RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

COLLECTION **GESTION DES RISQUES CYBER**

GUIDE EBIOS RISK MANAGER
FICHE METHODE 5 – Atelier 3

STRUCTURER LES MESURES DE TRAITEMENT DU RISQUE

Les fiches méthodes permettent aux responsables de la démarche d'analyse de risque d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

QUELLES SONT LES PARTIES PRENANTES (PP) A PRENDRE EN COMPTE ?

Tout ce qui interagit avec l'objet de l'étude est une partie prenante. Ce sont les **éléments dont la sécurité ne dépend pas directement du commanditaire du système étudié**. Généralement le commanditaire ne peut imposer des moyens de sécurité aux parties prenantes à l'inverse des biens supports.
L'écosystème comprend l'ensemble des parties prenantes qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions (partenaires, sous-traitants, filiales, etc.).
Les PP à prendre en considération peuvent être de deux natures:

PP EXTERNES :

- clients ;
- partenaires, cotraitants ;
- prestataires (sous-traitants, fournisseurs).

PP INTERNES :

- services connexes techniques (exemple : services supports proposés par une DSI) ;

- services connexes métier (exemple : entité commerciale utilisatrice des données métiers) ;
- filiales (notamment implantées dans d'autres pays).

Le nombre de PP au sein de l'écosystème peut s'avérer très élevé et donc difficile à gérer. Il revient au responsable projet, avec l'aide du RSSI, de définir **les catégories de PP à évaluer en priorité** et ainsi effectuer une première sélection. Par exemple, le responsable projet peut choisir d'inclure dans le périmètre d'analyse uniquement certaines PP internes à l'organisation. Nous vous recommandons alors d'établir des cartographies distinctes pour les PP internes à votre organisation et celles qui lui sont externes, car les mesures de sécurité seront certainement contractualisées différemment.

EXEMPLE : services support, services métier.

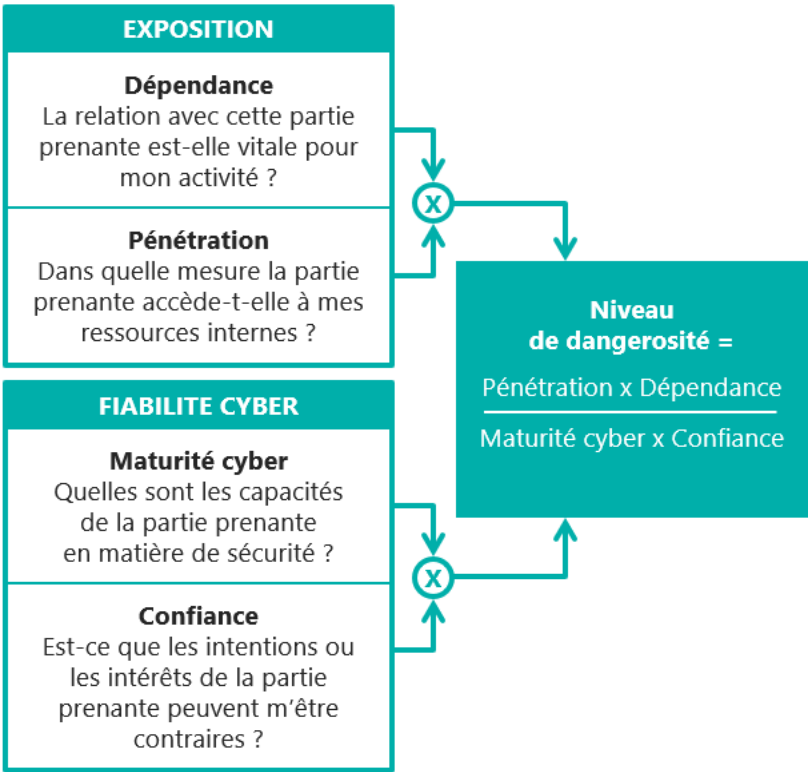
Nous vous recommandons également, si cela se révèle pertinent, d'établir une cartographie des PP **par phase de vie ou de mission**, ce qui permettra d'une part de segmenter l'effort d'évaluation, et d'autre part d'identifier les PP induisant en permanence une menace vis-à-vis de l'objet de l'étude et celles qui ne représentent une menace qu'à certaines étapes. **EX :** exploitation, maintenance.

> **NOTE :** les sources de risque identifiées dans l'atelier 2 ne sont pas à prendre en compte en tant que telles lors de la réalisation de cette étape. Les PP qui pourront également être considérées comme des sources de risque sont ici étudiées uniquement en tant que PP. **EX :** entreprise partenaire dans le contexte étudié mais concurrente par ailleurs.

◆

EVALUER LE NIVEAU DE MENACE QUE REPRESENTENT LES PP VIS-A-VIS DE L'OBJET DE L'ETUDE.

Nous proposons les critères d'évaluation ci-après, qui peuvent être adaptés et différents pour chaque organisation. Les critères d'exposition tendent à accroître la menace alors que ceux relatifs à la fiabilité cyber l'atténuent.



NOTE : la formule de calcul ci-dessus est générique et vous permettra de réaliser une première évaluation. Si vous souhaitez l'affiner en fonction du contexte, vous pouvez la calibrer afin de valoriser certains critères qui vous paraissent prépondérants par rapport aux autres. Par exemple, pour exprimer une plus grande sensibilité au niveau de maturité cyber, vous pouvez pondérer le critère de maturité cyber dans l'expression précédente. Dans le même ordre d'idée, si vous considérez qu'une partie prenante sera utilisée à ses dépens comme simple intermédiaire par un attaquant, alors le critère de confiance ne sera pas prépondérant et pourra être retiré de la formule.

Une métrique de cotation de chaque critère est proposée ci-après. Là encore, n'hésitez pas à l'adapter au contexte de votre activité et à l'objet de l'étude.

	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFIANCE
1	Pas de lien avec le SI de la partie prenante pour réaliser la mission.	Pas d'accès ou accès avec des privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, ordiphone, etc.).	Des règles d'hygiène sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne sont pas connues.
2	Lien avec le SI de la partie prenante utile à la réalisation de la mission.	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux bureaux de l'organisme.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est assurée selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	Lien avec le SI de la partie prenante indispensable mais non exclusif (possible substitution).	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Lien avec le SI de la partie prenante indispensable et unique (pas de substitution possible).	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires d'entreprise, DNS, DHCP, switchs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisme.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

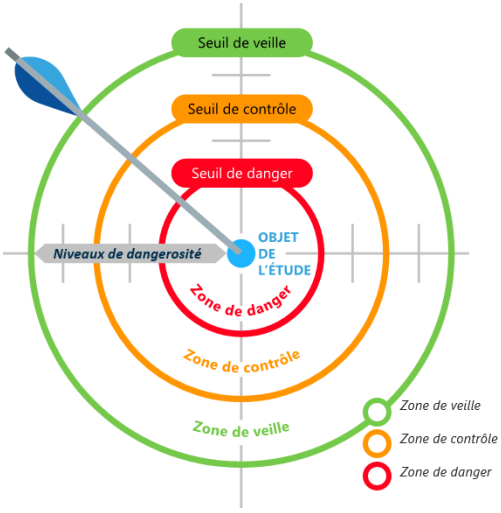
EXEMPLE : société de biotechnologie fabriquant des vaccins.

Les PP de l'écosystème ont été évaluées selon la métrique précitée :

CATÉGORIE	PARTIE PRENANTE	DÉPENDANCE	PÉNÉTRATION	MATURITÉ	CONFIANCE	NIVEAU DE MENACE
CLIENTS	C1 – Établissements de santé	1	1	1	3	0,3
	C2 – Pharmacies	1	1	2	3	0,2
	C3 – Dépositaires / Grossistes répartiteurs	1	2	2	3	0,3
PARTENAIRES	P1 – Universités	2	1	1	2	1
	P2 – Régulateurs	2	1	2	4	0,3
	P3 – Laboratoires	3	3	2	2	2,25
PRESTATAIRES	F1 – Fournisseurs industriels chimistes	4	2	2	3	1,3
	F2 – Fournisseurs de matériel de production	4	3	2	3	2
	F3 – Prestataire informatique	3	4	2	2	3

QUELLE REPRESENTATION ADOPTER ?

La représentation radar ci-contre est proposée. La distance radiale correspond au niveau de menace selon l'échelle d'évaluation utilisée. Plus une partie prenante fait peser une menace numérique importante pour l'objet de l'étude, plus elle se situe près du centre.



Les PP situées dans les zones de danger et de contrôle doivent être incluses dans le périmètre d'appréciation des risques car elles risquent d'être exploitées par un attaquant. Concrètement, ces PP dites critiques doivent être prises en compte dans l'élaboration des scénarios stratégiques.

ZONE DE DANGER : zone pour laquelle le niveau de menace est considéré comme très élevé et difficilement acceptable. Par conséquent, aucune partie prenante ne devrait se situer dans cette zone. Les mesures de sécurité prises par la suite devraient faire sortir de cette zone les PP qui viendraient à s'y trouver.

ZONE DE CONTRÔLE : zone pour laquelle le niveau de menace est considéré comme tolérable sous contrôle. Les PP qui s'y trouvent doivent faire l'objet d'une vigilance particulière et ont vocation, à moyen terme, à rejoindre une position moins menaçante au travers de mesures de réduction du risque.

EXEMPLE : enrôlement dans l'organisation de management du risque.

ZONE DE VEILLE : zone pour laquelle le niveau de menace est considéré comme faible et acceptable en l'état. Les PP qui s'y trouvent peuvent faire l'objet d'une veille sans être prises en compte dans l'élaboration des scénarios stratégiques.

HORS PÉRIMÈTRE : les PP situées à l'extérieur de la zone de veille représentent un niveau de menace jugé négligeable.

COMMENT FIXER LES VALEURS DELIMITANT LES ZONES DE MENACE ?

Le choix des valeurs seuil – veille, contrôle, danger – est de la responsabilité de la gouvernance projet selon le retour d'expérience disponible, la sensibilité au risque et les ambitions visées. Le chef de projet ou le RSSI aura pour rôle d'apporter son expertise pour définir des valeurs pertinentes. Dans la pratique, ces valeurs sont souvent définies après évaluation de l'ensemble des PP, de façon à obtenir un juste équilibre dans l'acceptation du risque lié à l'écosystème. Il est en général plus facile d'ajuster les valeurs par différence au regard des seuils fixés de manière plus ou moins approximative, dans un premier temps. Deux méthodes sont ainsi proposées.

SEUIL DE DANGER : il pourra être fixé en référence à une partie prenante considérée comme à la limite de l'admissibilité, soit pour l'exclure, soit pour l'inclure. La détermination de ce seuil entraînera des conséquences importantes sur la politique de sécurité : celle-ci devra permettre de diminuer en deçà du seuil de danger le risque associé ou de refuser d'établir ou maintenir l'interaction correspondante.

SEUIL DE CONTRÔLE : il pourra être fixé en utilisant comme référence des attaques antérieures, survenues dans un contexte comparable. La valeur de ce seuil est déterminante pour la suite de l'analyse car elle entraîne la prise en compte des PP dans l'élaboration des scénarios stratégiques.

SEUIL DE VEILLE : il est moins déterminant mais définit la sensibilité relative à la prise en compte ou non de PP dans le suivi des risques résiduels.

Si vous considérez manquer de retour d'expérience et en l'absence d'arbitrage de la gouvernance projet, vous pouvez fixer vos valeurs seuil comme suit, une fois l'évaluation de l'ensemble des PP effectuée :

- Périmètre de danger : 10 % des PP de niveaux de menace les plus élevés.
- Périmètre de contrôle : 40 % des PP suivantes.
- Périmètre de veille : 40 % des PP suivantes.
- Hors périmètre : les 10 % restants.

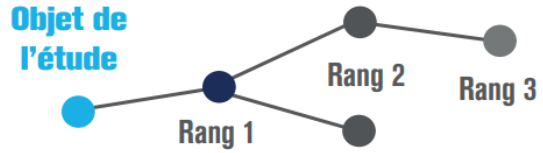
◆

QUEL DEGRE DE PROFONDEUR CHOISIR ?

En première approche et en l'absence de toute autre analyse, vous pouvez commencer par établir votre cartographie de menace en ne considérant que les PP qui interagissent directement avec l'objet étudié (partie prenante de rang 1).

Pour affiner cette analyse, considérez ensuite de façon itérative les PP de rang 2 voire de rang 3, en particulier si elles sont liées à une partie prenante de rang 1 jugée critique. Les règles suivantes peuvent vous aider à ajuster ce degré de profondeur :

- PP située dans le périmètre de danger : évaluation des PP connexes jusqu'au rang 3 ;
- PP située dans le périmètre de contrôle : évaluation des PP connexes de rang 2
- PP non critique (à l'extérieur du périmètre de contrôle) : pas d'analyse plus approfondie des PP connexes.



- Pour garantir une bonne lisibilité, les PP de rang 1 seront représentées en priorité sur la cartographie radar. Les PP de rangs 2 et 3 pourront éventuellement apparaître selon leur niveau de menace.