Formation « EBIOS Risk Manager »

Programme

- Les fondamentaux du management du risque
- Atelier 1 : cadrage et socle de sécurité
- Atelier 2 : sources de risque
- Atelier 3 : scénarios stratégiques
- Atelier 4 : scénarios opérationnels
- Atelier 5 : traitement du risque
- **Étude de cas**

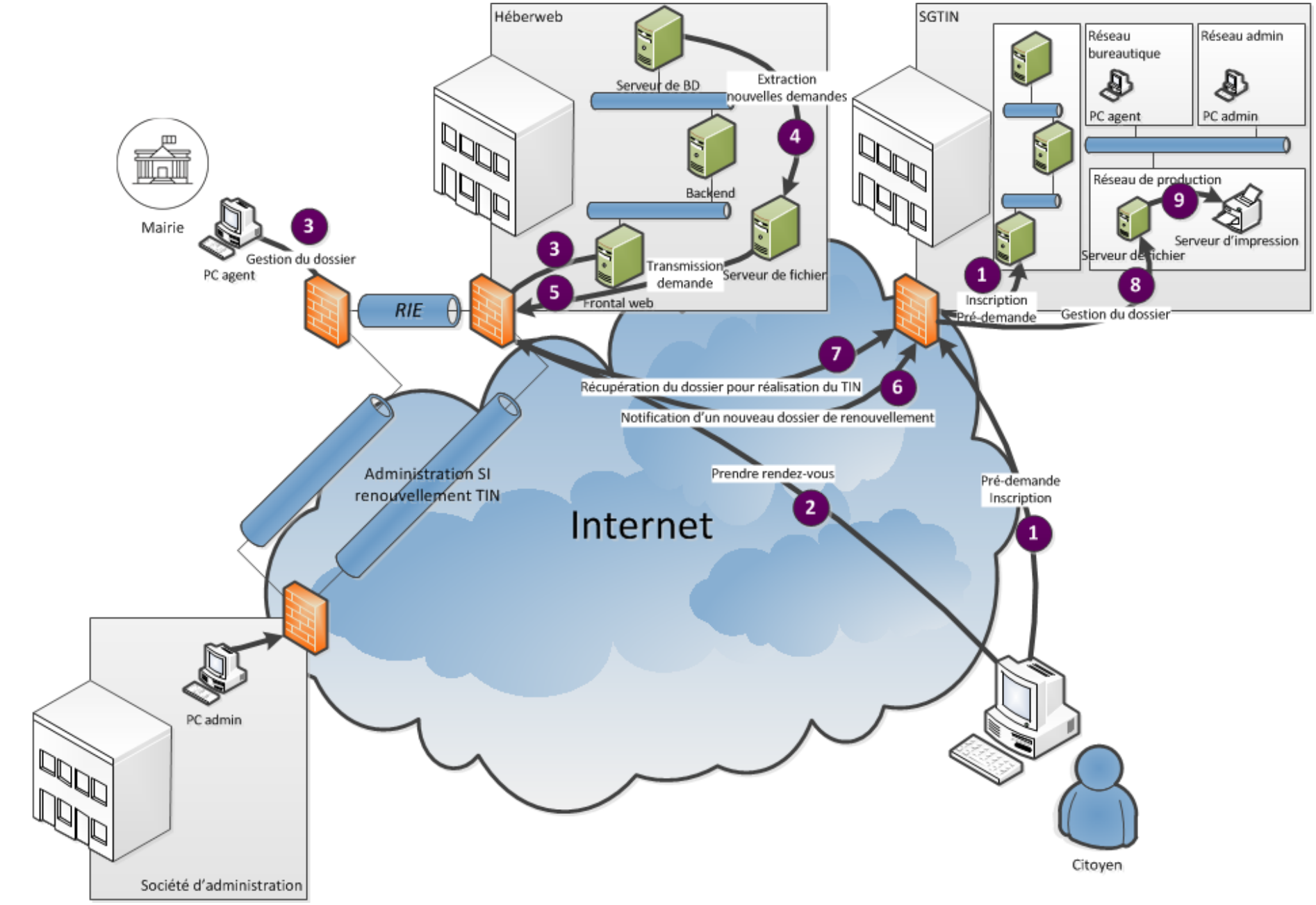
Livret stagiaire
p.37 à 41

Présentation de l'étude de cas

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)**.

L'objectif de l'étude est de **conduire une étude complète des risques sur le SI de renouvellement de TIN et ses interconnexions avec l'extérieur.** Le commanditaire de l'étude est la Société de Gestion des Titres d'Identité Numérique (SGTIN).

Vous pouvez désormais prendre connaissance du dossier d'étude de cas fourni.


Héberweb
Serveur de BD
Extraction nouvelles demandes
Backend
Transmission demande
Serveur de fichier
Frontal web
SGTIN
Réseau bureautique
PC agent
Réseau admin
PC admin
Réseau de production
Serveur d'impression
Serveur de fichier
Mairie
PC agent
Gestion du dossier
RIE
Inscription Pré-demande
Gestion du dossier
Récupération du dossier pour réalisation du TIN
Notification d'un nouveau dossier de renouvellement
Prendre rendez-vous
Pré-demande Inscription
Administration SI renouvellement TIN
Internet
PC admin
Société d'administration
Citoyen

A1

Définir le périmètre métier et technique

Livret stagiaire
p.42

Fiche méthode N°1

MISSION	RENOUVELER DES TITRES D'IDENTITÉ NUMÉRIQUE								
NOM DE LA VALEUR MÉTIER	Gestion des pré-demandes		Gestion des demandes de renouvellement de TIN		Impression des TIN		Distribution des TIN	Informations des citoyens	
NATURE DE LA VALEUR MÉTIER	Processus		Processus		Processus		Processus	Information	
ENTITÉ RESPONSABLE	SGTIN (responsable de la valeur métier même si elle peut déléguer l'exécution des processus à un prestataire)								
NOM DU/DES BIENS SUPPORTS ASSOCIÉS	SI de pré-demande	Locaux	SI de renouvellement de TIN	Locaux	SI d'impression des TIN	Locaux	Coursier	SI de la mairie	SI d'impression des TIN
ENTITÉ OU PERSONNE RESPONSABLE	SGTIN	SGTIN et Mairie	SGTIN	Mairie et Hébergeur	SGTIN	SGTIN	Société d'acheminement des TIN	Mairie	SGTIN

A1

Échelle de gravité validée pour le projet

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)

A1

Catégories d'impact (1/2)

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 oeuvre 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 oeuvre 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.

A1

Catégories d'impact (2/2)

Impact	Exemples (listes non exhaustives)
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.

A1

Identifier les événements redoutés

Livret stagiaire
p.43 à 45

Fiche méthode N°3

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	IMPACTS	GRAVITÉ	COMMENTAIRES / JUSTIFICATION
Impression des TIN	Les informations imprimées sur le TIN ne correspondent pas aux informations initialement données par le citoyen (sabotage)	• Impact financier lié au coût de réimpression du TIN • Impact juridique lié à l'implication de la SGTIN dans les procès pour création de fausses identités	4	• Usurpation d'identité • Fraude (création de faux TIN)
Distribution des TIN	Vol du TIN durant son acheminement à la mairie ayant fait la demande	• Impact juridique (RGPD) • Impact financier lié au coût de renouvellement de TIN	4	• Usurpation d'identité
Informations des citoyens	Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	• Impact juridique (RGPD) • Impact d'image	4	• Usurpation d'identité
Gestion des demandes de renouvellement de TIN	Le service permettant à un agent de mairie de faire une demande de renouvellement de TIN est indisponible	• Impact d'image • Impact financier lié au coût d'investigation et de retour à la normale	3	Pas d'existence de solution de contournement, impossibilité de réaliser la mission pendant la durée d'indisponibilité
Gestion des demandes de renouvellement de TIN	Le service de notification de renouvellement de TIN n'est pas accessible aux utilisateurs	• Impact d'image lié au délai d'obtention du TIN • Impact financier lié au coût d'investigation et de retour à la normale	2	Existence d'une solution de contournement avec une dégradation des performances (la mairie peut contacter par téléphone ou mail le citoyen pour le notifier)
Gestion des pré-demandes	Le service permettant de réaliser une pré-demande par internet auprès de la SGTIN est indisponible	• Impact d'image • Impact financier lié au coût d'investigation et de retour à la normale	1	Existence d'une solution de contournement (possibilité de renseigner les informations directement à la mairie)

A1

Déterminer le socle de sécurité

Livret stagiaire
p.46

TYPE DE RÉFÉRENTIEL	NOM DU RÉFÉRENTIEL	COMMENTAIRES
Cadre règlementaire	Référentiel général de sécurité (RGS)	Vise à renforcer la confiance des usagers dans les services électroniques proposés par les autorités administratives
Norme	Annexe A de l'ISO 27001	Mesures de référence en vue de l'établissement, de la mise en oeuvre, de la tenue à jour d'un système de management de la sécurité de l'information
Politique de sécurité	PSSI de l'organisation	Politique de sécurité des SI de l'organisation, qui doit être conforme à celle de l'État (PSSIE)
Bonnes pratiques	Guide d'hygiène informatique	Guide de l'ANSSI visant à renforcer la sécurité de son système d'information en 42 mesures

Malgré la présence de données à caractère personnel, le règlement RGPD n'est pas mentionné ici car il ne comprend pas une liste de mesures de sécurité à respecter

A2

Méthode d'évaluation de la pertinence des 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**

A2

Évaluer les couples SR/OV et sélectionner les plus pertinents

Livret stagiaire
p.47 et 48

Fiche méthode N°4

SOURCES DE RISQUE	OBJECTIF VISÉ	MOTIVATION	RESSOURCES	PERTINENCE
Organisation de malfaiteurs	Gagner de l'argent en récoltant des informations à caractère personnel en vue de créer des faux TIN	Fortement motivé	Ressources importantes	**Très pertinent**
Espion (rémunéré par une organisation malveillante)	Collecter des données précises sur un citoyen ciblé	Fortement motivé	Ressources importantes	**Très pertinent**
État	Obtenir des faux TIN pour faire circuler des espions sur le territoire	Fortement motivé	Ressources illimitées	**Très pertinent**
Agent malveillant SGTIN	Discréditer ou saboter le service de renouvellement de TIN	Assez motivé	Ressources significatives	**Plutôt pertinent**
Terroriste	Créer un faux TIN pour entrer sur le territoire	Assez motivé	Ressources limitées	**Moyennement pertinent**
Citoyen malhonnête	Créer une fausse identité	Très peu motivé	Ressources limitées	Peu pertinent
Hacker amateur	Tester ses compétences sur un système « grandeur nature »	Peu motivé	Ressources limitées	Peu pertinent

A1 ↔ A2

Lien entre les ER (atelier 1) et les couples SR/OV retenus (atelier 2)

Livret stagiaire
p.49

ER les plus graves

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ
Impression des TIN	Les informations imprimées sur le TIN ne correspondent pas aux informations initialement données par le citoyen (sabotage)
Distribution des TIN	Vol du TIN durant son acheminement à la mairie ayant fait la demande
Informations des citoyens	Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)

SR/OV les plus pertinents

SOURCES DE RISQUE	OBJECTIF VISÉ
Organisation de malfaiteurs	Gagner de l'argent en récoltant des informations à caractère personnel en vue de créer des faux TIN
Espion (rémunéré par une organisation malveillante)	Collecter des données précises sur un citoyen ciblé
État	Obtenir des faux TIN pour faire circuler des espions sur le territoire

A3

Fiche méthode N°5

Construire la cartographie de menace numérique de l'écosystème

Pour chaque partie prenante, évaluer 4 critères :

EXPOSITION

Dépendance
La relation avec cette partie prenante est-elle vitale pour mon activité ?

Pénétration
Dans quelle mesure la partie prenante accède-t-elle à mes ressources internes ?

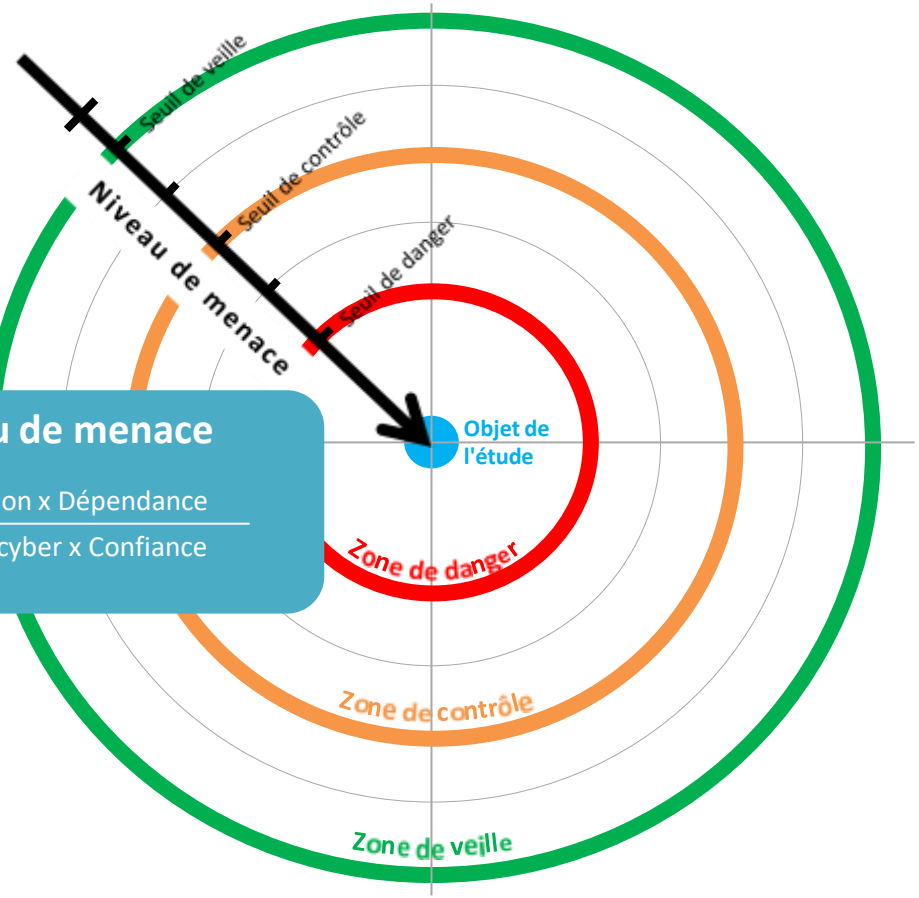
FIABILITE CYBER

Maturité cyber
Quelles sont les capacités de la partie prenante en matière de sécurité ?

Confiance
Est-ce que les intentions ou les intérêts de la partie prenante peuvent m'être contraires ?

Niveau de menace

Pénétration x Dépendance
Maturité cyber x Confiance



A3

Critères de cotation de la menace proposés

Livret stagiaire
p.50 à 52

	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 terminaux utilisateur du système d'information de la SGTIN 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 oeuvre 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.

A3

Evaluer le niveau de menace associé aux parties prenantes de l'écosystème

Livret stagiaire
p.50 à 52

CATÉGORIE	NOM	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFIANCE	NIVEAU DE MENACE
Utilisateur	Citoyen	2	1	1	1	2
Partenaire	Mairie	2	2	1	3	1,3
Partenaire	Autorité Nationale de Gestion des Titres (ANGT)	1	3	1	4	0,75
Prestataire	Société d'administration	3	4	2	3	2
Prestataire	Hébergeur (Héberweb)	3	4	3	3	1,3
Prestataire	Société d'acheminement des TIN	3	3	1	1	9

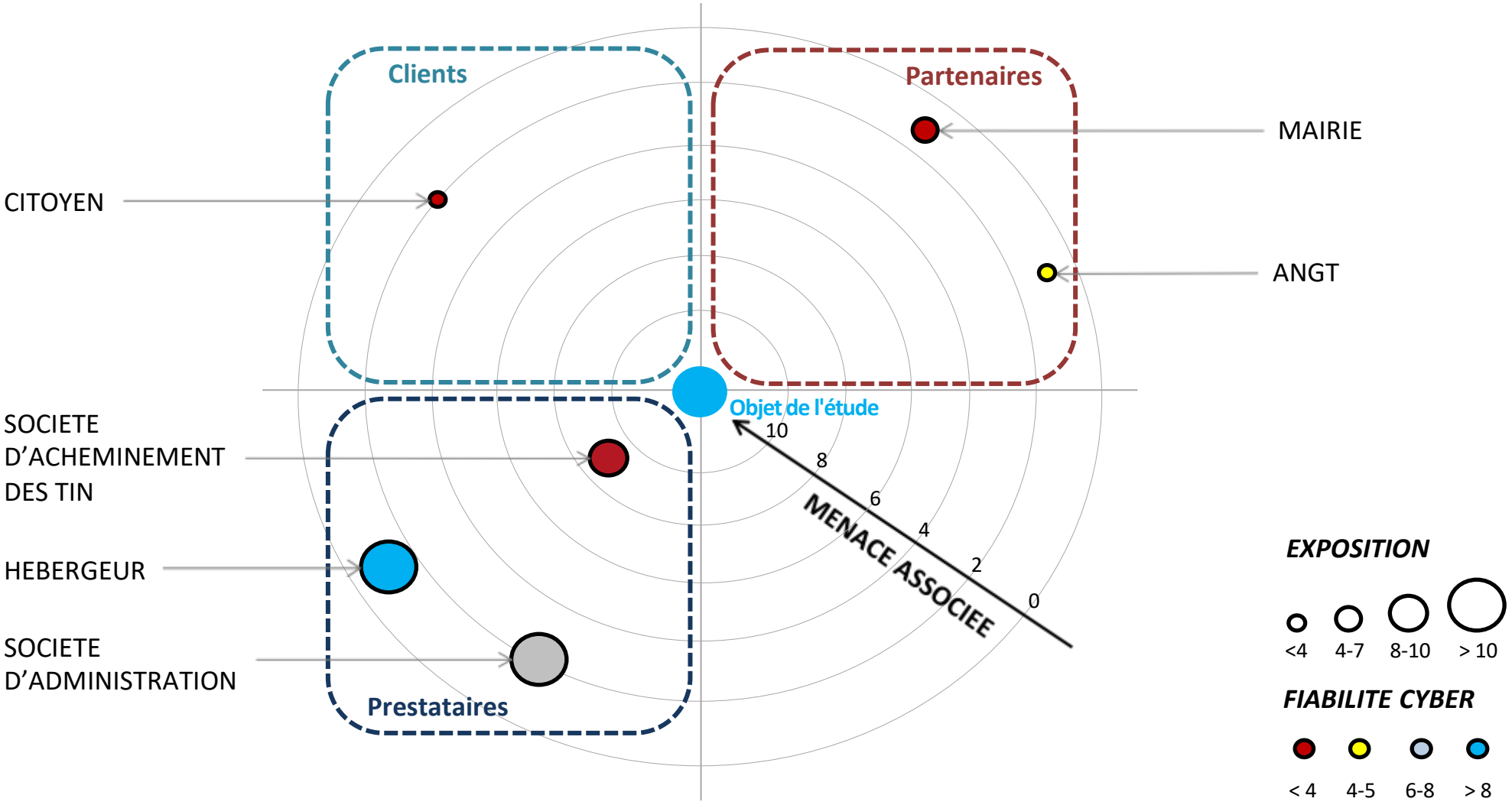
EXPOSITION

FIABILITÉ CYBER

A3

Construire la cartographie de menace numérique de l'écosystème

Livret stagiaire
p.50 à 52

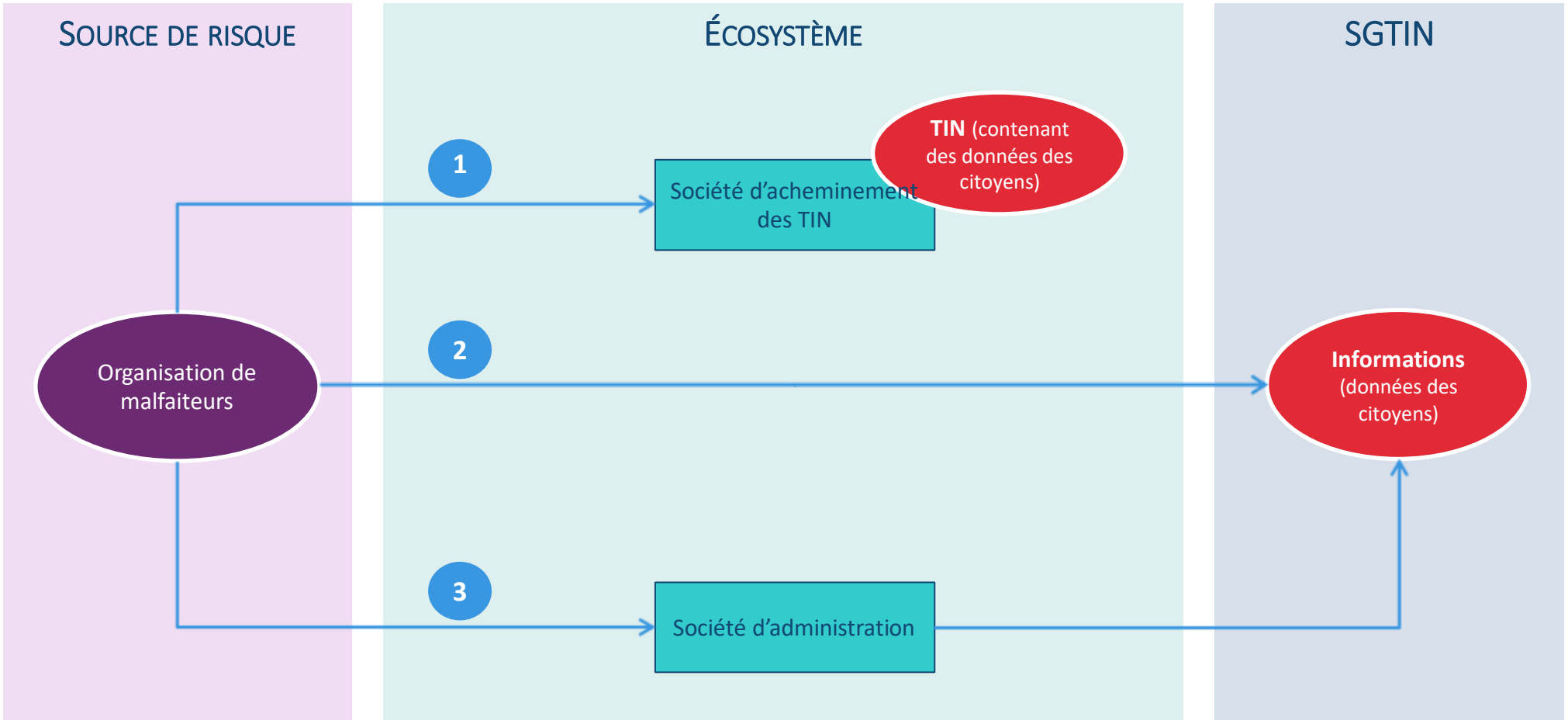


A3

Élaborer des scénarios stratégiques

Livret stagiaire
p.53

A2 **Source de risque :** Organisation de malfaiteurs **Objectif visé :** Collecter des données à caractère personnel

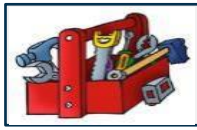


Gravité : 4

A4

Élaborer les scénarios opérationnels

Livret stagiaire
p.54 à 57



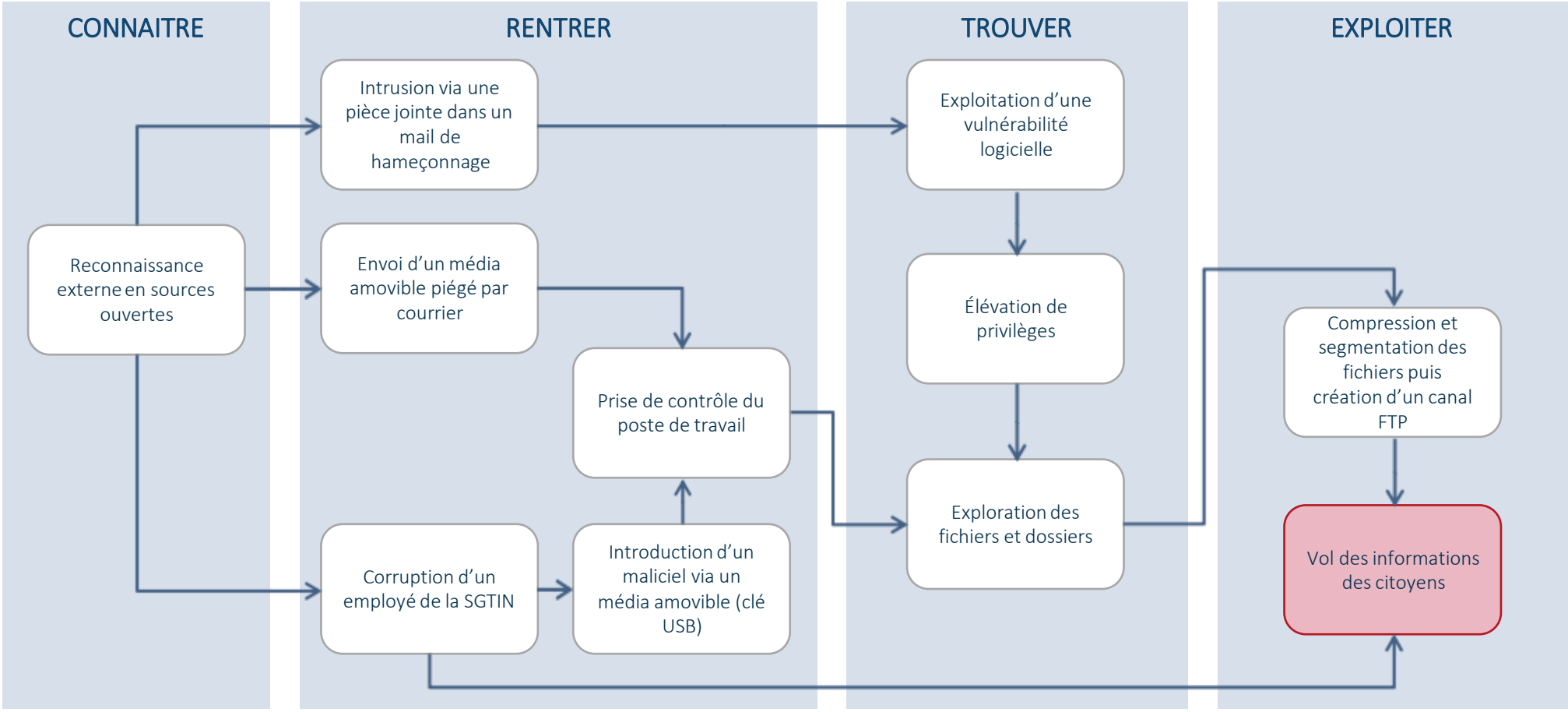
Fiche méthode N°7

A3

Scénario stratégique : Organisation de malfaiteurs qui veut voler des données personnelles

Chemin d'attaque : n°2 – « attaque directe »

Gravité : 4



Échelle de vraisemblance validée pour le projet

ÉCHELLE	DÉFINITION
V4 – QUASI CERTAIN	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
V1 – PEU VRAISEMBLABLE	La source de risque a peu de chances d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible

Livret stagiaire
p.58

Réaliser une synthèse des scénarios de risque