



Livret stagiaire

Formation CFSSI

EBIOS Risk Manager : les bases

RISQUE

Possibilité qu'un événement redouté survienne et que ses effets perturbent les missions de l'objet de l'étude

Objet de l'étude : la voiture
Mission : arriver à destination



Événement redouté : la voiture percute un arbre

Exercice

Éléments utiles à l'estimation...

... du niveau de risque

Importance de la valeur métier considérée

-

Exposition aux menaces considérées

-

• Gravité

Existence de vulnérabilités

-

Facilité d'exploitation des vulnérabilités

-

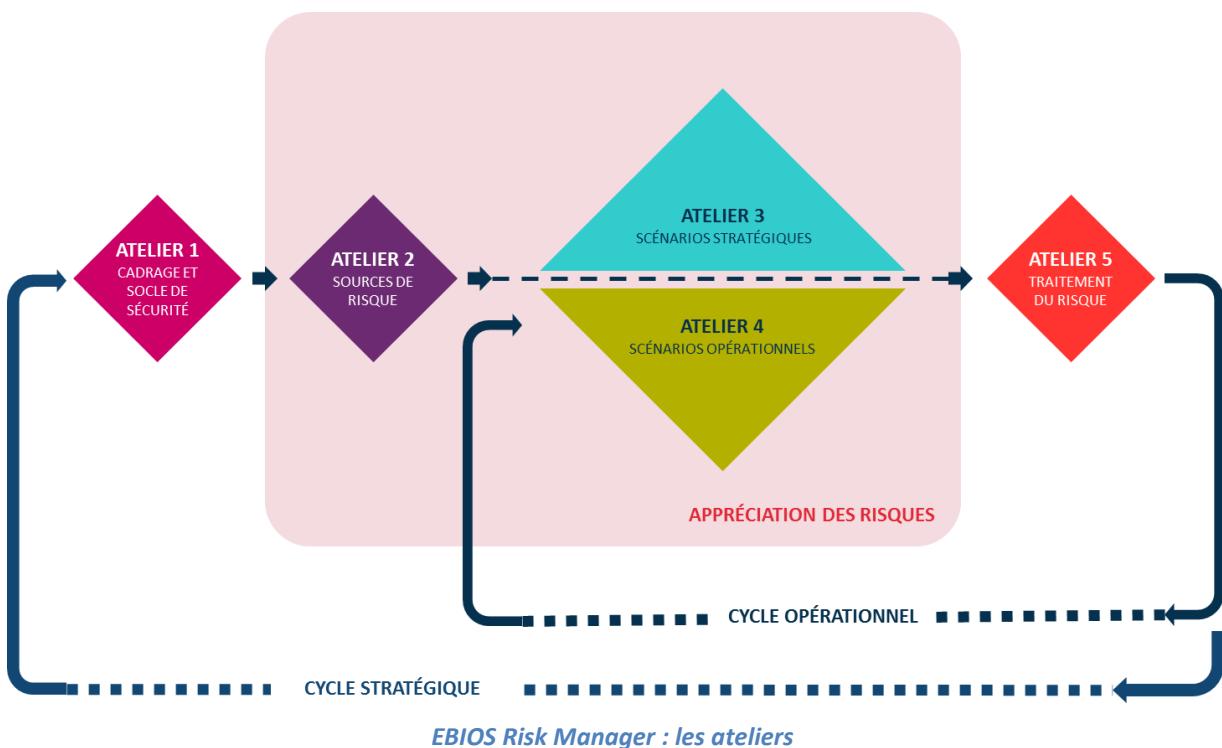
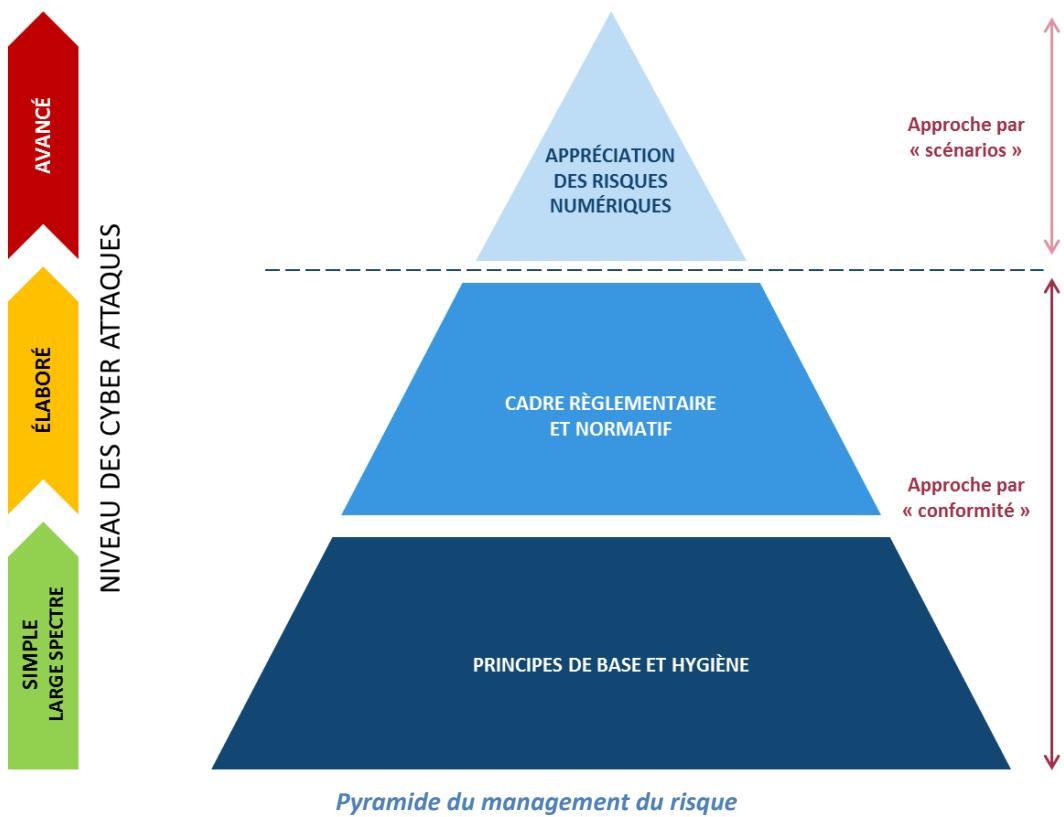
• Vraisemblance

Capacité et motivation des sources de risque

-

Nombre d'impacts identifiés

-



Atelier 1 : cadrage et socle de sécurité

Société de biotechnologies – Identifier le périmètre métier et technique

| MISSION | IDENTIFIER ET FABRIQUER DES VACCINS | | | |
|---|-------------------------------------|--|--|--|
| DÉNOMINATION DE LA VALEUR MÉTIER | | | Fabriquer des vaccins | |
| NATURE DE LA VALEUR MÉTIER (PROCESSUS OU INFORMATION) | | | Processus | |
| DESCRIPTION | | | Activité consistant à réaliser : <ul style="list-style-type: none"> • le remplissage de seringues (stérilisation, remplissage) ; • le conditionnement (étiquetage et emballage). | |
| ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE) | | | Responsable production | |
| DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS | | | | |
| DESCRIPTION | | | | |
| ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE) | | | | |

Exercice

Quelles sont les qualités d'une bonne échelle ?

VRAI

FAUX

Elle n'est pas ambiguë

Elle permet de faire du bricolage

Elle est explicite

Elle est comprise de ceux qui vont l'utiliser

Tous les niveaux sont susceptibles d'être utilisés

Elle privilégie un nombre de niveau pair

Société de biotechnologies – Identifier les événements redoutés

| ÉCHELLE | DÉFINITION |
|--------------------|---|
| G4 – CRITIQUE | Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée) |
| G3 – GRAVE | Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé) |
| G2 – SIGNIFICATIVE | Dégradation des performances de l'activité sans impacts sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé) |
| G1 – MINEURE | Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges) |

Échelle de gravité définie par la société de biotechnologies

| Impact | Exemples (listes non exhaustives) |
|---|--|
| Impacts sur les missions et services de l'organisme | |
| Conséquences directes ou indirectes sur la réalisation des missions et services. | Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé. |
| Impacts sur la gouvernance de l'organisme | |
| <u>Impacts sur la capacité de développement ou de décision</u> Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement. | Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés. |
| <u>Impacts sur le lien social interne</u> Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation. | Perte de confiance des employés dans la pérennité de l'organisme, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, affaiblissement/perte de sens des valeurs communes. |
| <u>Impacts sur le patrimoine intellectuel ou culturel</u> Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes. | Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés. |
| Impacts humains, matériels ou environnementaux | |
| <u>Impacts sur la sécurité ou sur la santé des personnes</u> Conséquences directes ou indirectes sur l'intégrité physique de personnes. | Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire. |
| <u>Impacts matériels</u> Dégâts matériels ou destruction de biens supports. | Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématuée de matériels. |
| <u>Impacts sur l'environnement</u> Conséquences écologiques à court ou long terme, directes ou indirectes. | Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère. |
| Impacts financiers | |
| Conséquences pécuniaires, directes ou indirectes. | Perte de chiffre d'affaire, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées. |
| Impacts juridiques | |
| Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle. | Procès, amende, condamnation d'un dirigeant, amendement de contrat. |
| Impacts sur l'image et la confiance | |
| Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients. | Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété, perte de confiance d'usagers. |

Catégories d'impacts proposées dans EBIOS Risk Manager

Formation EBIOS Risk Manager – Livret stagiaire

| VALEUR MÉTIER | ÉVÉNEMENT REDOUTÉ | IMPACTS | GRAVITÉ |
|---------------|--|---|---------|
| R&D | Perte ou destruction des informations d'études et recherches | <ul style="list-style-type: none"> • Impacts sur les missions et services de l'organisme • Impacts sur les coûts de développement • Impacts sur le patrimoine intellectuel | 2 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Société de biotechnologies – Déterminer le socle de sécurité

Quels sont les référentiels qui s'appliquent à la société de biotechnologies ? OUI NON

Politique de sécurité (PSSI) de l'organisation

Règlement européen de protection des données (RGPD)

Guide d'hygiène informatique

Annexe A de l'ISO 27001

Code de la santé publique

Arrêté sectoriel « produits de santé » (Loi de programmation militaire)

Instruction Générale Interministérielle 1300 (IGI 1300)

Atelier 2 : sources de risque

Société de biotechnologies – Évaluer les couples SR/OV

| | | RESSOURCES | | | |
|------------|--|--|---------------------------|------------------------|-----------------------|
| | | Incluant les ressources financières, le niveau de compétences cyber, l'ouillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc. | | | |
| | | Ressources limitées | Ressources significatives | Ressources importantes | Ressources illimitées |
| MOTIVATION | Intérêts, éléments qui poussent la source de risque à atteindre son objectif | Fortement motivé | Moyennement pertinent | Plutôt pertinent | Très pertinent |
| | | Assez motivé | Moyennement pertinent | Plutôt pertinent | Très pertinent |
| | | Peu motivé | Peu pertinent | Moyennement pertinent | Plutôt pertinent |
| | | Très peu motivé | Peu pertinent | Peu pertinent | Moyennement pertinent |

Échelle de pertinence des couples SR/OV définie par la société de biotechnologies

| SOURCES DE RISQUE | OBJECTIFS VISÉS | MOTIVATION | RESSOURCES | PERTINENCE |
|-------------------|---|------------|---------------------------|-----------------------|
| Hacktiviste | Divulguer des informations sur les tests animaliers | Peu motivé | Ressources significatives | Moyennement pertinent |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Exercice

Un adolescent de 15 ans « pirate » le système de son collège pour améliorer ses notes.

Un adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.

[Sources Internet : Le Point.fr et ZDNet]

| | PREMIÈRE ATTAQUE | SECONDE ATTAQUE |
|--------------------------|---|-----------------|
| Source de risque | Adolescent | |
| Objectif visé | Modifier ses résultats scolaires | |
| Évènement redouté | Les résultats scolaires d'un ou plusieurs collégiens sont erronées | |
| Valeur métier | Résultats scolaires (information) | |
| Bien support | Système informatique de gestion des résultats scolaires | |
| Impacts | <ul style="list-style-type: none"> • Impact sur la poursuite d'études des collégiens • Impact d'image vis-à-vis des autres établissements scolaires | |

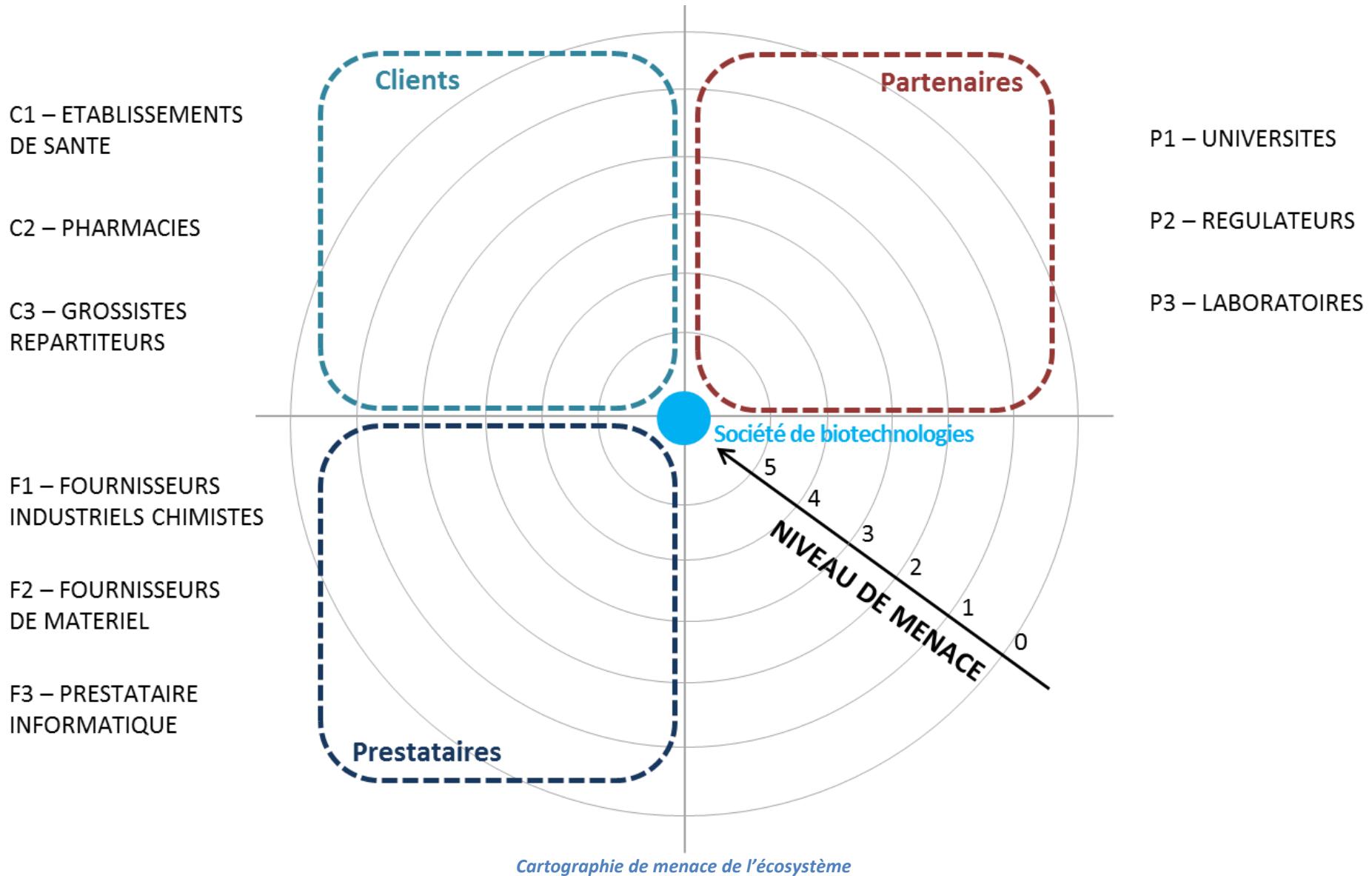
Atelier 3 : scénarios stratégiques

Société de biotechnologies – Évaluer le niveau de menace de chaque partie prenante

| | 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 priviléges 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 priviléges 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 priviléges 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 priviléges 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. |

Échelle d'évaluation du niveau de menace des parties prenantes définie par la société de biotechnologies

| CATÉGORIE | NOM | DÉPENDANCE | PÉNÉTRATION | MATURITÉ CYBER | CONFiance | NIVEAU DE MENACE |
|-------------|--|------------|-------------|----------------|-----------|------------------|
| Client | C1 - Établissements de santé | | | | | |
| Client | C2 - Pharmacies | | | | | |
| Client | C3 - Grossistes répartiteurs | | | | | |
| Partenaire | P1 - Universités | | | | | |
| Partenaire | P2 - Régulateurs (ANSM, EMA...) | | | | | |
| Partenaire | P3 - Laboratoires | | | | | |
| Prestataire | F1 - Fournisseurs industriels chimistes | | | | | |
| Prestataire | F2 - Fournisseurs de matériel (chaine de production) | | | | | |
| Prestataire | F3 - Prestataire informatique | | | | | |



Société de biotechnologies – Élaborer des scénarios stratégiques

A2

Source de risque : Concurrent

Objectif visé : Voler des informations

SOURCE DE
RISQUE



CONCURRENT

ECOSYSTÈME

SOCIÉTÉ DE BIOTECHNOLOGIE

Informations
de R&D



Atelier 4 : scénarios opérationnels

A3

Scénario stratégique : Un concurrent
vole des informations de R&D

Chemin d'attaque : n°1 – attaque directe

Gravité : 3

CONNAITRE

RENTRER

TROUVER

EXPLOITER

Vol et exploitation
de données de
R&D

Exercices

ACCUEIL > HIGH-TECH

Piratage massif du groupe hôtelier Marriott, 500 millions de clients touchés

CYBERSECURITE C'est le second plus gros vol de données après celui dont avait été victime Yahoo en 2013...

Source : 20 minutes – 30/11/2018

« *C'est une méga-fuite de données. Le groupe hôtelier américain Marriott a révélé qu'il avait été victime d'un piratage massif, avec des accès non-autorisés à la base de données de sa filiale Starwood.*

Noms, adresses postale et électronique, dates de réservation, numéros de téléphone et de passeport... Les informations d'environ 500 millions de clients ont été dérobées. [...]

Les accès non autorisés, avec une duplication de la base de données ont commencé en 2014. Marriott assure que les numéros de cartes de crédit étaient chiffrés [...] Mais la chaîne n'exclut pas que les éléments nécessaires au déchiffrement des données aient été compromis. »

| | |
|-------------------|--|
| Source de risque | |
| Objectif visé | |
| Évènement redouté | |
| Valeur métier | |
| Bien support | |
| Impacts | |

Pathé victime d'une arnaque au président à 19 millions d'euros

Des escrocs sont parvenus à convaincre l'ancien directeur financier de Pathé Pays-Bas que la direction de Pathé lui ordonnait de verser d'importantes sommes sur un compte tiers pour financer une acquisition à Dubaï.

Au total, **plus de 19,2 millions d'euros** auraient ainsi été dérobés à l'entreprise en mars 2018. Les faits n'ont été révélés publiquement que lors du procès opposant l'ex-employé incriminé à son entreprise dans le cadre de son licenciement. Selon Pathé, il aurait « *négligé des signaux* » qui auraient dû l'alerter du caractère frauduleux des opérations.

Source : Next impact – 12/11/2018

| | |
|--------------------------|--|
| Source de risque | |
| Objectif visé | |
| Évènement redouté | |
| Valeur métier | |
| Bien support | |
| Impacts | |

Société de biotechnologies – Atelier 1 : corrigé

| MISSION | IDENTIFIER ET FABRIQUER DES VACCINS | | | | |
|---|---|---|--|---|---|
| DÉNOMINATION DE LA VALEUR MÉTIER | Recherche & développement (R&D) | | Fabriquer des vaccins | Traçabilité et contrôle | |
| NATURE DE LA VALEUR MÉTIER (PROCESSUS OU INFORMATION) | Processus | | Processus | Information | |
| DESCRIPTION | Activité de recherche et développement des vaccins nécessitant : <ul style="list-style-type: none"> l'identification des antigènes ; la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage ; l'évaluation préclinique ; le développement clinique. | | Activité consistant à réaliser : <ul style="list-style-type: none"> le remplissage de seringues (stérilisation, remplissage) ; le conditionnement (étiquetage et emballage). | Informations permettant d'assurer le contrôle qualité et la libération de lot (exemples : antigène, répartition aseptique, conditionnement, libération finale...) | |
| ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE) | Pharmacien | | Responsable production | Responsable qualité | |
| DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS | Serveurs bureautiques (internes) | Serveurs bureautiques (externes) | Systèmes de production des antigènes | Systèmes de production | Serveurs bureautiques (internes) |
| DESCRIPTION | Serveurs bureautiques permettant de stocker l'ensemble des données de R&D | Serveurs bureautiques permettant de stocker une partie des données de R&D | Ensemble de machines et équipements informatiques permettant de produire des antigènes | Ensemble de machines et équipements informatiques permettant de fabriquer des vaccins à grande échelle | Serveurs bureautiques permettant de stocker l'ensemble des données relatives à la traçabilité et au contrôle, pour les différents processus |
| ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE) | DSI | Laboratoires | Laboratoires | DSI + Fournisseurs de matériel | DSI |

Société de biotechnologies – Atelier 2 : corrigé

| SOURCES DE RISQUE | OBJECTIFS VISÉS | MOTIVATION | RESSOURCES | PERTINENCE |
|-------------------|--|------------------|---------------------------|-----------------------|
| Concurrent | Voler des informations | Fortement motivé | Ressources importantes | Très pertinent |
| Hacktiviste | Saboter la campagne nationale de vaccination | Assez motivé | Ressources significatives | Plutôt pertinent |
| Hacktiviste | Divulguer des informations sur les tests animaliers | Peu motivé | Ressources significatives | Moyennement pertinent |
| Cyber-terroriste | Altérer la composition des vaccins à des fins de bioterrorisme | Peu motivé | Ressources limitées | Peu pertinent |

Les couples SR/OV très pertinents ou plutôt pertinents seront retenus pour la suite de l'étude

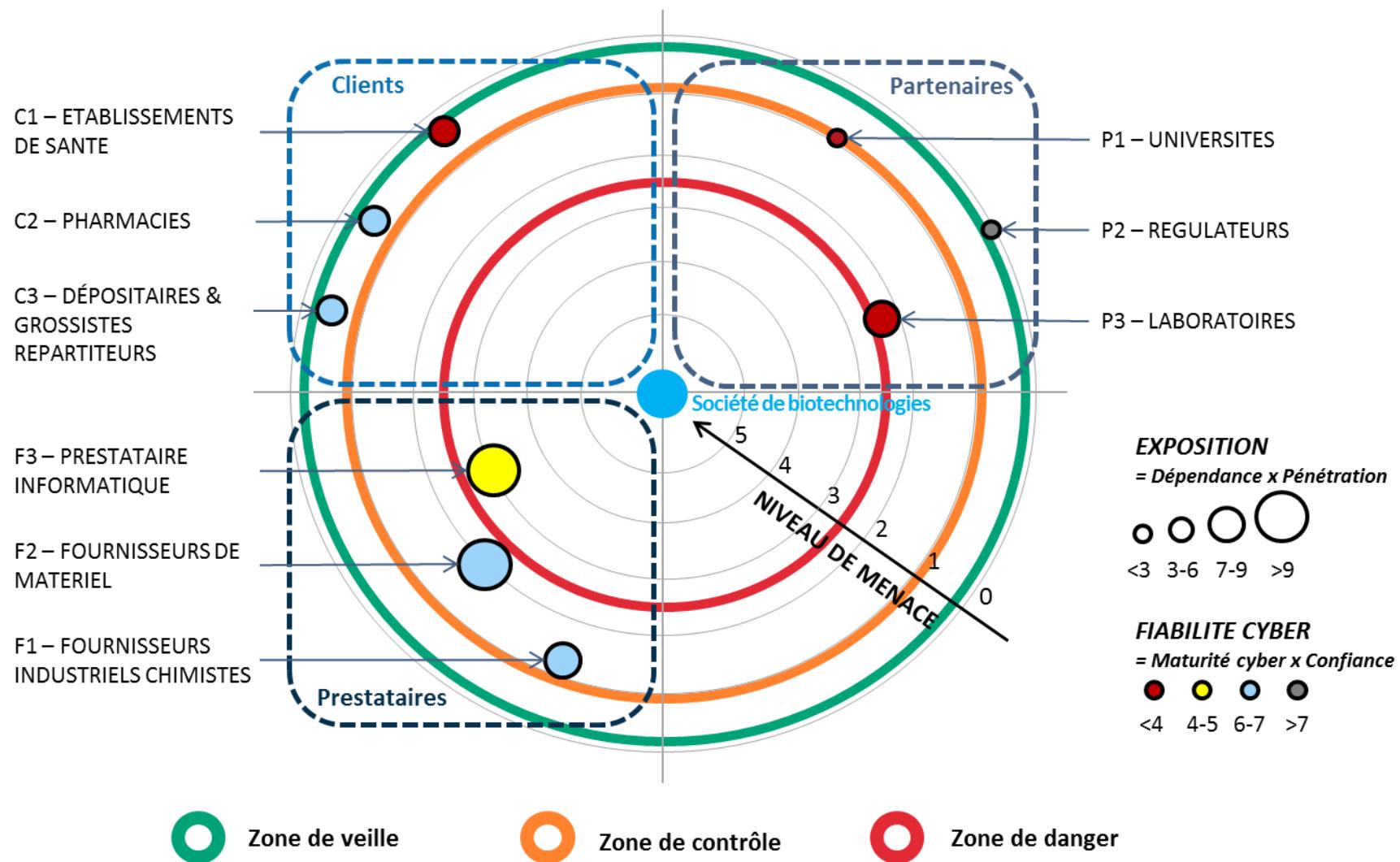
Société de biotechnologies – Atelier 3 : corrigé

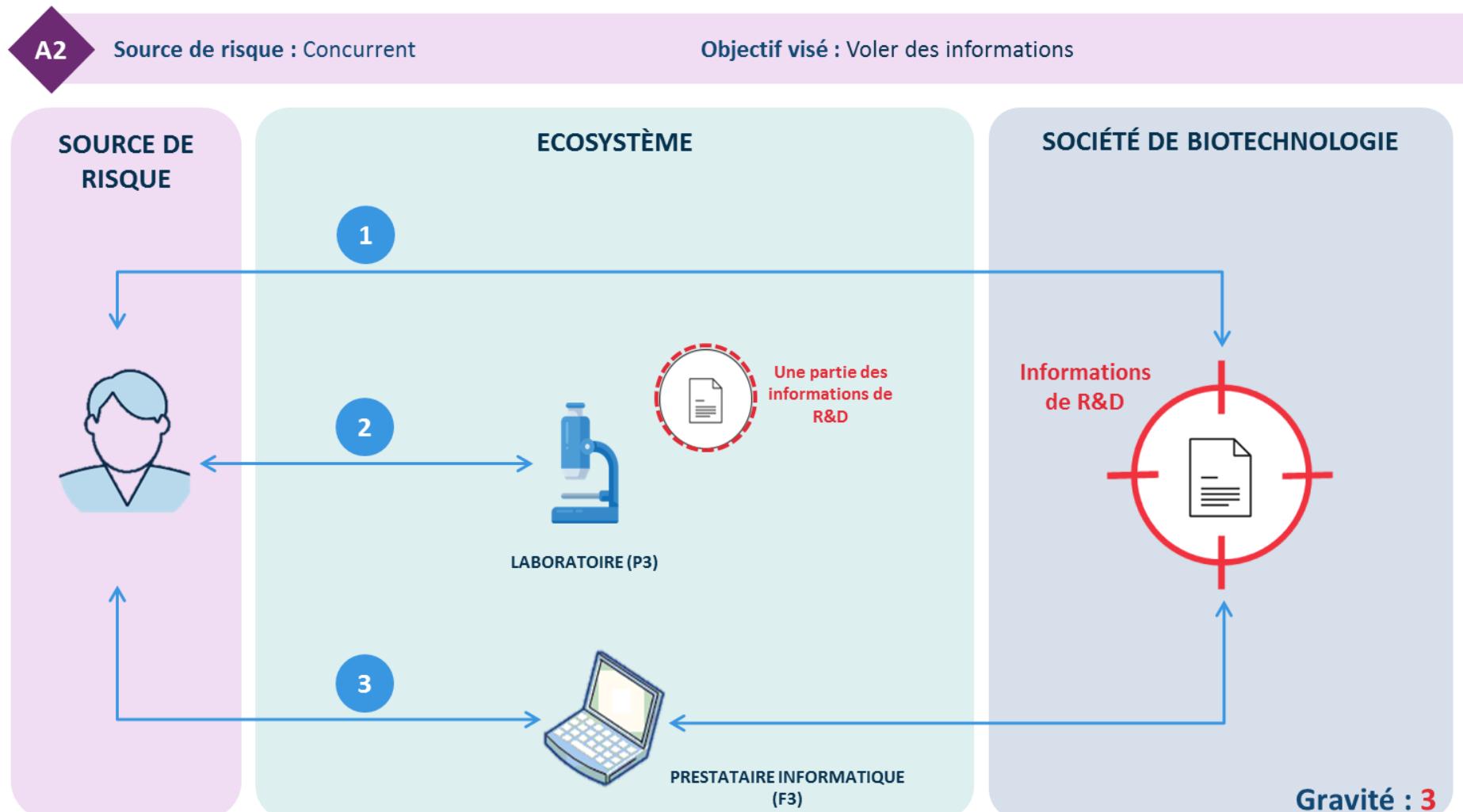
| CATÉGORIE | NOM | DÉPENDANCE | PÉNÉTRATION | MATURITÉ CYBER | CONFiance | NIVEAU DE MENACE |
|-------------|--|------------|-------------|----------------|-----------|------------------|
| Client | C1 - Établissements de santé | 1 | 1 | 1 | 3 | 0,3 |
| Client | C2 - Pharmacies | 1 | 1 | 2 | 3 | 0,2 |
| Client | C3 - Grossistes répartiteurs | 1 | 2 | 2 | 3 | 0,3 |
| Partenaire | P1 - Universités | 2 | 1 | 1 | 2 | 1 |
| Partenaire | P2 - Régulateurs (ANSM, EMA...) | 2 | 1 | 2 | 4 | 0,25 |
| Partenaire | P3 - Laboratoires | 3 | 3 | 2 | 2 | 2,25 |
| Prestataire | F1 - Fournisseurs industriels chimistes | 4 | 2 | 2 | 3 | 1,3 |
| Prestataire | F2 - Fournisseurs de matériel (chaîne de production) | 4 | 3 | 2 | 3 | 2 |
| Prestataire | F3 - Prestataire informatique | 3 | 4 | 2 | 2 | 3 |



EXPOSITION

FIABILITÉ CYBER





Un scénario stratégique constitué de 3 chemins d'attaque

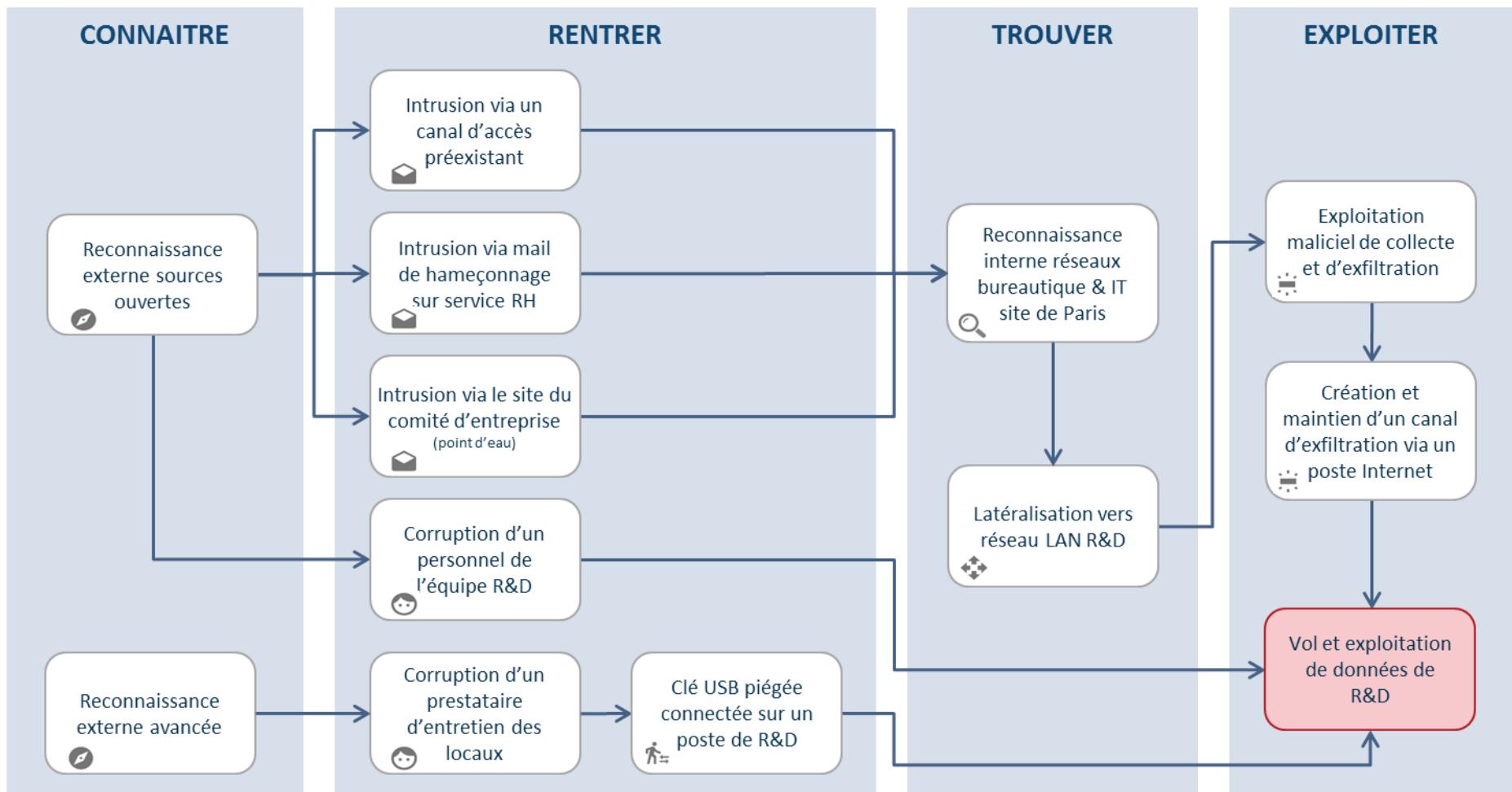
Société de biotechnologies – Atelier 4 : corrigé

A3

Scénario stratégique : Un concurrent vole des informations de R&D

Chemin d'attaque : n°1 – attaque directe

Gravité : 3



Etude de cas – Renouvellement de titre d'identité numérique

Introduction

Vous êtes amené à réfléchir sur un cas d'étude se basant sur la démarche administrative de renouvellement d'un titre d'identité numérique (TIN).

Bien que s'appuyant sur une démarche concrète, l'ensemble des éléments présentés dans la suite de ce dossier est fictif (les noms des organisations, les vulnérabilités énoncées, l'architecture des différents systèmes d'information, etc.).

Les éléments décrits dans le présent dossier ont vocation à accompagner le participant à :

- visualiser la démarche de renouvellement d'un titre d'identité numérique ;
- visualiser l'écosystème dans lequel cette démarche s'inscrit ;
- présenter l'architecture des différents systèmes d'information ;
- identifier les vulnérabilités disséminées alimentant l'étude de cas.

Contexte

Généralités

Dans le cadre de l'homologation du système d'information utilisé pour la démarche administrative de renouvellement de titre d'identité numérique, la Société de Gestion des Titres d'Identité Numérique (SGTIN) vous sollicite pour constituer le dossier d'homologation. À ce titre, vous êtes chargé de la réalisation d'une étude des risques cyber dont le périmètre couvre la mission de renouvellement de titres d'identité numérique.

Le système d'information étudié étant déjà en production, l'autorité d'homologation, afin de prononcer l'homologation, a commandité un audit de la sécurité du système d'information qui doit permettre de vérifier les pratiques de sécurité d'un point de vue organisationnel, physique et technique.

Les éléments fournis dans la suite du présent dossier de l'étude de cas sont issus :

- des entretiens avec les « métiers » pour la compréhension de la démarche de renouvellement d'un titre d'identité numérique ;
- des entretiens avec les « opérationnels » pour la compréhension du système d'information, et les interconnexions associées, mis en œuvre dans le cadre du renouvellement d'un titre d'identité numérique ;
- des résultats de l'audit SSI du système étudié qui présentent, entre autres, les points faibles relevés.

Réglementation

Compte-tenu de la nature des acteurs et des services étudiés, le Référentiel Général de Sécurité est pleinement applicable aux acteurs et aux systèmes d'information suivants :

- acteurs : la mairie et la SGTIN ;
- systèmes d'information : les systèmes d'information sous la responsabilité des acteurs listés ci-après.

Présentation de la démarche administrative : renouvellement de titre d'identité numérique

L'étude de cas se penche, comme rappelé en introduction, sur la démarche administrative de renouvellement de titre d'identité numérique. La Figure 1 illustre le déroulé de ladite démarche.

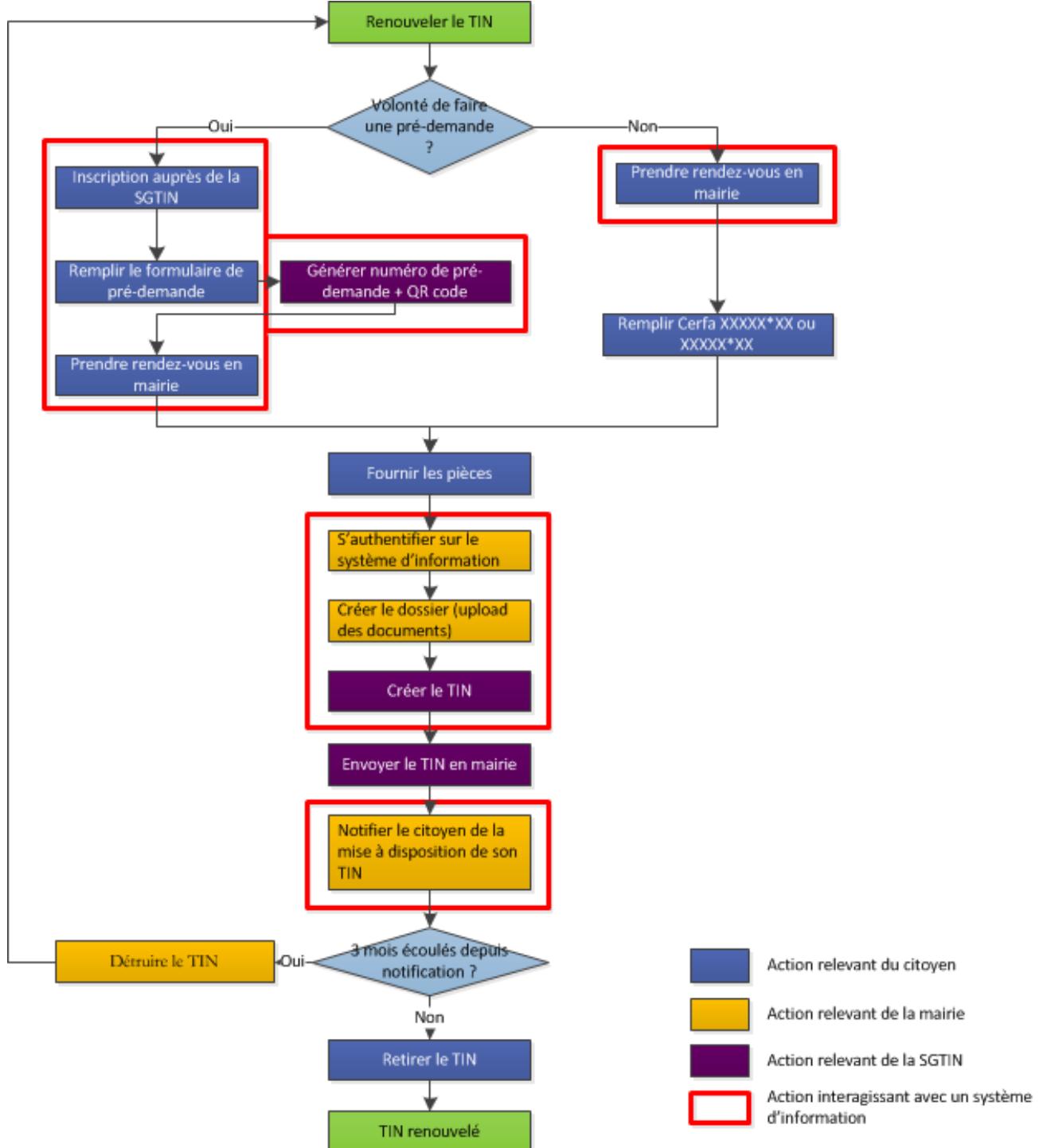


Figure 1 : Diagramme de flux de la démarche de renouvellement de titres d'identité numérique

N.B. : sont exclus de la présente étude des risques :

- *le processus de déclaration de perte ou de vol du titre d'identité numérique ;*
- *le processus de destruction du titre d'identité numérique.*

Présentation de l'écosystème entourant la démarche de renouvellement de titres d'identité numérique

Les acteurs

Dans le cadre de cette démarche, nous avons retenu un certain nombre d'acteurs qui participent directement à la démarche de renouvellement de titres d'identité numérique. Ainsi nous identifions :

- **l'Autorité Nationale de Gestion des Titres d'identité numérique (ANGT)** : autorité en charge des questions relatives aux TIN, à savoir :
 - définition des caractéristiques relatives aux titres d'identité numérique,
 - agrément (définition du processus et acte de délivrance de l'agrément) des sociétés à produire des titres d'identité numérique,
 - contrôle des sociétés produisant des titres d'identité numérique ;
- **le citoyen** : il est l'acteur à l'origine du processus ;
- **la mairie** : elle est l'acteur en charge de :
 - la prise en compte de la demande de renouvellement,
 - la saisie de la demande dans le système d'information de renouvellement de TIN et le contrôle des pièces justificatives,
 - la remise du titre d'identité numérique (il n'est pas utile de prendre rendez-vous pour récupérer son TIN en mairie) ;
- **la Société de Gestion des Titres d'Identité Numérique (SGTIN)** : la SGTIN est la société qui s'occupe de l'édition des titres d'identité numérique. L'agent de cette société a pour rôle de traiter les informations contenues dans la demande saisie par la mairie, pour l'édition et l'envoi du TIN à cette dernière. Cette société fait l'objet d'inspections annuelles de la part de l'ANGT afin de s'assurer du respect des exigences contractuelles de qualité et de sécurité ;
- **la société d'administration du SI de renouvellement de TIN** : la société a pour rôle d'infogérer le système d'information (**Maintien en Condition Opérationnelle (MCO)**, **Maintien en Condition de Sécurité (MCS)**, évolutions fonctionnelles...) mis en œuvre dans le cadre du renouvellement des TIN ainsi que de prendre en main à distance le poste de travail de l'agent en mairie si besoin ; l'équipe en charge de l'administration du SI de renouvellement des titres d'identité numérique sera appelée « service d'administration » dans la suite de ce dossier d'étude. Cette société, sélectionnée via un marché interministériel (pour lequel des exigences de niveau de service et de sécurité sont définies), dispose d'une certification valide selon la norme ISO 9001:2015 sur le domaine d'application couvrant notamment les activités de MCO / MCS d'infrastructures et d'application ;
- **Héberweb, la société d'hébergement du SI de renouvellement des TIN**, sélectionnée via un marché interministériel (pour lequel des exigences de niveau de service et de sécurité sont définies). Cette société dispose d'une certification valide selon la norme ISO/CEI 27001:2013 sur le domaine d'application couvrant les activités d'hébergement et de services associées à l'hébergement. Elle assure notamment :
 - l'hébergement physique du SI,
 - la fourniture des gestes de proximité (redémarrage d'un serveur, installation physique d'équipement, câblage, etc.),
 - la fourniture d'un accès internet,
 - le contrôle d'accès physique,

- la fourniture des dispositifs de protection contre les menaces environnementales (protection incendie, dispositifs de refroidissement, dispositifs de protection électrique) ;
- **la société d'acheminement des titres d'identité numérique** qui livre les TIN, imprimés par la SGTIN, à la mairie concernée. Le contrat entre la société d'acheminement des titres d'identité numérique et la SGTIN ne mentionne pas de clauses de sécurité particulières.

Les systèmes d'information en présence

A l'exception de la société d'acheminement des TIN, nous considérons l'ensemble des systèmes d'information de l'ensemble des acteurs listés ci-dessus. Nous détaillons ici le rôle de chacun des systèmes d'information (SI) :

- **le SI du citoyen** : architecture basique qui se compose :
 - du poste de travail de l'utilisateur ;
 - du routeur/pare-feu fourni et préconfiguré par le FAI (fournisseur d'accès à Internet) permettant à l'utilisateur d'accéder à Internet ;
- **le SI de la mairie**, qui est constitué :
 - du poste de travail de l'agent en mairie ;
 - d'un routeur qui permet aux agents de mairie d'accéder à Internet et qui assure également la fonction de pare-feu ;
- **le SI de renouvellement de TIN** : hébergé chez Héberweb, un hébergeur spécialisé, c'est le système central qui permet de gérer le processus de renouvellement de titres d'identité numérique. Il se présente sous la forme d'une architecture trois tiers classique avec le frontal qui permet à l'utilisateur d'interagir avec le SI (couche de présentation), un serveur de traitement des requêtes faites par l'utilisateur (couche application) et la base de données contenant les dossiers de renouvellement (couche base de données). Les fonctions assurées par le SI sont les suivantes :
 - l'enregistrement des prises de rendez-vous en mairie,
 - la saisie d'une nouvelle demande et le téléversement (*upload*) des pièces fournies,
 - la notification à la SGTIN de l'existence d'une nouvelle demande de renouvellement à prendre en compte,
 - le partage d'informations entre le SI de la mairie et le SI de la SGTIN au moyen d'un serveur de fichiers sur lequel sont déposées les nouvelles demandes de titres d'identité numérique via une extraction quotidienne depuis la base de données ;
- **le SI de la SGTIN** qui se décompose en deux sous-systèmes :
 - **le SI de pré-demande**, permettant aux citoyens de faciliter la démarche en mairie en effectuant une pré-demande en ligne et dont l'architecture est similaire à celle du SI de renouvellement de titres d'identité numérique détaillée précédemment,
 - **le SI d'impression des TIN** dans lequel nous retrouvons un serveur de fichiers qui permet le rapatriement des dossiers de renouvellement de titres d'identité numérique sur le SI de la SGTIN et le serveur d'impression pour l'impression des TIN.

Il est à noter que l'interconnexion entre le SI de la mairie et le SI de renouvellement de TIN repose sur un réseau homologué. Les besoins de sécurité de ce réseau sont en adéquation avec les besoins du SI de renouvellement de TIN.

Le schéma ci-après donne une représentation simplifiée des différents SI et de leurs interactions.

E BIOS Risk Manager – Cas d'étude fictif : Renouvellement de titres d'identité numérique

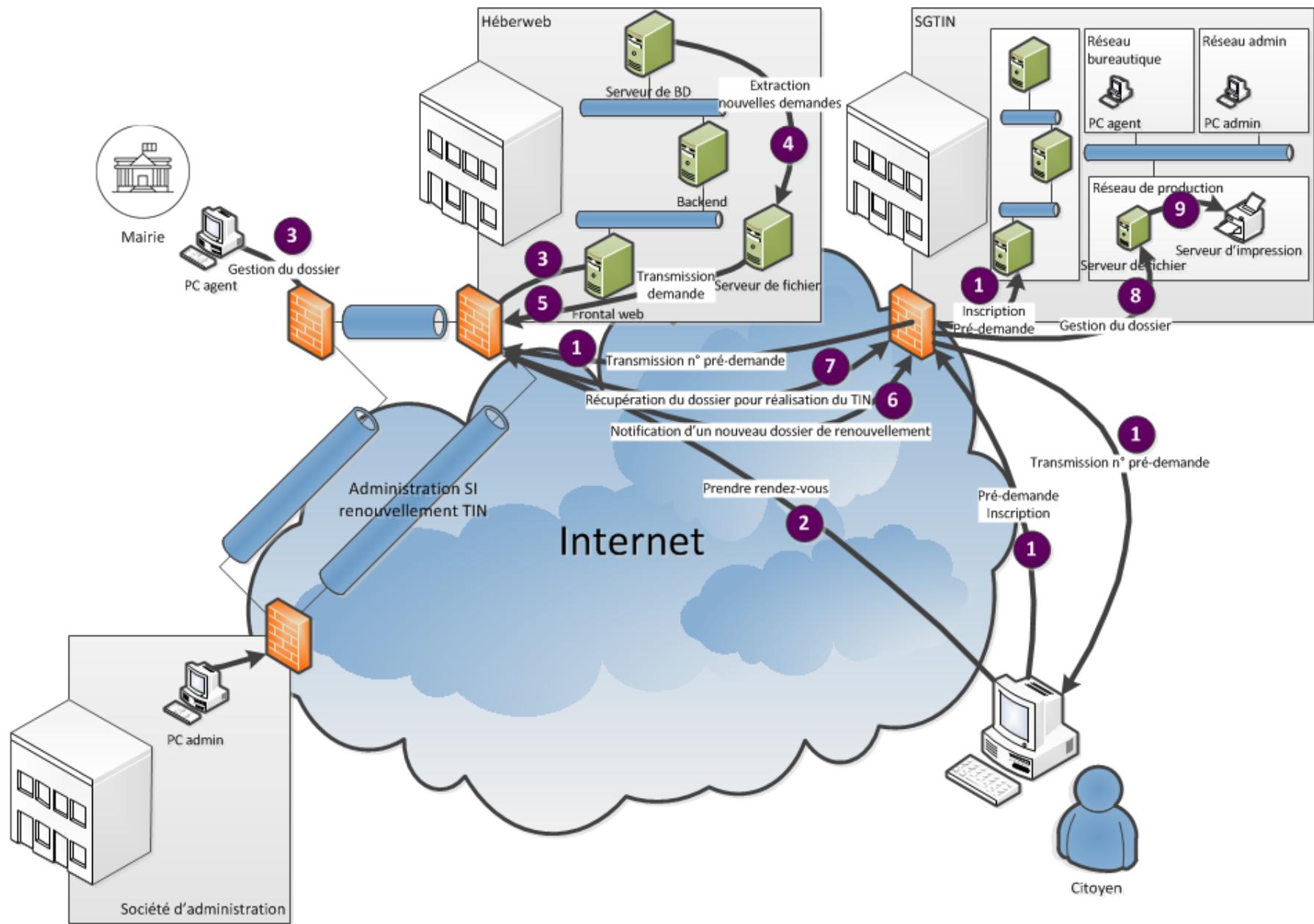


Figure 2 : Schéma d'infrastructure réseau

SGTIN – Définir le périmètre métier et technique

| MISSION | RENOUVELER DES TITRES D'IDENTITÉ NUMÉRIQUE | | | | | | | |
|------------------------------------|--|--|--|--|--|--|--|--|
| NOM DE LA VALEUR MÉTIER | | | | | | | | |
| NATURE DE LA VALEUR MÉTIER | | | | | | | | |
| ENTITÉ RESPONSABLE | | | | | | | | |
| NOM DU/DES BIENS SUPPORTS ASSOCIÉS | | | | | | | | |
| ENTITÉ OU PERSONNE RESPONSABLE | | | | | | | | |

SGTIN – Identifier les événements redoutés

| ÉCHELLE | DÉFINITION |
|--------------------|---|
| G4 – CRITIQUE | Les impacts découlant de la réalisation de l'événement redouté peuvent conduire à la création d'identités erronées ou à l'usurpation d'identité |
| G3 – GRAVE | Les impacts découlant de la réalisation de l'événement redouté ne permettent pas à l'organisation de réaliser tout ou partie de son activité |
| G2 – SIGNIFICATIVE | Les impacts découlant de la réalisation de l'événement redouté sont significatifs sur les performances de l'activité (dégradation des performances) |
| G1 – MINEURE | Les impacts découlant de la réalisation de l'événement redouté sont négligeables (des solutions de contournement existent et sont efficaces) |

Échelle de gravité définie par la SGTIN

| Impact | Exemples (listes non exhaustives) |
|---|--|
| Impacts sur les missions et services de l'organisme | |
| Conséquences directes ou indirectes sur la réalisation des missions et services. | Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé. |
| Impacts sur la gouvernance de l'organisme | |
| <u>Impacts sur la capacité de développement ou de décision</u> Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement. | Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés. |
| <u>Impacts sur le lien social interne</u> Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation. | Perte de confiance des employés dans la pérennité de l'organisme, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, affaiblissement/perte de sens des valeurs communes. |
| <u>Impacts sur le patrimoine intellectuel ou culturel</u> Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes. | Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés. |
| Impacts humains, matériels ou environnementaux | |
| <u>Impacts sur la sécurité ou sur la santé des personnes</u> Conséquences directes ou indirectes sur l'intégrité physique de personnes. | Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire. |
| <u>Impacts matériels</u> Dégâts matériels ou destruction de biens supports. | Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématuée de matériels. |
| <u>Impacts sur l'environnement</u> Conséquences écologiques à court ou long terme, directes ou indirectes. | Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère. |
| Impacts financiers | |
| Conséquences pécuniaires, directes ou indirectes. | Perte de chiffre d'affaire, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées. |
| Impacts juridiques | |
| Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle. | Procès, amende, condamnation d'un dirigeant, amendement de contrat. |
| Impacts sur l'image et la confiance | |
| Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients. | Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété, perte de confiance d'usagers. |

Catégories d'impacts proposées dans EBIOS Risk Manager

| VALEUR MÉTIER | ÉVÉNEMENT REDOUTÉ | CATÉGORIES D'IMPACT | GRAVITÉ | COMMENTAIRES / JUSTIFICATION |
|---------------------------|---|---|---------|---|
| Informations des citoyens | Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.) | <ul style="list-style-type: none"> Impact juridique (RGPD) Impact d'image | 4 | <ul style="list-style-type: none"> Usurpation d'identité |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

SGTIN – Évaluer les couples SR/OV

| | | RESSOURCES | | | |
|--|------------------|--|---------------------------|------------------------|-----------------------|
| | | Incluant les ressources financières, le niveau de compétences cyber, l'ouillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc. | | | |
| | | Ressources limitées | Ressources significatives | Ressources importantes | Ressources illimitées |
| MOTIVATION Intérêts, éléments qui poussent la source de risque à atteindre son objectif | Fortement motivé | Moyennement pertinent | Plutôt pertinent | Très pertinent | Très pertinent |
| | Assez motivé | Moyennement pertinent | Plutôt pertinent | Plutôt pertinent | Très pertinent |
| | Peu motivé | Peu pertinent | Moyennement pertinent | Plutôt pertinent | Plutôt pertinent |
| | Très peu motivé | Peu pertinent | Peu pertinent | Moyennement pertinent | Moyennement pertinent |

Échelle de pertinence des couples SR/OV définie par la SGTIN

| SOURCES DE RISQUE | OBJECTIF VISÉ | MOTIVATION | RESSOURCES | PERTINENCE |
|----------------------------|--|--------------|---------------------------|------------------|
| Agent malveillant SGTIN | Discréder ou saboter le service de renouvellement de TIN | Assez motivé | Ressources significatives | Plutôt pertinent |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

SGTIN – Établir le lien entre les événements redoutés et les couples SR/OV

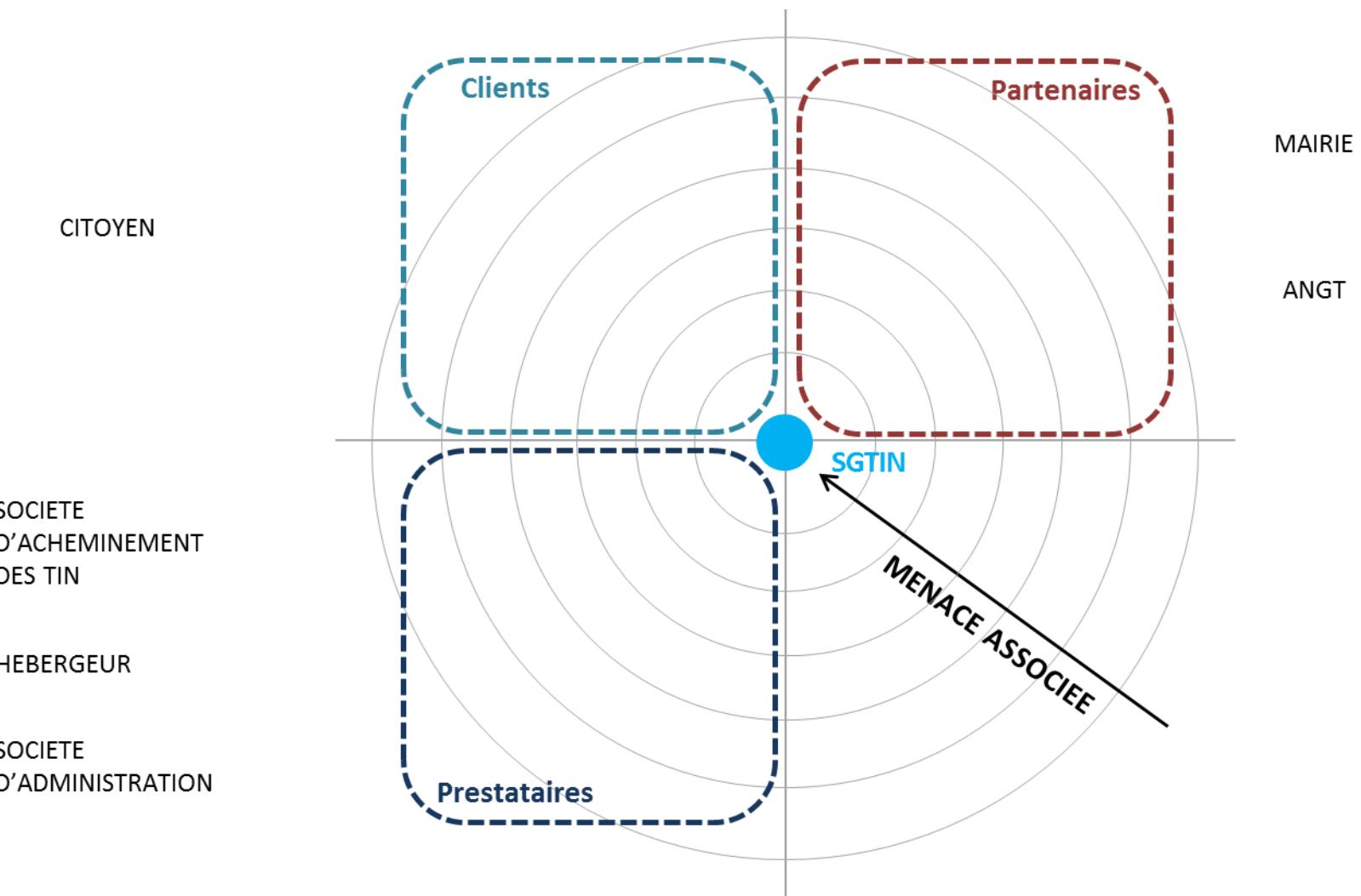
| SR/OV les plus pertinents | | ER les plus graves | |
|-----------------------------|--|---|---------------------------|
| SOURCES DE RISQUE | OBJECTIF VISÉ | ÉVÉNEMENT REDOUTÉ | VALEUR MÉTIER |
| Organisation de malfaiteurs | Gagner de l'argent en collectant des informations ou en revendant des TIN | Certains TIN imprimés ne correspondent pas à des demandes légitimes | Impression des TIN |
| Hacktiviste | Perturber la fabrication des TIN | Vol de TIN légitimes durant leur acheminement à la mairie | Distribution des TIN |
| État | Faire fabriquer des faux TIN pour faire circuler des espions sur le territoire | Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.) | Informations des citoyens |

SGTIN – Construire la cartographie de menace de l'écosystème

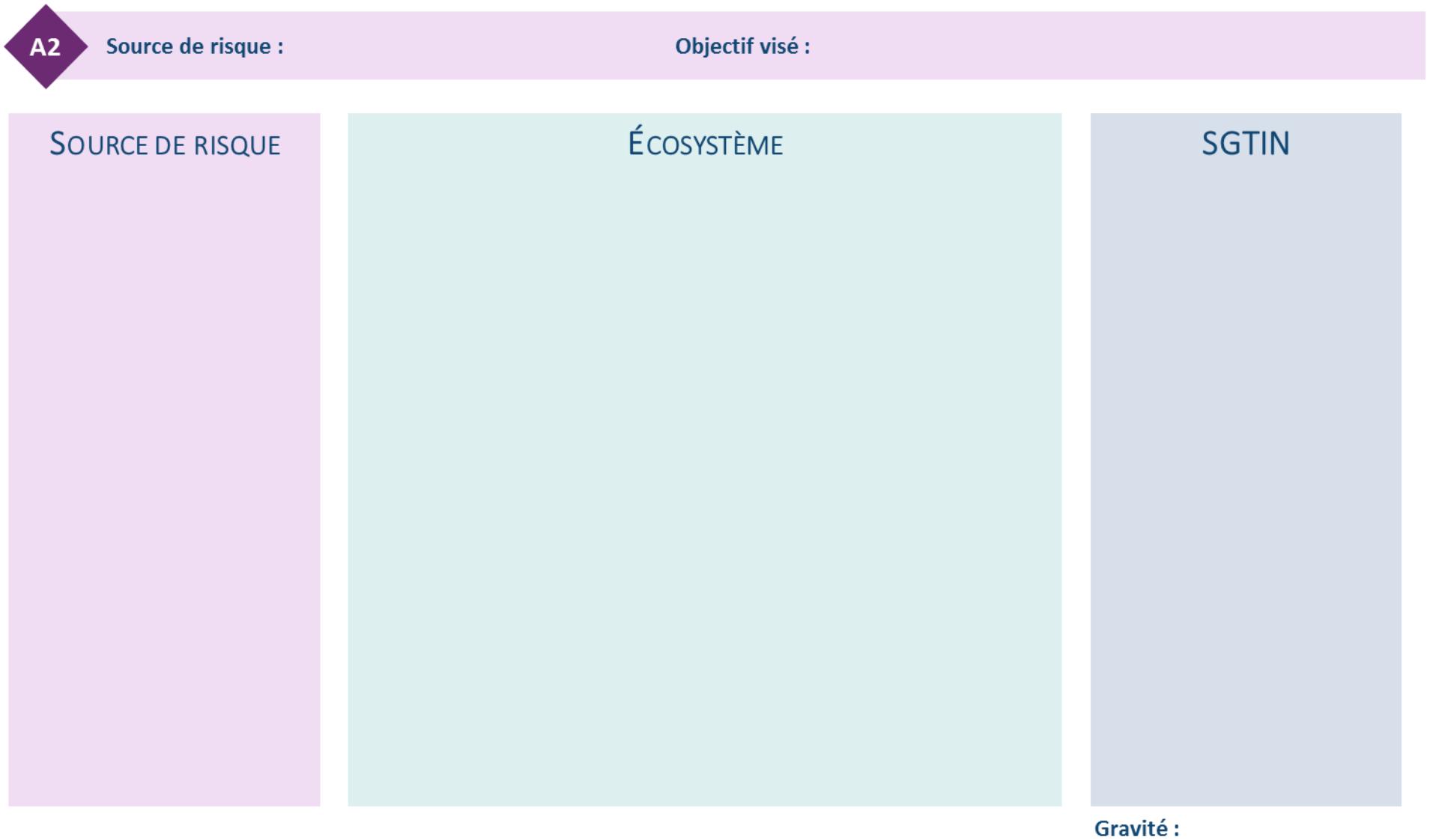
| | | DÉPENDANCE | PÉNÉTRATION | MATURITÉ CYBER | CONFIANCE |
|---|---|--|-------------|--|---|
| 1 | Pas de lien avec le SI de la partie prenante pour réaliser la mission | Pas d'accès au système d'information de la SGTIN ni aux TIN. | | <ul style="list-style-type: none"> • Pas d'information sur le niveau de maturité • OU 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 à des postes de travail de la SGTIN en mode utilisateur ou accès physique aux bureaux de la SGTIN | | <p>Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale.</p> <p>La sécurité numérique est assurée selon un mode réactif.</p> | 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) | <ul style="list-style-type: none"> • Accès avec priviléges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.) • OU accès aux TIN • OU accès étendu au SI ponctuellement à des fins d'audit et de contrôle | | <p>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.</p> | 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) | <ul style="list-style-type: none"> • Accès avec priviléges de type administrateur à des équipements d'infrastructure (annuaires d'entreprise, DNS, baies de stockage, etc.) • OU accès physique aux salles serveurs où sont stockées les informations des citoyens | | <p>La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive.</p> | Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée. |

Formation EBIOS Risk Manager – Livret stagiaire

| CATÉGORIE | NOM | DÉPENDANCE | PÉNÉTRATION | MATURITÉ CYBER | CONFiance | NIVEAU DE MENACE |
|-------------|---|------------|-------------|----------------|-----------|------------------|
| Utilisateur | Citoyen | | | | | |
| Partenaire | Mairie | | | | | |
| Partenaire | Autorité Nationale de Gestion des Titres (ANGT) | | | | | |
| Prestataire | Société d'administration | | | | | |
| Prestataire | Hébergeur (Héberweb) | | | | | |
| Prestataire | Société d'acheminement des TIN | | | | | |



SGTIN – Élaborer des scénarios stratégiques



Les conclusions de l'audit

Les conclusions de l'audit ont remonté un certain nombre de points dont voici une synthèse.

Sécurité de Héberweb

L'audit de la sécurité physique de l'hébergeur du SI de renouvellement de titres d'identité numérique a permis de vérifier qu'un contrôle d'accès strict était mis en œuvre pour permettre aux seules personnes en ayant le besoin, d'accéder aux zones d'hébergement. Les personnes amenées à intervenir ponctuellement dans les locaux de Héberweb (prestataires, fournisseurs, visiteurs, etc.) sont systématiquement accueillies et enregistrées dans un cahier d'émargement. Elles sont accompagnées en permanence, pendant toute la durée de leur intervention dans les zones d'hébergement.

La sécurité physique chez Héberweb a permis de vérifier que des bonnes pratiques quant au dimensionnement et au maintien en condition de sécurité des équipements de sûreté environnementale (refroidissement, protection incendie, protection électrique) étaient en place.

De plus l'audit a permis de démontrer un bon maintien en condition de sécurité des équipements sous la responsabilité de l'hébergeur (parc homogène avec des systèmes d'exploitation et des applicatifs maintenus par leurs éditeurs et pour lesquels les correctifs de sécurité très récents avaient été appliqués).

En revanche, l'audit a mis en évidence une absence de gestion de l'acquisition, de la maintenance et de la fin de vie des équipements informatiques. En effet les auditeurs ont constaté que les équipements en attente de mise en production ou désengagés étaient entreposés dans un local dont l'accès était ouvert à l'ensemble du personnel de Héberweb. Pour le cas particulier de la fin de vie, l'hébergeur a confié attendre d'avoir accumulé un volume conséquent de matériels avant de les jeter dans un point de collecte.

De même, pour ces équipements informatiques, les entrevues ont permis d'identifier que l'hébergeur ne disposait pas de procédure de renvoi au fournisseur et que les informations sensibles (règles de filtrage, fichiers de configuration, mots de passe, etc.) pouvaient être amenées à sortir de l'organisation sans contrôle particulier (échange ou réparation de matériel dans le cas d'une garantie par exemple).

Sécurité des moyens d'administration du SI de renouvellement de TIN

Lors de cette phase de l'audit, les auditeurs ont pu observer les pratiques suivantes :

- la connexion de l'administrateur sur les équipements du SI de renouvellement de mot de passe s'effectue via le protocole SSH¹ sur le pare-feu qui sert de machine rebond pour administrer les équipements du SI. La configuration du service d'authentification SSH est une authentification simple par mot de passe ;
- le poste de travail de l'administrateur est utilisé aussi bien pour des tâches bureautiques (messagerie, navigation sur Internet, etc.) que pour des tâches d'administration du SI de renouvellement de titres d'identité numérique ;

¹ **Secure SHell** : protocole d'authentification et de communication, successeur de Telnet, apportant des fonctions de sécurité liées à la confidentialité (chiffrement) et l'intégrité (somme de contrôle) des échanges.

- le frontal web, bien que privilégiant le protocole HTTPS², autorise, lors de l'établissement de la session, l'utilisation de SSL³v3. De plus, un aperçu des ports a permis d'identifier que les ports TCP 137, 139 et 445 (SMBv1⁴) n'étaient pas filtrés alors que les services SMB sont actifs sur ce frontal.
- Globalement, les audits de configuration effectués sur le SI de renouvellement de TIN (dont le service d'administration à la charge) ont montré une forte hétérogénéité et l'existence de serveurs Windows 2008 R2, notamment pour le serveur de fichier. Ce constat est renforcé par l'observation d'outils de télé-administration (TeamViewer) sur ces serveurs pour lesquels l'administrateur n'a su fournir d'explication ; les entretiens ont mis en évidence que l'authentification par l'agent de mairie sur le SI de renouvellement de titres d'identité numérique s'effectue par mot de passe, sans application d'une politique contraignante de format de mot de passe. De plus, les comptes utilisateurs ne sont pas automatiquement verrouillés après saisie d'un certain nombre de tentatives de connexion infructueuses consécutives. Ces constats ont été confirmés par l'audit de configuration.

Sécurité de la mairie

L'audit a mis en évidence des lacunes au niveau de la sécurité physique, compte tenu du fait que la zone d'accueil des visiteurs est mitoyenne à la zone de travail, sans présence de contrôle d'accès. De plus, les entretiens ont montré que le poste de travail de l'agent en mairie était utilisé aussi bien pour les aspects bureautiques (messagerie, navigation sur Internet, etc.) que pour les actions relevant de la mairie dans le cadre de la démarche de renouvellement de TIN. Pour des raisons opérationnelles, le poste de travail de l'agent est portable. Il utilise un système d'exploitation maintenu par l'éditeur et, afin d'alléger le service d'administration, les droits d'administration ont été octroyés à l'utilisateur pour lui permettre d'installer les outils dont il a besoin dans la limite définie dans la charte informatique. L'audit a permis, également, d'identifier qu'aucun mécanisme de chiffrement de disque n'était mis en œuvre.

Sécurité du SI de la SGTIN

L'audit de la SGTIN a permis d'identifier qu'aucune vérification particulière n'était effectuée sur les dossiers de demande de renouvellement de titres d'identité numérique qu'elle récupérait depuis le serveur de fichier du SI de renouvellement de TIN. Ce constat a été appuyé, lors de l'entretien, par la survenance par le passé d'incidents de qualité impliquant des informations erronées sur les titres d'identité numérique imprimés pour lesquels aucune investigation n'avait été menée mais qui avaient contraint la SGTIN à réimprimer les TIN incriminés.

² **HyperText Transfer Protocol Secure** : protocole de communication sur Internet apportant les fonctions de sécurité (confidentialité, intégrité, authenticité) qui manquaient au protocole HTTP

³ **Secure Socket Layer** : protocole de sécurisation des échanges dont les fonctions de sécurité sont la confidentialité, l'intégrité et l'authenticité. Au moment de l'écriture de l'étude de cas, le protocole SSL est reconnu vulnérable à différentes attaques et les experts du domaine conseillent l'adoption du protocole TLSv1.2 (TLSv1.3 ayant fait l'objet d'une approbation en mars 2018 par l'IETF, son implémentation n'est pas encore répandue)

⁴ **Server Message Block** : protocole de partage de ressources (fichiers et imprimantes)

De plus, les entretiens avec les personnes de la SGTIN ont permis d'identifier que la récupération des dossiers de demande de renouvellement depuis le serveur de fichier du SI de renouvellement de titres d'identité numérique s'effectue via le protocole d'échange de fichier FTP⁵.

L'authentification au sein de la SGTIN est centralisée au moyen du SSO⁶ qui s'appuie sur un annuaire d'entreprise géré par un Active Directory. Les entretiens ont permis de constater que le serveur de fichiers est utilisé pour d'autres activités de la SGTIN (RH, Achat, etc.) et que le cloisonnement entre les différentes activités est assuré par des répertoires distincts pour chaque activité. Cependant, un contrôle plus poussé a permis aux auditeurs de constater que l'accès au répertoire propre à l'activité de renouvellement des TIN était ouvert à l'ensemble des collaborateurs de la SGTIN.

⁵ **File Transfer Protocol** : protocole de transfert de fichier qui ne fournit pas de fonction de sécurité particulière

⁶ **Single Sign On** : dispositif de centralisation de l'authentification permettant aux utilisateurs grâce à un moyen unique d'authentification, d'accéder à un ensemble de ressources (serveurs, applications, fichiers, etc.)

SGTIN – Élaborer des scénarios opérationnels

A3

Scénario stratégique :

Chemin d'attaque :

Gravité :

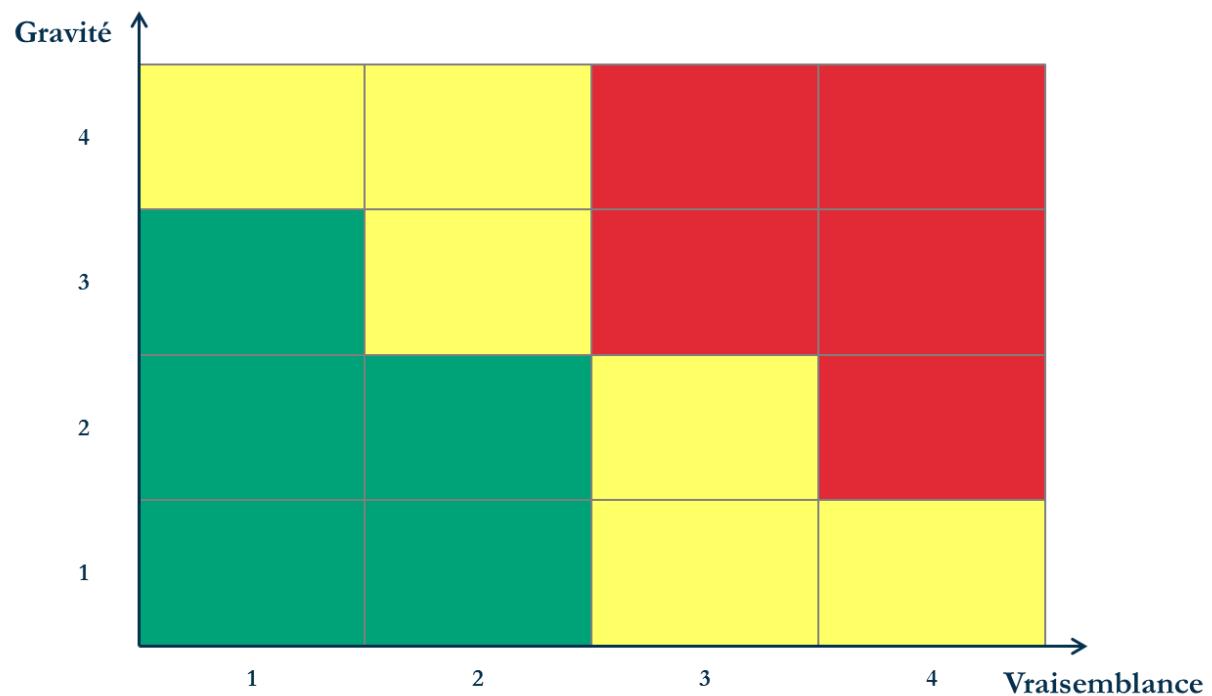
CONNAITRE

RENTRER

TROUVER

EXPLOITER

SGTIN – Réaliser une synthèse des risques



SGTIN – Définir le plan d'amélioration continue de la sécurité (PACS)

| MESURE DE SÉCURITÉ | SCÉNARIOS DE RISQUES ASSOCIÉS | RESPONSABLE | FREINS ET DIFFICULTÉ DE MISE EN ŒUVRE | COÛT / COMPLEXITÉ | ÉCHÉANCE | STATUT |
|--------------------|-------------------------------|-------------|---------------------------------------|-------------------|----------|--------|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |