socle à la louche. Cependant, nous voulons être certains qu'il n'y a pas d'angle mort (ce que la méthode mentionne également à l'atelier 2).
De ce fait, lorsque l'on utilise la méthode pour la première fois et qu'aucune analyse de risque n'a jamais été effectuée par l'organisation, il est difficile de trouver une bonne balance entre le plus évident/critique et retenir suffisant d'éléments à étudier afin de ne pas avoir d'angle mort.

Solution(s)

Nous cherchons à ne pas avoir d'angle mort, quitte à sortir un peu plus d'évènements redoutés ou de couples SR/OV que ce qui est conseillé par la méthode.

Nous compensons cette charge de travail par le fait que :

- nous laissons tomber les évènements redoutés ayant un impact de niveau 1 (le plus faible sur notre échelle) sauf si nous pensons que le niveau de vraisemblance pourrait être plus élevé que supposé (à l'évaluation du socle) ;
- beaucoup de scénarios opérationnels se répètent que ce soit d'une valeur métier à l'autre ou d'un processus à l'autre parce qu'il s'agit du même bien support et donc des mêmes vulnérabilités et donc de la même vraisemblance. Nous avons donc construit un *template* de ces scénarios opérationnels que nous récupérons lorsque nécessaire et nous adaptons le contexte.

### DUREE TROP LONGUE & CHAMP D'APPLICATION TROP LARGE DE L'ATELIER 1

Contexte

Analyse de risque sur projet, notamment en phase BID

Difficulté(s) / intérêt(s)

L'étendue, au sens du nombre de concepts couverts, de l'atelier 1 est très importante, notamment au regard des ateliers 2, 3 et 5. Cet atelier étant le premier, il peut conduire à donner une image d'ateliers compliqués et longs pour la méthode.

Solution(s)

La partie architecture (i.e. biens supports) est traitée dans l'atelier 1, mais cette architecture ne va pas vraiment servir avant l'atelier 4. Serait-il possible de déplacer cette activité dans l'atelier 4 ? Je sais que l'atelier 4 est déjà long, mais il y a une vraie cohérence d'ensemble entre architecture et scénarios opérationnels.
De plus, cela inverse l'ordre dans lequel on définit les biens supports et les parties prenantes, à savoir qu'on commencera par les parties prenantes (atelier 3) avant d'identifier les biens supports (atelier 4). Il y a une certaine logique à faire cela, car les parties prenantes peuvent s'identifier alors que le système est en boîte noire, alors que les biens supports exigent un système en boîte blanche. Je suis persuadé que cela aide à lever la confusion entre biens supports et parties prenantes (cf. RETEX ci-dessous sur l'écosystème en §4.7). En gros, ce qui a été correctement identifié et caractérisé comme partie prenante ne peut pas (plus) être un bien support. Je pratique déjà cette inversion dans les formations que je donne en école d'ingénieurs, avec un certain succès.

### VRAISEMBLANCES (AU PLURIEL) : EXPLICITATION NECESSAIRE

Contexte

Analyse de risque sur projet.

Difficulté(s) / intérêt(s)

La méthode fait intervenir plusieurs types de vraisemblance, sans jamais être très claire sur le sujet. Il y a notamment :

- la pertinence des couples SR/OV, qui s'assimile à une vraisemblance de passage à l'acte de la source de risques pour un objectif spécifique ;
- la criticité des parties prenantes, qui s'assimile à une vraisemblance de la partie prenante à servir de vecteur d'attaque, et qui est double, à savoir qu'elle peut être calculée avant et après la définition du socle de mesures sur l'écosystème ;
- la vraisemblance des scénarios opérationnels, qui traduit surtout une vraisemblance de réussite de l'attaque, et qui est double, à savoir qu'elle peut être calculée avant traitement et après traitement du risque ;
- la vraisemblance du risque, qui doit plus ou moins rendre compte des toutes les vraisemblances ci-dessus, et qui est aussi double, à savoir qu'elle peut être calculée avant traitement et après traitement du risque.

Solution(s)

Être plus explicite dans le guide sur la façon de calculer la vraisemblance du risque, en tenant compte de la pertinence des couples SR/OV, de la criticité des parties prenantes, de la vraisemblance des scénarios opérationnels, et de l'effet des mesures de sécurité des socles (ateliers 1 et 3).

### CONVAINCRE UNE AUTORITE DE CERTIFICATION OU D'HOMOLOGATION NON-FRANÇAISE

Contexte

Certification ou homologation d'un système.

Difficulté(s) / intérêt(s)

La plupart des autorités de certification ou d'homologation s'attendent à trouver une analyse de risque exhaustive en support à la certification ou l'homologation. Comment les convaincre que l'approche d'EBIOS *Risk Manager* fait l'affaire, et que l'analyse exhaustive n'est pas nécessaire ? La question m'a notamment été remontée par des Néerlandais.

Solution(s)

Construire et proposer un argumentaire solide dans la méthode démontrant qu'EBIOS *Risk Manager* est apte à supporter un processus d'homologation / certification. Faire valider cet argumentaire par plusieurs autorités de certification ou d'homologation européenne, dont évidemment l'ANSSI.

### DEFINITION TROP FLOUE DE L'ECOSYSTEME

Contexte

Cadrage du système (atelier 1) et définition de l'écosystème (atelier 3).

Difficulté(s) / intérêt(s)

Il est difficile de faire la part des choses entre :

- sources de risques et parties prenantes de l'écosystème : l'atelier 3 se situe juste après l'atelier 2, où l'on a étudié les sources de risques. Les gens ont vite fait de placer des sources de risques comme parties prenantes dans l'écosystème ;
- biens supports et parties prenantes de l'écosystème. Un flou certain règne. Par exemple, dans le cas d'étude du kit de formation, le coursier est défini dans les biens supports organisationnels, tandis que la Société d'Acheminement figure parmi les parties prenantes !

Solution(s)

Lors de l'atelier 3, éviter de parler de « menace » au sujet des parties prenantes, car c'est source de confusion avec les sources de risques. Je propose de parler de criticité des parties prenantes à la place. Ceci serait un vocabulaire identique aux biens supports critiques, d'où une certaine cohérence d'ensemble.
Par ailleurs, dans l'atelier 1, mieux définir les biens supports pour éviter de décrire des parties prenantes à ce stade.

Voir aussi mon RETEX n°1 ci-dessous, où il est proposé de basculer l'identification des biens supports de l'atelier n°1 vers l'atelier n°4. Identifier les parties prenantes avant les biens supports est une façon très pratique (et éprouvée) d'éviter la confusion entre les 2 concepts.

SOURCE DE RISQUE VERSUS ACTEUR DE RISQUE

Contexte

Atelier 4.

Difficulté(s) / intérêt(s)

Les actions élémentaires d'un scénario opérationnel ne sont pas toutes réalisées par la source de risque à l'origine de l'attaque (et qui profitera à terme de l'attaque). Il peut y avoir d'autres acteurs, e.g. personne corrompue par la source de risques, qui réalisent des actions. La connaissance et la modélisation de ces acteurs sont importantes pour évaluer la vraisemblance d'un scénario opérationnel.

Solution(s)

Introduire la notion d'acteur de risque en sus de la source de risques. La méthode anglaise IS1&2 le fait déjà avec les notions de *Risk Source* et *Risk Actor*.

# 3 Annexes aux propositions d'amélioration

## 3.1 Principales forces, faiblesses, opportunités et menaces (SWOT)

De manière synthétique, le SWOT spécifique à la méthode EBIOS *Risk Manager* est le suivant :

Principales forces (S)

1. La notion de socle de sécurité
2. Une méthode participative
3. L'estimation de la gravité par les impacts et non les besoins
4. La capacité d'adaptation à différents objectifs
5. La capacité d'intégration cohérente : sécurité de l'information et protection de la vie privée, plusieurs études en une, *etc*.

Principales faiblesses (W)

1. Des termes ou concepts mal compris
2. Un manque de distinction entre ce qui est important et ce qui l'est moins ou illustratif
3. Une discontinuité dans les ateliers
4. Un atelier 4 peu outillé
5. Un atelier 5 peu décrit, notamment en termes de suivi des risques

Principales opportunités (O)

1. De nombreuses contributions (ex : Collège des praticiens) qui pourraient être intégrées, ou permettre d'améliorer l'existant, ou pointées depuis la méthode
2. La révision d'ISO/IEC 27005 en cours
3. La possibilité de développer la position de la gestion des risques au cœur des tâches de sécurité de l'information (conception, conformité et audits, gestion des incidents, *etc*.)
4. Un besoin de bases de connaissances plus riches et d'exemples de livrables qui peuvent être simples
5. Des explications quant à l'intégration dans un système de management

**Principales menaces (T)**

1. Une volonté de certains d'absolument étudier l'accidentel sous forme de scénarios
2. La compréhension insuffisante ou erronée de l'esprit de la méthode (« elle ne traite pas d'accidentel », présentation de résultats génériques/non personnalisés ou de tableaux de chiffres, *etc*.)
3. Une application parfois trop scolaire menant à des résultats non pertinents et/ou « lourds »
4. Des critiques qui persistent (lourdeur, complexité, *etc*.), fondées sur un mauvais usage ou une mauvaise lecture

permettraient de renforcer le lien avec les normes internationales

5. L'application par des personnes seules, sans interaction

## 3.2 Évaluation des travaux et référentiels

Les tableaux suivants présentent une évaluation de l'apport potentiel de productions externes et internes au Club EBIOS à l'amélioration d'EBIOS *Risk Manager* (seules les références utiles y figurent).

### 3.2.1 Évaluation d'éléments produits par le Club EBIOS

| Élément évalué | Évaluation de l'utilité | Principaux éléments utiles |
|---|---|---|
| Productions du Club EBIOS | Les productions du Club EBIOS, qui s'enrichissent et se mettent régulièrement à jour, peuvent être utiles, sans pour autant devoir être intégrées à la révision de la méthode | - FAQ<br>- Études de cas<br>- Techniques spécifiques |
| Club EBIOS, EBIOS, l'approche générique | Ce guide peut utilement servir d'inspiration, notamment sur la forme, dans sa manière de présenter les modules, et sur le fond, dans ses explications sur la méthode et son lien avec certains référentiels | - Grands principes<br>- Présentation du contenu des modules sous la forme d' « outils » (composant la boîte à outils)<br>- Présentation du contenu des modules sous la forme de questions<br>- Idée de montrer la correspondance avec les normes (ex : ISO 31000, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27701, ISO/IEC 29134…), voire avec des réglementations ou autres<br>- Description des composants d'un risque et de son appréciation par raffinements successifs<br>- Termes et définitions |
| Déclinaison de la matrice ATT&CK du MITRE | La déclinaison de la matrice ATT&CK du MITRE à la méthode EBIOS *Risk Manager* peut constituer un outil/une aide pour d'élaborer les scénarios opérationnels | - Sélecteur de technique basé sur le référentiel ATT&CK du MITRE<br>- Excel en libre accès |
| Présentation sur les opérations d'influence (CAIRE, CONCHON) | La typologie des « stratégies d'influence » peut être utile pour créer une base de connaissances d'actions sur des biens supports humains dans le cadre de l'analyse des scénarios opérationnels | - Diapositive 11 : typologie de stratégies d'influence |
| Présentation sur le « standard » FAIR (FORET, ROYER) | Les sous-critères d'estimation du niveau de risque pourraient être utiles à développer l'estimation de la gravité et de la vraisemblance | - Quantification des risques en termes financiers (diapositive 7 : variables) |
| Présentation de l'utilisation d'EBIOS pour SAFECARE (TOURRON) | L'intégration de concepts et d'une approche visuelle augmentée de BowTie pourrait venir enrichir les techniques de la méthode | - Corrélation des impacts et des attaques<br>- Améliorations proposées sur le visuel des scénarios opérationnels (diapositive 18)<br>- Idée de définir les biens supports détaillés lors de l'analyse des scénarios opérationnels<br>- Représentation des mesures sur ce sur quoi elles portent |

| Élément évalué | Évaluation de l'utilité | Principaux éléments utiles |
|---|---|---|
| Présentation EBIOS *Risk Manager* (GRISPAN, AUVRAY) | Le retour d'expérience met en évidence plusieurs améliorations testées dans une approche collaborative | pour contrer ou ralentir les attaques (diapositives 19 à 21) / Rattacher les mesures aux composants<br>- Notion de propagation d'incidents (lien entre biens supports ou événements redoutés)<br>- Représentation globale des scénarios, mesures et impacts (diapositive 21)<br>- Accent sur la capacité de détection et son amélioration<br>- Représentation de la préparation et du déroulement des ateliers sous forme synthétique (points d'attention, données en entrée, outillage, séances, durée, participants)<br>- Représentation visuelle globale des scénarios stratégiques<br>- Technique pour analyser les scénarios opérationnels (diapositive 13)<br>- Idée de présenter le vocabulaire utile à chaque atelier<br>- Mise en évidence de la restitution aux participants<br>- Ajout d'une évaluation de l'efficacité de la mise en place des mesures de sécurité<br>- Structuration du socle de sécurité selon les 4 axes de la défense en profondeur |
| Présentation d'un retour d'expérience au sein de THALES (VAN CAUTER) | Cette présentation vient challenger la méthode d'EBIOS *Risk Manager* en utilisant un vocabulaire « plus parlant ». | - Évaluation de la « capacité d'attaque » des sources de risque en approfondissant la notion de « ressources »<br>- Évaluation de la « difficulté » des scénarios opérationnels à partir de la « capacité d'attaque » et « chance de succès »<br>- PACS : pilotage de la performance SSI selon 3 dimensions : « renseignement », « agilité » et « engagement » (diapo 8) |
| Présentation sur l'élaboration de *kill chains* (CONCHON, CAIRE) | Dans cette présentation, trois méthodes sont proposées pour élaborer les scénarios opérationnels. | - Proposition 1 : assumer le caractère systémique de la *kill chain*<br>- Proposition 2 : utiliser la même grammaire pour chaque étape de la *kill chain*<br>- Proposition 3 : considérer la *kill chain* comme un schéma narratif et pour assurer la cohérence globale |
| Q&R Quelles sont les étapes pour déployer une démarche EBIOS *Risk Manager* dans une grande entreprise ? | Donne des éléments de réponses pour les grandes entreprises qui souhaitent effectuer une étude de risques avec EBIOS *Risk Manager* | - Différents éléments de réponse selon la maturité des entreprises |
| Q&R EBIOS *Risk Manager* pour analyser un SI : Comment ne pas s'y perdre ? Comment aborder la démarche ? | Tout est possible quant au champ d'application d'EBIOS *Risk Manager* | - Modélisation du champ d'application en fonction de la cible de l'étude et de l'objectif recherché<br>- Adaptation du niveau de détail de chaque atelier à la taille du périmètre |
| Q&R EBIOS est-il conforme à l'ISO 27005 ? | EBIOS *Risk Manager* répond aux principes de la gestion des risques décrits par la norme ISO/IEC 27005 | - Éléments de langage pour expliquer comment EBIOS *Risk Manager* couvre bien la norme |
| Q&R Les mesures peuvent-elles modifier la gravité ? | Les mesures sont prises en compte dans plusieurs ateliers de la méthode | - Un événement redouté peut avoir une gravité réduite parce que des mesures existantes sont considérées dans le socle de sécurité<br>- La réduction de la gravité des scénarios stratégiques et scénarios opérationnels est évaluée lors de l'atelier 3 par l'application de mesures de sécurité sur l'écosystème |

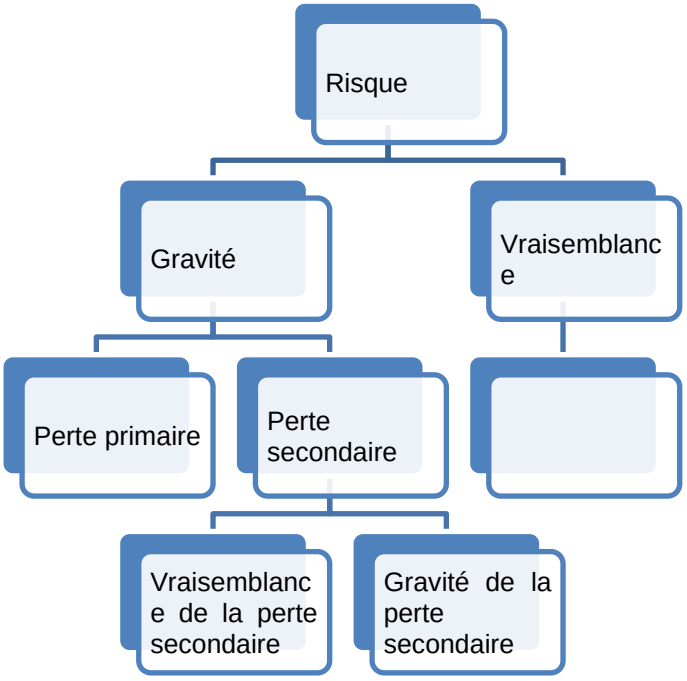
| Élément évalué | Évaluation de l'utilité | Principaux éléments utiles |
|---|---|---|
| Q&R Concrètement, qui déroule la méthode ? RSSI ou *Risk manager* ? | EBIOS *Risk Manager* n'est pas déroulée par un acteur unique | - Au travers des différents ateliers, les points de vue de plusieurs acteurs (directions, métiers, RSSI, DSI, etc.) sont réunis<br>- Le *Risk Manager* peut être l'un de ces acteurs, notamment en fournissant des éléments de décision de traitement des risques |
| Q&R Comment faire une FEROS avec EBIOS *Risk Manager* ? | Adaptation du *template* d'une FEROS proposé par l'ANSSI | - Renommage des parties du template de l'ANSSI de façon à reprendre les grandes séquences d'EBIOS *Risk Manager* |
| Q&R Quelles sont les nouveautés apportées par EBIOS *Risk Manager* par rapport à la version 2010 ? | La nouvelle version EBIOS *Risk Manager* propose une méthode d'analyse plus agile de l'ensemble des systèmes, dans leur environnement global, avec des résultats visibles étape par étape. | - Éléments de langage : procédé d'analyse qui offre un aperçu plus réaliste et qualitatif, analyse plus agile, ciblée et ancrée dans la réalité de la menace cyber, *etc*. |
| Q&R À quoi la "pyramide" du management du risque sert-elle ? | La pyramide explique qu'EBIOS *Risk Manager* vise l'efficacité plutôt que l'exhaustivité | - Éléments de langage : gestion des risques qui peuvent encore survenir après application de la réglementation et des pratiques de base |
| Q&R J'ai déjà réalisé des analyses de risques avec EBIOS dans sa version précédente (2010). Comment réintégrer le travail déjà effectué ? | Les analyses de risques réalisées avec la version précédente sont réutilisables dans EBIOS *Risk Manager* | - Mesures identifiées et mises en place dans la version EBIOS 2010 peuvent être intégrées dans le socle de sécurité (atelier 1) |
| Q&R Comment utiliser des échelles d'impacts hétérogènes ? | Une cohérence transverse de la gradation des impacts dans les échelles est nécessaire. | - Une échelle pour chaque type d'impacts (financiers, sur l'image, juridiques, sur le fonctionnement, sur la vie privée…)<br>- Corrélation des impacts (côte à côte) lors de l'analyse des événements redoutés et de l'estimation de leur gravité<br>- Estimation des impacts auprès des responsables en recherchant un consensus<br>- Certaines échelles peuvent avoir des cases vides (niveau n'ayant pas d'équivalence pour toutes les natures d'impacts considérées).<br>- Rappel des différents impacts et de leur estimation au moment de la présentation de la cartographie |
| Q&R Le critère de traçabilité est-il utile ? | La traçabilité n'est pas un critère de sécurité. C'est une mesure de sécurité. | - Considérer l'information « traces » (ou « preuve », ou « log ») comme une valeur métier, et la traçabilité devient l'intégrité et la disponibilité de cette valeur métier<br>- Se limiter à l'étude des « traces » qui induisent un événement redouté<br>- La traçabilité relève de la bonne mise en œuvre d'une mesure de sécurité, qu'il n'est pas nécessaire de traiter comme un risque |
| Q&R Avez-vous des exemples de niveaux de "motivation", pour décrire les sources de risque à l'atelier 2 ? | Pas d'exemple à proprement parlé. | - Les niveaux de motivation doivent être évalués comme des valeurs relatives<br>- S'appuyer sur l'expérience et la connaissance d'un spécialiste en analyse de la menace numérique pour apprécier le niveau de motivation |
| Q&R Dans l'atelier 2 du guide, comment est évaluée la pertinence des couples « source de | La motivation, les ressources et l'activité de la source de risque permettent | - Cotation à trois niveaux, représentée par des « + »<br>- Pertinence faible si la somme « motivation + ressources + activité » est égale à 3 ou 4<br>- Pertinence moyenne si la somme est égale à 5, 6 ou 7 |

| Élément évalué | Évaluation de l'utilité | Principaux éléments utiles |
|---|---|---|
| risque (SR) / objectif visé (OV) » dans le tableau page 37 ? | d'évaluer la pertinence des couples SR/OV. | - Pertinence élevée si le score est 8 ou 9. |

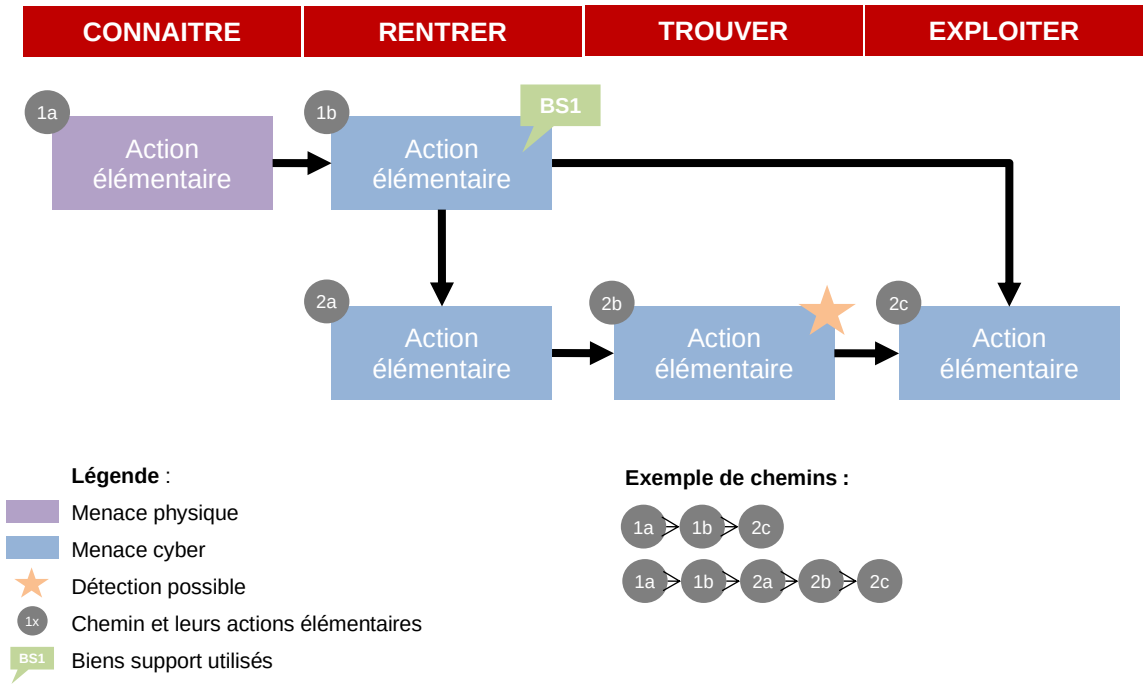
### 3.2.2 Évaluation d'éléments externes

| Élément évalué | Évaluation de l'utilité | Principaux éléments utiles |
|---|---|---|
| ISO/IEC 27005 en cours de révision à l'ISO | Il conviendrait de se rapprocher au maximum de cette norme afin de pouvoir justifier, le plus naturellement possible, qu'EBIOS *Risk Manager* est une/la méthode, pleinement compatible avec ISO/IEC 27005 et permettant de mettre concrètement ce guide de bonnes pratiques en œuvre. | - Termes, définitions, sous-processus et description des composants d'un risque, pour ajustement terminologique et compléments<br>- Description des mesures et du plan de traitement<br>- Facteurs internes et externes à considérer<br>- Actions de communication et consultation<br>- Informations documentées nécessaires<br>- Suivi des risques et du plan de traitement<br>- Critères (échelles, critères d'acceptation, *etc*.)<br>- Typologie de biens supports en strates (disparue de la dernière version), sources de risques, objectifs visés, et parties intéressées, et très éventuellement menaces et vulnérabilités<br>- Présentation des approches par événements et par biens au travers des scénarios stratégiques et opérationnels |
| ISO/IEC 27002 en cours de révision | Autre incontournable de la sécurité de l'information, cette norme s'est complètement restructurée et pourrait donc au moins servir de référence en termes de classement de mesures. | - Structuration des mesures<br>- Liste des mesures<br>- Idée d'utiliser d'attributs (*tags*) pour de multiples classements<br>- Terminologie |
| ANSSI, Guide d'hygiène informatique | Les 42 mesures peuvent servir de référentiel, par exemple pour décrire le socle de règles de ceux qui n'ont pas de politique | - 42 mesures |
| ANSSI, Recommandations pour les systèmes sensibles | Même si ces recommandations sont teintées « systèmes sensibles », elles peuvent servir de référentiel de bonnes pratiques (avec celles de l'II 901), pour le socle de règles et/ou des bases de mesures. | - Tableur Excel des mesures du guide et de l'II 901 |
| Arrêté du 14/09/2018 fixant les règles des OSE et FSN | Bien que destinées aux OSE et FSN, les règles résultant de la transposition de la Directive NIS peuvent être utiles pour le socle de règles et/ou des bases de mesures. | - Structure des règles<br>- Règles |
| CNIL, Guide PIA-3 | Ces bases de connaissances pourraient être utiles pour enrichir celles d'EBIOS *Risk Manager* | - Bases de connaissances : échelles, menaces<br>- Structuration des mesures, mesures |
| AMRAE et ANSSI, Maîtrise du risque numérique | Bien qu'ayant un champ plus large que la seule gestion des risques, il pourrait être utile en termes de vocabulaires et d'exemples | - Terminologie<br>- Exemples synthétiques<br>- Exemples d'indicateurs |

## 3.3 Proposition de quantification de la gravité en termes financiers



## 3.4 Proposition d'un visuel légendé d'un scénario opérationnel



## 3.5 Compléments sur les métriques

| Niveau | Dépendance fonctionnelle<br>Dans quelle mesure peut-on subsister la partie prenante si elle est compromise ? | Dépendance SSI<br>Dans quelle mesure a-t-on besoin de la partie prenante en matière de SSI ? | Pénétration logique<br>Dans quelle mesure la partie prenante a-t-elle un accès logique à l'objet de l'étude ? | Pénétration physique<br>Dans quelle mesure la partie prenante a-t-elle un accès physique à l'objet de l'étude ? |
|---|---|---|---|---|
| 1 | Relation non nécessaire aux fonctions stratégiques.<br>En cas de compromission, il est aisé de se passer de la partie prenante ou de la substituer. | Relation non nécessaire à la SSI de l'objet de l'étude.<br>Aucun besoin de la partie prenante pour nous protéger, réagir, détecter ou restaurer en cas d'attaques. | Pas d'accès logique aux supports de données privées de l'organisme (données personnelles, données financières, données de publications, *etc*.) et valeurs métiers essentielles ou accès sans privilège. | Pas d'accès physique aux supports de données privées de l'organisme et valeurs métiers essentielles ou accès restreint (ex : zone publique). |
| 2 | Relation utile aux fonctions stratégiques.<br>En cas de compromission, il est difficile de se passer de la partie prenante ou de la substituer. | Relation utile à la SSI de l'objet de l'étude.<br>La partie prenante peut contribuer à protéger, réagir, détecter ou restaurer en cas d'attaques. | Accès avec privilèges à des terminaux utilisateurs contenant des données privées de l'organisme (ex : administrateur local).<br>La partie prenante peut provoquer un évènement redouté dont la gravité est significative. | Accès physique à des supports de données privées de l'organisme.<br>La partie prenante peut provoquer un évènement redouté dont la gravité est significative. |
| 3 | Relation indispensable, mais non exclusive.<br>En cas de compromission, il est très difficile de se passer de la partie prenante ou de la substituer. | Relation indispensable à la SSI de l'objet de l'étude.<br>La partie prenante joue un rôle essentiel à protéger, réagir, détecter ou restaurer en cas d'attaques. | Accès avec privilèges de type administrateur aux biens supports sensibles de l'organisme (ex : administrateur métier).<br>La partie prenante peut provoquer un évènement redouté dont la gravité est importante. | Accès physique à des zones restreintes contenant des biens supports sensibles de l'organisme.<br>La partie prenante peut provoquer un évènement redouté dont la gravité est importante. |
| 4 | Relation indispensable et unique (pas de substitution possible à court terme).<br>En cas de compromission, il est impossible de se passer de la partie prenante ou de la substituer. | Relation indispensable et unique à la SSI de l'objet de l'étude.<br>La partie prenante est la seule à pouvoir nous protéger, réagir, détecter ou restaurer en cas d'attaques. | Accès avec privilèges aux biens supports critiques de l'organisme (ex : administrateur infrastructure, fournisseur d'une solution de type IaaS/PaaS/SaaS, qui administre l'application, sa configuration, et l'infrastructure sous-jacente).<br>La partie prenante peut provoquer un évènement redouté dont la gravité est maximale. | Accès physique aux biens supports critiques de l'organisme (salles serveurs).<br>La partie prenante peut provoquer un évènement redouté dont la gravité est maximale. |

**Exposition**
=
Max ([Dépendance fonctionnelle] ; [Dépendance SSI])
X
Max ([Pénétration logique] ; [Pénétration physique])

NB : les parties prenantes non humaines (ex : interface avec un système interconnecté) sont également considérées.

## 3.6 Références

### 3.6.1 Security baseline

Systématisation d'une démarche de sécurisation par conformité ajustée aux besoins et enjeux de sécurité – une revue critique // *A critical review of approaches to securing proportionally to the needs and stakes – with automation considerations*.

https://conf.researchr.org/details/cesar-2021/call-for-papers/1/Syst-matisation-d-une-d-marche-de-s-curisation-par-conformit-ajust-e-aux-besoins-et-

### 3.6.2 Lien entre risk management et vulnerability management

*Automation of risk-based vulnerability management based on a cyber kill chain model*

https://conf.researchr.org/details/cesar-2021/call-for-papers/2/Automation-of-risk-based-vulnerability-management-based-on-a-cyber-kill-chain-model

### 3.6.3 MITRE ATT&CK *Workbench*

voir site du MITRE