FORMATION

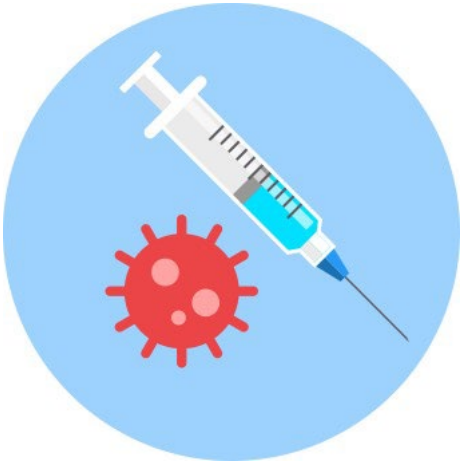
EBIOS *Risk Manager*

Livret stagiaire

V.2.1 • Mai 2024

Formation CFSSI

Biotech : Société de biotechnologie fabriquant des vaccins



Estimation d'un niveau de maturité faible en matière de sécurité numérique

Sensibilisation basique à la sécurité du numérique à la prise de poste des salariés

Existence d'une charte informatique

Exercice : Définir le périmètre métier et technique

Mission(s) :

Dénomination de la Valeur Métier				
Nature de la valeur métier *(processus ou information)*				
Description				
Propriétaire *(interne / externe)*				
Dénomination du / des biens supports associés				
Description				
Propriétaire *(interne / externe)*				

Exercice : Identifier les événements redoutés

Note : les tableaux d'impacts et de gravité se trouvent page suivante.

Valeur métier	Événement redouté	Catégories d'Impact	Gravité
R & D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques	
Fabriquer des vaccins			
Traçabilité et contrôle			

Liste des impacts potentiels

- **Impacts sur les missions et service de l'organisation**
- **Impacts humains, matériels ou environnementaux**
- **Impacts sur la gouvernance**
- **Impacts financiers**
- **Impacts juridiques**
- **Impacts sur l'image et la confiance**

Echelle de gravité

Echelle	Définition
G1 • Mineur	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)
G2 • Significatif	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)
G3 • Important	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)
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)

Exercice : 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)		
Référentiel Général de Sécurité (RGS)		

Exercice : Identifier les événements redoutés

Note : le tableau d'évaluation des couples SR/OV se trouve page suivante.

Source de Risque	Objectif Visé	Motivation	Ressources	Pertinence
Hacktiviste	Divulguer des informations sur les tests animaliers	Peu motivé	Ressources significatives	Moyennement pertinent

Tableau d'évaluation de la pertinence des couples SR/OV

		RESSOURCES Incluant les ressources financières, le niveau de compétences cyber, l'outillage, 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**

Exercice Marriott

**Piratage massif du groupe hôtelier Marriott.
500 millions de clients touchés.**

[Source : 20 minutes – 30/11/2018]

« C'est une méga-fuite de données. Le groupe hôtelier américain Mariott 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. Mariott assure que les numéros de cartes de crédit étaient chiffrés […] Mais la chaine 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	

Exercice Pathé

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

Source : Next inpact – 12/11/2018

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 de risque	
Objectif visé	
Évènement redouté	
Valeur métier	
Bien support	
Impacts	

Exercice : Evaluer la criticité des parties prenantes

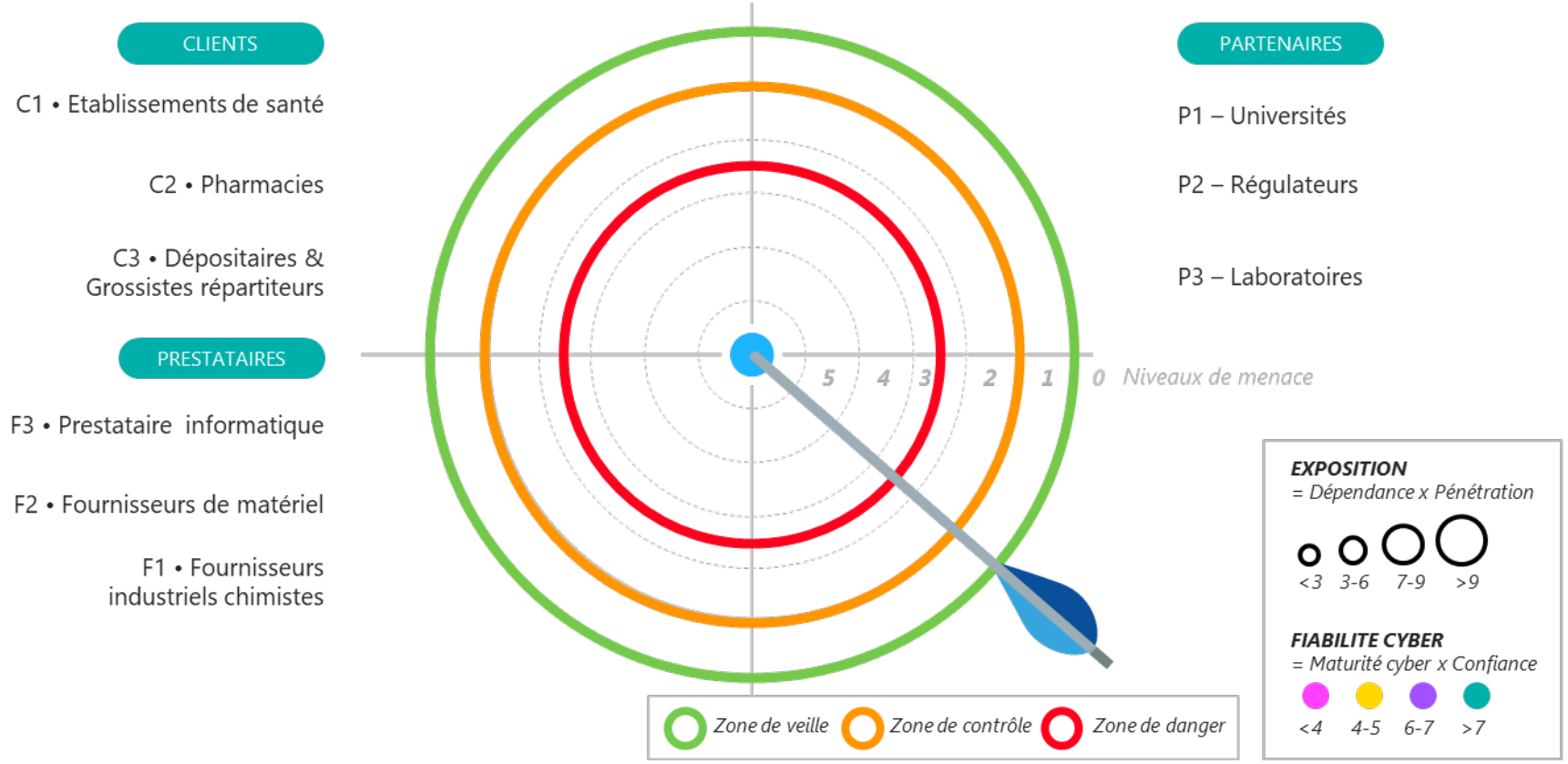
Note : les échelle d'évaluation du niveau de menace des parties prenantes définie par la société de biotechnologies se trouve page suivante.

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					
Prestataire	F2 – Fournisseurs de matériel (chaine de production)					
Prestataire	F3 – Prestataire informatique					

Echelles d'évaluation du niveau de menace des parties prenantes définie par la société de biotechnologies se trouve page suivante.

	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.

Exercice : Construire la cartographie de menace de l'écosystème



Vous pouvez utiliser les cercles ci-dessous pour positionner les parties prenantes puis les colorer.

Exercice : Élaborer les scénarios stratégiques

Source de risque : Concurrent
Objectif visé : Voler des informations
Événement redouté : Fuite des informations d'études et recherches de l'entreprise

Source de risque	Ecosystème	Société de biotechnologie
 Concurrent		 Informations de R&D

Exercice : Définir les mesures de sécurité sur l'écosystème

Partie prenante	Chemin d'attaque stratégique	Mesures de sécurité	Menace initiale	Menace résiduelle
F2 Fournisseur de matériel	Arrêt de production par compromission de l'équipement de maintenance	**Réduire le risque de piègeage des équipements de maintenance utilisés sur le système industriel.** Dotation de matériels de maintenance administrés par la DSI et qui seront mis à disposition du prestataire sur site.	**2**	**1,3**
F3 Prestataire informatique	Vol d'informations en passant par le prestataire informatique		**3**	
P3 Laboratoires	Vol d'informations sur le système d'information du laboratoire		**2,25**	

Exercice : Elaborer les scénarios opérationnels

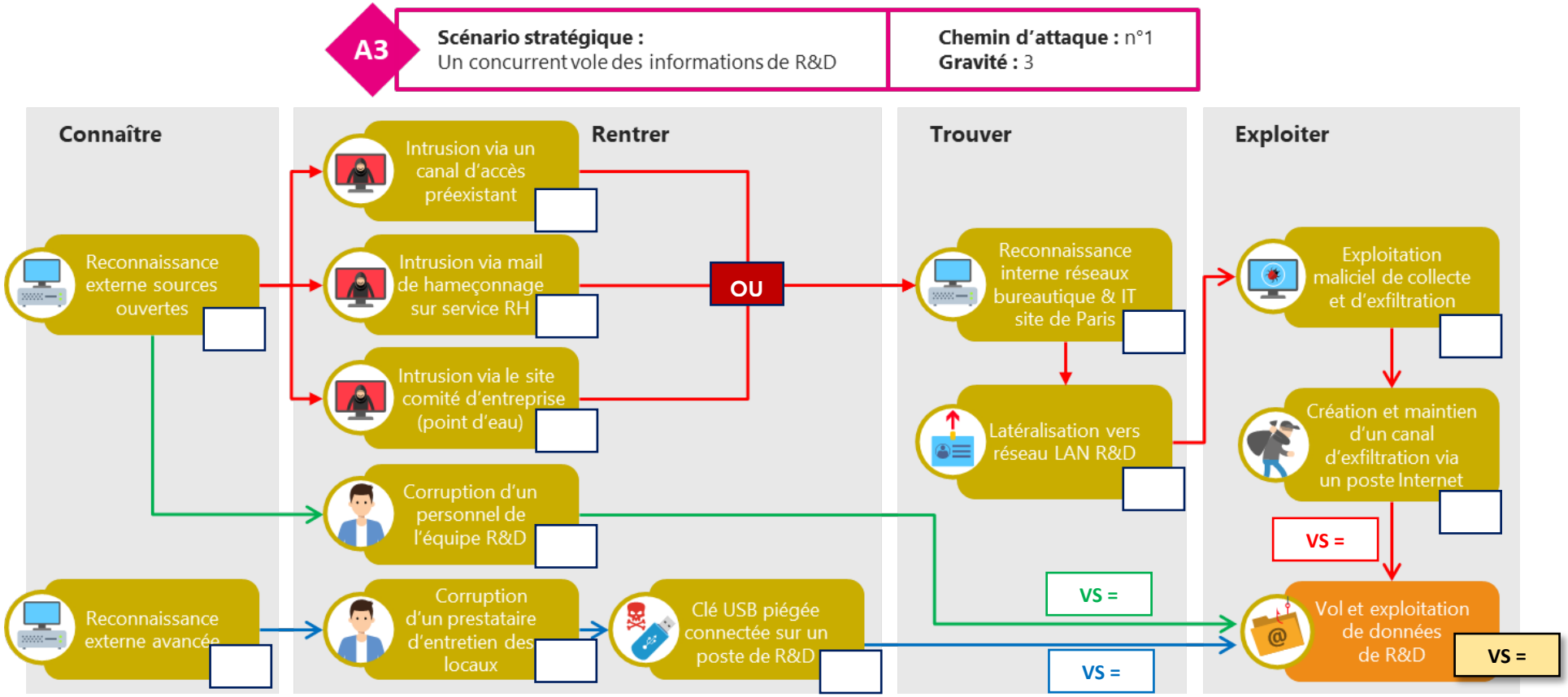
A3

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

Chemin d'attaque : n°1
Gravité : 3

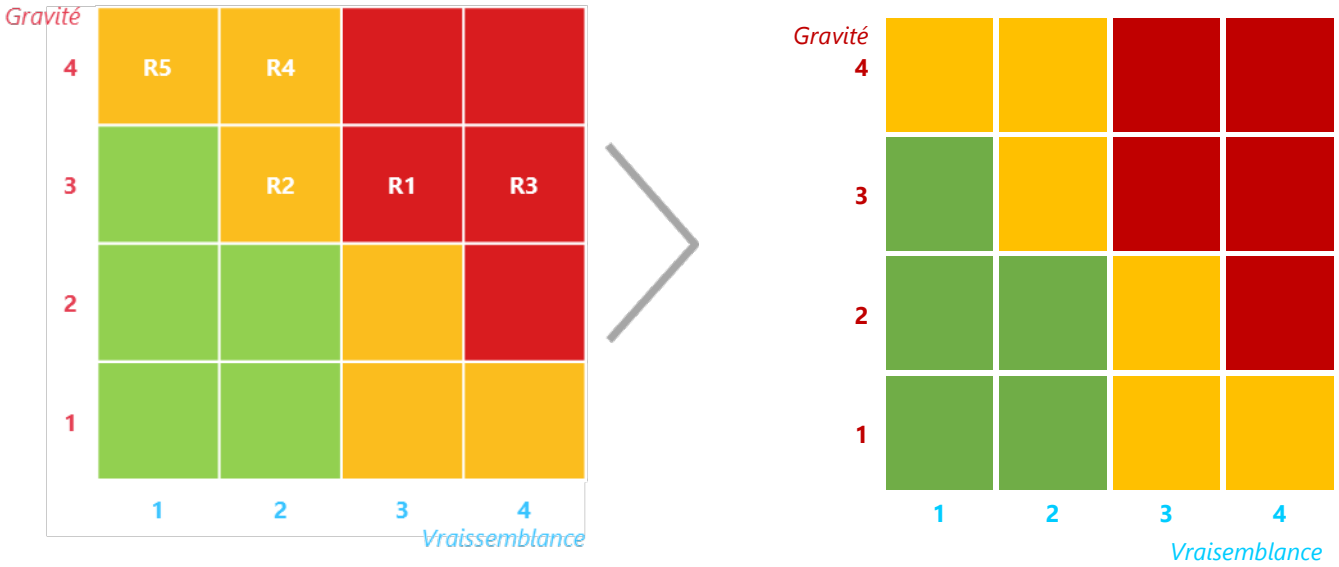
CONNAITRE	RENTRER	TROUVER	EXPLOITER
			Vol et exploitation de données de R&D

Exercice : Evaluation de la vraisemblance



Exercice : Evaluer la cartographie des risques résiduels

Note : les mesures du plan de traitement du risque se trouvent page suivante.



Mesure de sécurité	Risques associés	Responsable	Freins et difficultés de mise en œuvre	Coût / Complexité	Charge estimée	Échéance	Priorité	Statut
GOUVERNANCE								
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation de la hiérarchie obligatoire	+		6 mois		En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI		++	10 j / h		P1	A lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires	R2, R3, R4	Équipe juridique	Effectué au fil de l'eau à la renégociation des contrats	++		18 mois		En cours
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / Équipe juridique		++	5 j / h		P2	A lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires	++		12 mois		A lancer
Limitation des données transmises au laboratoire au juste besoin	R2	Équipe R&D		+		3 mois		Terminé
PROTECTION								
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI		+++		9 mois		En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté		++		3 mois		Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI		++	20 j / h		P3	A lancer
DEFENSE								
Sensibilisation Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil	R1	RSSI	Achat d'un outil, budget à provisionner	++		9 mois		A lancer
RESILIENCE								
Renforcement du plan de continuité d'activité	R4, R5	Équipe continuité d'activité		++		12 mois		En cours

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.

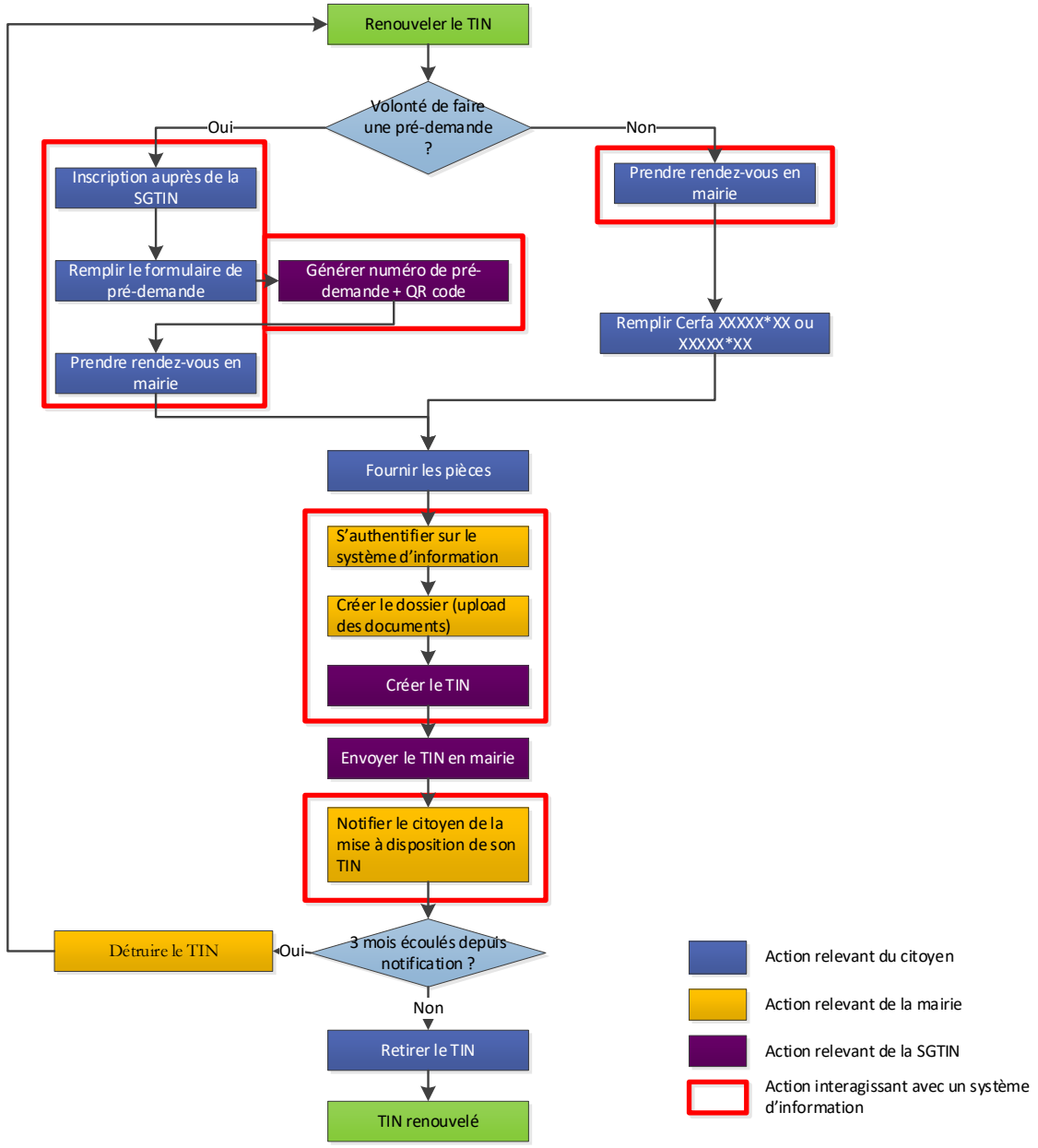


Figure 1 : Diagramme de flux de la démarche de renouvellement de titres d'identité numérique

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.

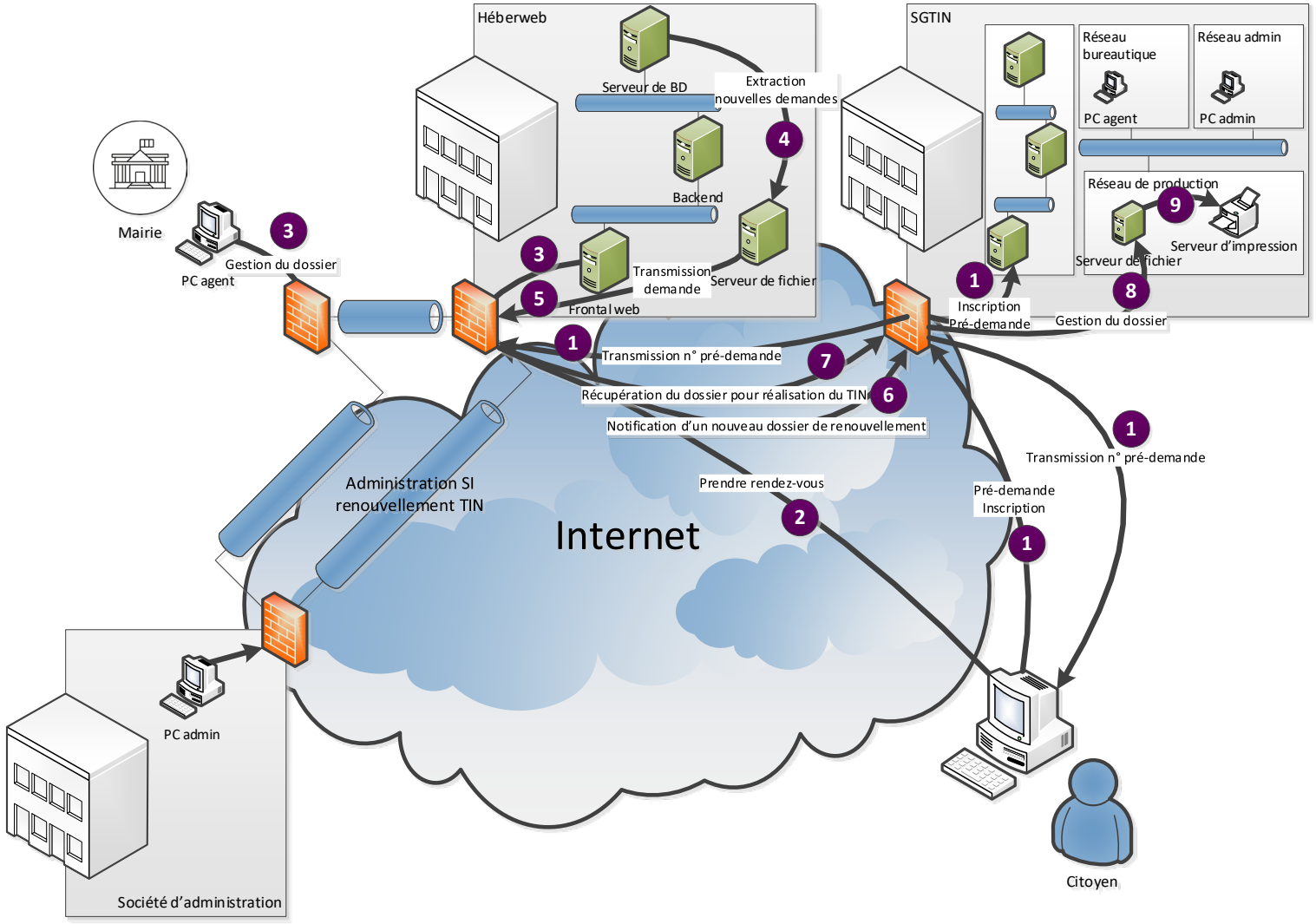


Figure 2 : Schéma d'infrastructure réseau

SGTIN – Définir le périmètre métier et technique

Mission	**Renouveler des titres d'identité numérique**								
Nom de la valeur métier									
Nature de la valeur métier									
Propriétaire									
Nom du/des biens supports associés									
Entité ou personne en charge de la mise en œuvre									

SGTIN – Identifier les événements redoutés

ÉCHELLE	DÉFINITION
G4 – CRITIQUE	Les impacts découlant de la réalisation de l'événement redouté peut 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)

Figure 3 : 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	
Impacts sur la capacité de développement ou de décision 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.
Impacts sur le lien social interne 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.
Impacts sur le patrimoine intellectuel ou culturel 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	
Impacts sur la sécurité ou sur la santé des personnes 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.
Impacts matériels Dégâts matériels ou destruction de biens supports.	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
Impacts sur l'environnement 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, règlementaire, 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.

Figure 4 : Catégories d'impacts proposées dans EBIOS Risk Manager

Valeur métier	Evènement redouté	Catégories d'impact	Gravité	Commentaires / Justification
		•		
		•		
		•		
		•		
		•		
		•		
		•		
		•		
		•		

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**

Figure 5 : Échelle de pertinence des couples SR/OV définie par la SGTIN

Sources de risque	Objectif visé	Motivation	Ressources	Pertinence

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

SR/OV les plus pertinents	
Source de Risque	**Objectif Visé**

ER les plus graves	
Evénement Redouté	**Valeur Métier**

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.	• 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	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.) • **OU** accès aux TIN • **OU** accès étendu au SI ponctuellement à des fins d'audit et de contrôle	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, baies de stockage, etc.) • **OU** accès physique aux salles serveurs où sont stockées les informations des citoyens	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.

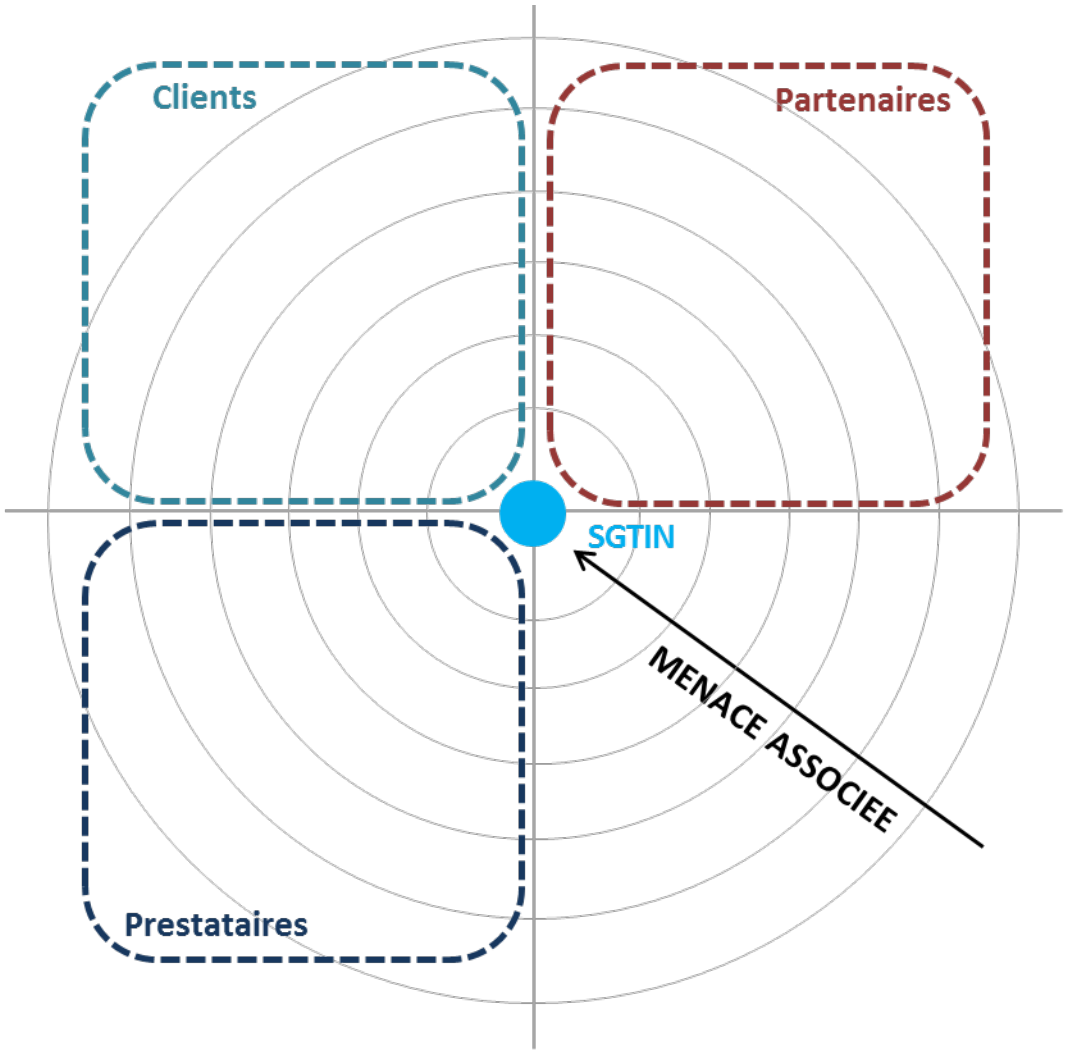
Catégorie	Nom	Dépendance	Pénétration	Maturité cyber	Confiance	Niveau de menace

CITOYEN

SOCIETE
D'ACHEMINEMENT
DES TIN

HEBERGEUR

SOCIETE
D'ADMINISTRATION



MAIRIE

ANGT

SGTIN – Élaborer des scénarios stratégiques

Source de Risque :	**Objectif Visé**

Source de risque	**Ecosystème**	**SGTIN**

Gravité :

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 SSH[1] 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 HTTPS[2], autorise, lors de l'établissement de la session, l'utilisation de SSL[3]v3. De plus, un aperçu des ports a permis d'identifier que les ports TCP 137, 139 et 445 (SMBv1[4]) 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.

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

[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)

renouvellement de titres d'identité numérique s'effectue via le protocole d'échange de fichier FTP[5].

L'authentification au sein de la SGTIN est centralisée au moyen du SSO[6] 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.

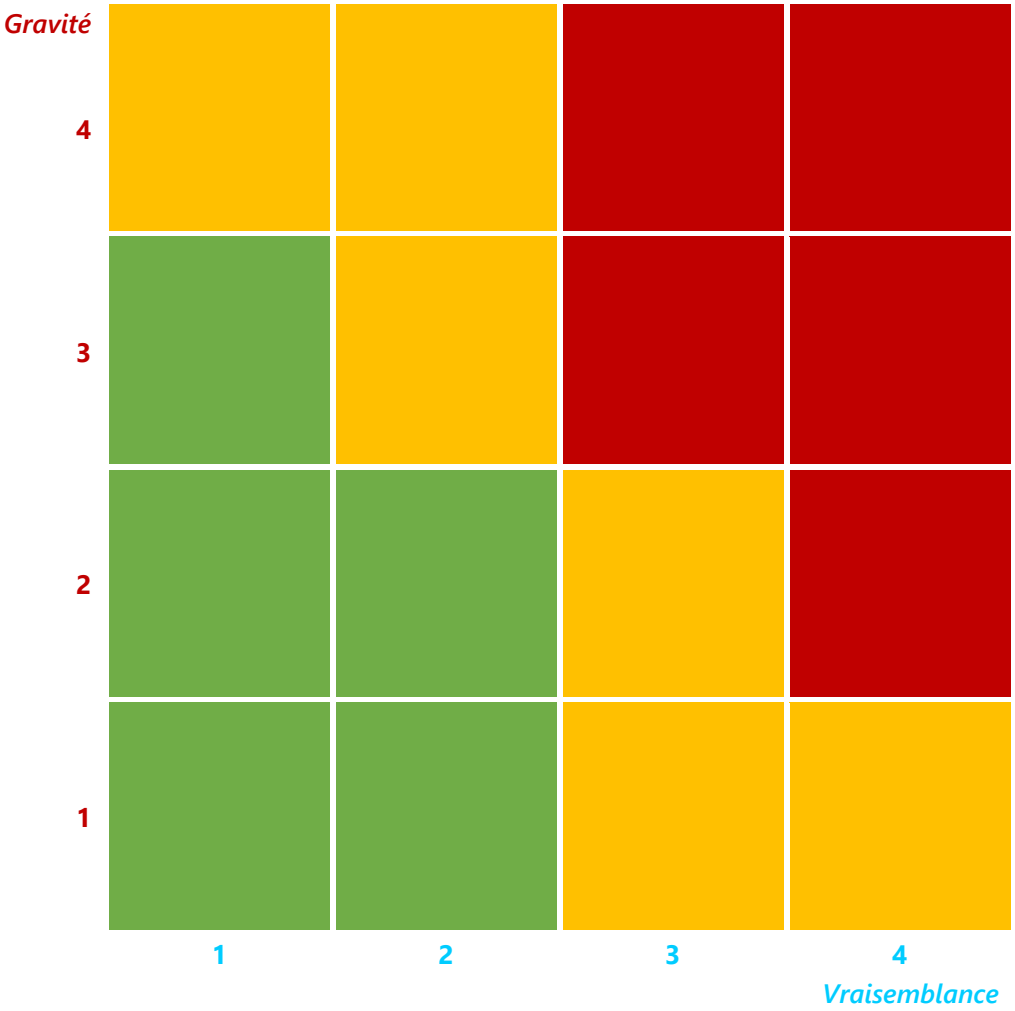
[5] **File Transfer Protocol** : protocole de transfert de fichier qui ne fournit pas de fonction de sécurité particulière
[6] **Single Sign On** : dispositif de centralisation de l'authentification permettant aux utilisateurs grâce à un moyen unique d'authentification, d'accéder à un ensemble de ressources (serveurs, applications, fichiers, etc.)

SGTIN – Élaborer des scénarios opérationnels

Scénario stratégique :	**Chemin d'attaque :**	**Gravité :**

CONNAITRE	RENTRER	TROUVER	EXPLOITER

SGTIN – Réaliser une synthèse des risques



SGTIN – Définir le plan de traitement du risque

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficulté de mise en œuvre	Coût / Complexité	Charge estimée	Echéance	Priorité	Statut