



EBIOS Risk Manager

Livret stagiaire



VERSIONS

Version	Action	Éditeur	État
24/06/2025	Création du document, sur la base de la dernière version de la présentation	Matthieu GRALL	Document de travail
01/07/2025	Intégration de l'étude de cas, sur la base du kit de l'ANSSI	Matthieu GRALL	Amélioration continue

DOCUMENTS DE RÉFÉRENCE

- **Kit de formation EBIOS *Risk Manager* de 2024** (ANSSI)
- **Kit de formation EBIOS *Risk Manager* de 2025** (Matthieu GRALL)

RESSOURCES UTILISÉES

- **Page de garde** : Grid, par Magic Creative, de PIXABAY
- **Logo** : Matthieu GRALL
- **Illustrations liées à EBIOS *Risk Manager*** : kit de formation de l'ANSSI



OBJET DU DOCUMENT

Le kit de formation à EBIOS *Risk Manager*, la méthode de gestion des risques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), comprend :

- une **présentation** servant de fil directeur à la formation ;
- le **livret stagiaire**, utilisable par les personnes formées pour réaliser les exercices ;
- le **livret formateur**, utilisable par le formateur pour gérer sa formation.

Le présent document constitue le livret stagiaire.

SOMMAIRE

1	EXERCICES	4
1.1	CONTEXTE DES EXERCICES	4
1.2	ÉTABLIR LE CONTEXTE.....	5
1.2.1	<i>Vos notes.....</i>	5
1.2.2	<i>Décrivez l'objet de l'étude : valeurs métier et biens supports.....</i>	6
1.2.3	<i>Décrivez l'écosystème de l'objet de l'étude : parties prenantes.....</i>	6
1.2.4	<i>Et chez-vous alors ? Choisissez et illustrez un objet d'étude</i>	7
1.3	APPRÉCIER LES RISQUES – APPROCHE PAR CONFORMITÉ.....	8
1.3.1	<i>Vos notes.....</i>	8
1.3.2	<i>Et chez-vous alors ? Choisissez et évaluez un socle de règles</i>	9
1.4	APPRÉCIER LES RISQUES – APPROCHE PAR SCÉNARIOS	10
1.4.1	<i>Vos notes.....</i>	10
1.4.2	<i>Analysez et estimez les principaux événements redoutés</i>	11
1.4.3	<i>Analysez et estimez les principales sources de risques.....</i>	12
1.4.4	<i>Estimez les critères et calculez la dangerosité des parties prenantes</i>	13
1.4.5	<i>Analysez les chemins d'attaques de la source de risques.....</i>	15
1.4.6	<i>Appréciez le chemin d'attaque</i>	16
1.4.7	<i>Et chez-vous alors ? Appréciez un scénario de risque.....</i>	17
1.5	TRAITER LES RISQUES.....	18
1.5.1	<i>Vos notes.....</i>	18
1.5.2	<i>Et chez-vous alors ? Planifiez la mise en œuvre d'une mesure</i>	19
2	ÉTUDE DE CAS COMPLÈTE.....	20
2.1	CONTEXTE DE L'ÉTUDE DE CAS	20
2.2	DOSSIER FOURNI	21
2.2.1	<i>Informations recueillies.....</i>	21
2.2.2	<i>Conclusions d'un audit</i>	26
2.3	DÉFINIR LE PÉRIMÈTRE MÉTIER ET TECHNIQUE.....	28
2.4	IDENTIFIER LES ÉVÉNEMENTS REDOUTÉS (ER)	29
2.5	ÉVALUER LES COUPLES SOURCES DE RISQUES / OBJECTIFS VISÉS (SR/OV)	32
2.6	ÉTABLIR LE LIEN ENTRE LES ÉVÉNEMENTS REDOUTÉS ET LES COUPLES SR/OV	33
2.7	CONSTRUIRE LA CARTOGRAPHIE DE L'ÉCOSYSTÈME	34
2.8	ÉLABORER DES SCÉNARIOS STRATÉGIQUES	36
2.9	ÉLABORER DES SCÉNARIOS OPÉRATIONNELS	37
2.10	RÉALISER UNE SYNTHÈSE DES RISQUES.....	40
2.11	DÉFINIR LE PLAN DE TRAITEMENT DES RISQUES.....	41



1 EXERCICES

1.1 Contexte des exercices

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



1.2 Établir le contexte

1.2.1 VOS NOTES



1.2.2 DÉCRIREZ L'OBJET DE L'ÉTUDE : VALEURS MÉTIER ET BIENS SUPPORTS

Valeurs métier	Description Quelles activités ? Quelles données ?	Biens supports Sur quoi les valeurs métier reposent-elles ?
Recherche & développement (R&D)		
Fabriquer des vaccins		
Traçabilité et contrôle		

1.2.3 DÉCRIREZ L'ÉCOSYSTÈME DE L'OBJET DE L'ÉTUDE : PARTIES PRENANTES

Type de parties prenantes	Parties prenantes Quels sont les acteurs de l'écosystème de l'objet d'étude ?
Clients	
Partenaires	
Sous-traitants	
Fournisseurs	



1.2.4 ET CHEZ-VOUS ALORS ? CHOISISSEZ ET ILLUSTRER UN OBJET D'ÉTUDE

Consignes	Réponses
Choisissez 1 objet d'étude Sur quel sujet que vous connaissez (organisation, produit, service, système, traitement de données, etc.) pourriez-vous mener une étude de risques ?	
Choisissez 1 valeur métier Quelle est l'activité ou la donnée essentielle de l'objet d'étude choisi ?	
Choisissez 1 bien support Sur quoi la valeur métier choisie repose-t-elle principalement (système, matériel, logiciel, réseau, personnels, etc.) ?	
Choisissez 1 partie prenante Quel est le principal acteur de l'écosystème (client, partenaire, sous-traitant, fournisseur, etc.) concerné par la valeur métier choisie ?	



1.3 Apprécier les risques – Approche par conformité

1.3.1 VOS NOTES



1.3.2 ET CHEZ-VOUS ALORS ? CHOISISSEZ ET ÉVALUEZ UN SOCLE DE RÈGLES

Consignes	Réponses
Choisissez 1 socle de règles Quel est le principal référentiel qui définit les règles que l'objet d'étude choisi doit respecter ?	
Choisissez 1 méthode d'évaluation du socle Quelle est/serait la manière la plus efficace de vérifier que le socle choisi est respecté (déclaratif global ou détaillé, contrôle interne, audit, etc.) ?	
Choisissez 1 règle du socle Quelle est la règle la plus importante du socle choisi ?	
Évaluez le respect de la règle Selon vous, la règle choisie est-elle/sera-t-elle respectée (oui totalement, généralement oui, généralement non, non pas du tout) ?	
Déterminer 1 mesure complémentaire Si la règle choisie n'est pas parfaitement respectée, quelle est la principale action qui permettrait d'améliorer la situation ?	



1.4 Apprécier les risques – Approche par scénarios

1.4.1 VOS NOTES



1.4.2 ANALYSEZ ET ESTIMEZ LES PRINCIPAUX ÉVÉNEMENTS REDOUTÉS

Gravité	Description
1. Mineure	Aucune conséquence opérationnelle 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)
2. Significative	Dégradation des performances de l'activité sans conséquence sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)
3. Importante	Forte dégradation des performances de l'activité, avec d'éventuelles conséquences significatives sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé)
4. Critique	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuelles conséquences graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée)

Valeur métier	Événements redoutés Quelles sont les atteintes à la disponibilité, à l'intégrité et à la confidentialité possibles ?	Conséquences potentielles Quels seraient les impacts (sur l'organisation, les personnes concernées, etc.) si l'événement redouté survenait ?	Gravité
R&D			
Fabriquer des vaccins			
Traçabilité et contrôle			



1.4.3 ANALYSEZ ET ESTIMEZ LES PRINCIPALES SOURCES DE RISQUES

		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

Sources de risques Quels sont les attaquants à considérer dans le cadre de l'objet d'étude ?	Objectifs visés Quels sont les objectifs de ces attaquants ?	Motivation	Ressources	Pertinence



1.4.4 ESTIMEZ LES CRITÈRES ET CALCULEZ LA DANGEROUSITÉ DES PARTIES PRENANTES

Niveau	Dépendance	Pénétration	Maturité cyber	Confiance
1. Minimale	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. Faible	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. Importante	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. Maximale	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, <i>switchs</i> , 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.



Catégorie	Nom	Dépendance	Pénétration	Maturité cyber	Confiance	Dangerosité*
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 (chaîne de production)					
Prestataire	F3 - Prestataire informatique					

* Dangerosité = (Pénétration x Dépendance) / (Maturité cyber x Confiance)

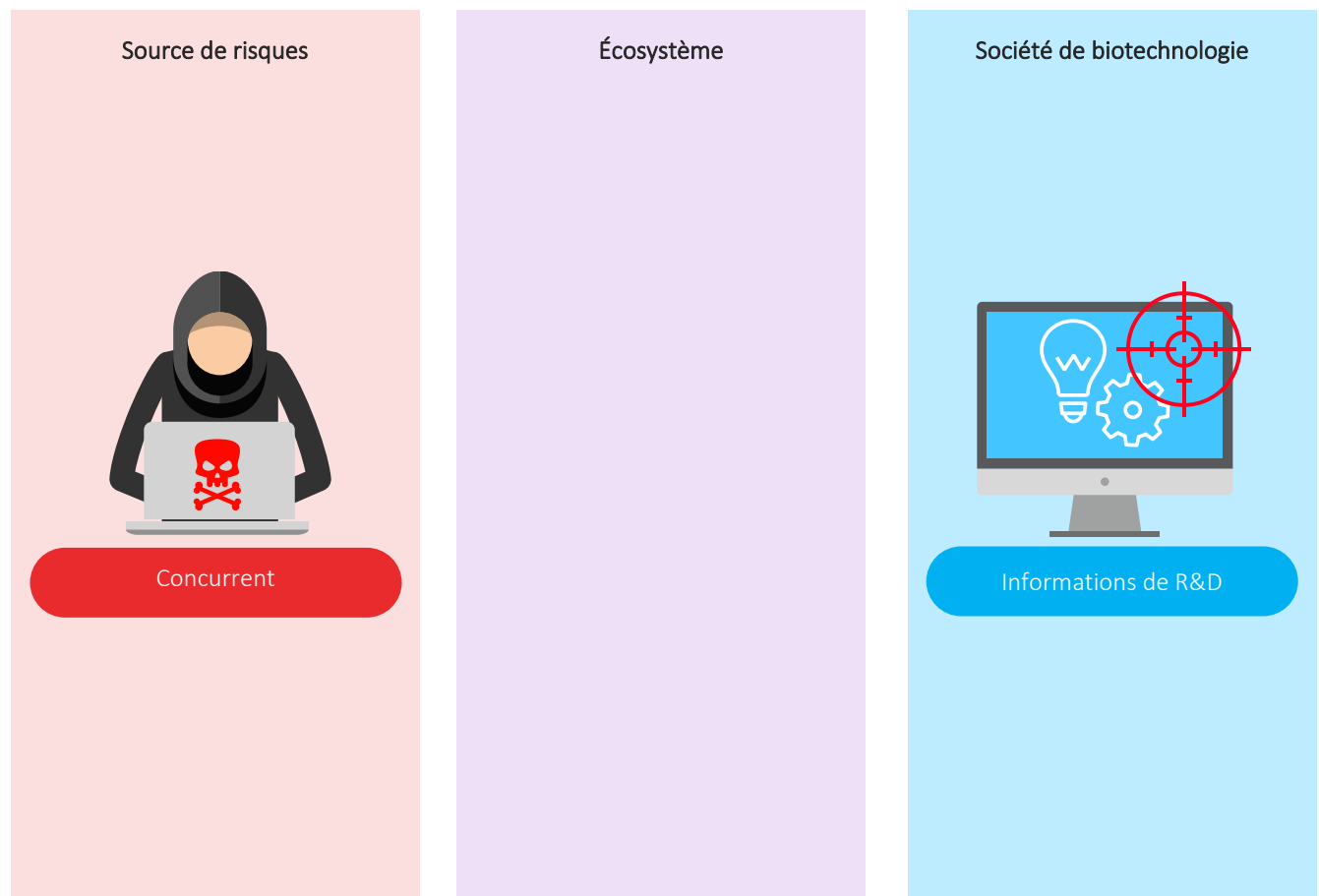


1.4.5 ANALYSEZ LES CHEMINS D'ATTAQUES DE LA SOURCE DE RISQUES

Source de risques : Concurrent

Objectif visé : Voler des informations

Événement redouté : Fuite des informations d'études et recherches de l'entreprise





1.4.6 APPRÉCIEZ LE CHEMIN D'ATTAQUE

Vraisemblance	Description
4. Maximale	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés OU un tel scénario s'est déjà produit au sein de l'organisme (historique d'incidents)
3. Importante	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
2. Faible	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
1. Minimale	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

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

Chemin d'attaque : n°1

Gravité : 3

Connaître	Rentrer	Trouver	Exploiter

**1.4.7 ET CHEZ-VOUS ALORS ? APPRÉCIEZ UN SCÉNARIO DE RISQUE**

Consignes	Réponses
Appréciez 1 événement redouté représentatif Quel est l'événement le plus à craindre (disparition, modification ou accès) sur la valeur métier choisie ? Quelles conséquences ? Quelle gravité ?	
Appréciez 1 source de risques pertinente Quel exemple d'attaquant serait susceptible d'engendrer l'événement redouté formulé ? Quelles motivation, ressources et pertinence ?	
Choisissez 1 scénario stratégique La source de risques choisie attaquerait-elle plus vraisemblablement directement le système ou via un client, fournisseur ou partenaire ?	
Choisissez 1 scénario opérationnel Quelle séquence d'actions (connaître, trouver, rentrer, exploiter) serait nécessaire pour réaliser le scénario stratégique choisi ? quelle vraisemblance ?	
Déterminer 1 mesure complémentaire Quelle serait la mesure la plus efficace pour traiter le risque ainsi apprécié ? sur quel composant du risque agirait-elle ?	



1.5 Traiter les risques

1.5.1 VOS NOTES

**1.5.2 ET CHEZ-VOUS ALORS ? PLANIFIEZ LA MISE EN ŒUVRE D'UNE MESURE**

Consignes	Réponses
Choisissez 1 des mesures complémentaires précédemment déterminée Quelle serait la mesure à mettre en œuvre en premier ?	
Identifiez le composant du risque sur lequel agit la mesure choisie Que permettent-elles de traiter (
Identifiez l'option de traitement À quelle option de traitement des risques la mesure choisie correspond-elle (réduction, refus, partage, prise du risque) ?	
Identifiez les gains potentiels En quoi la mesure choisie est-elle importante ? Agit-elle sur la gravité ou la vraisemblance ? Beaucoup ? D'autres apports ?	
Identifiez les difficultés potentielles La mesure choisie serait-elle compliquée à mettre en œuvre, lourde en charges, chère à l'acquisition ou à maintenir ? D'autres difficultés prévisibles ?	
Planifiez sa mise en œuvre Qui pourrait être chargé de la mise en œuvre de la mesure choisie ? Dans quels délais ?	

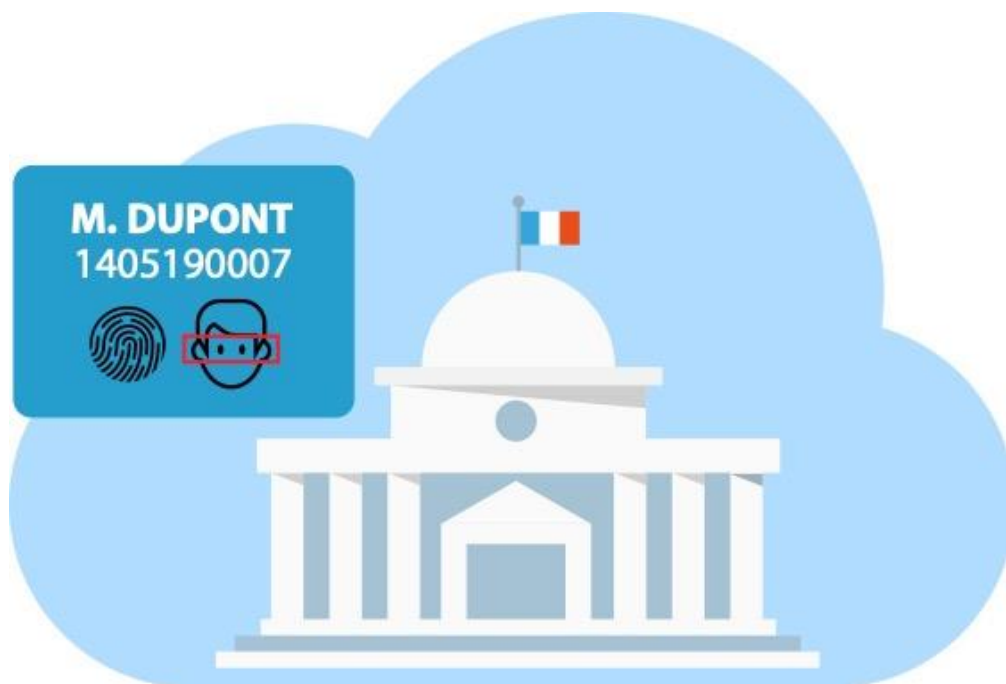
2 ÉTUDE DE CAS COMPLÈTE

2.1 Contexte de l'étude de cas

SGTIN : renouvellement des titres d'identité numérique

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).





2.2 Dossier fourni

2.2.1 INFORMATIONS RECUEILLIES

2.2.1.1 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.

2.2.1.2 Contexte

2.2.1.2.1 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.

2.2.1.2.2 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.

2.2.1.3 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.

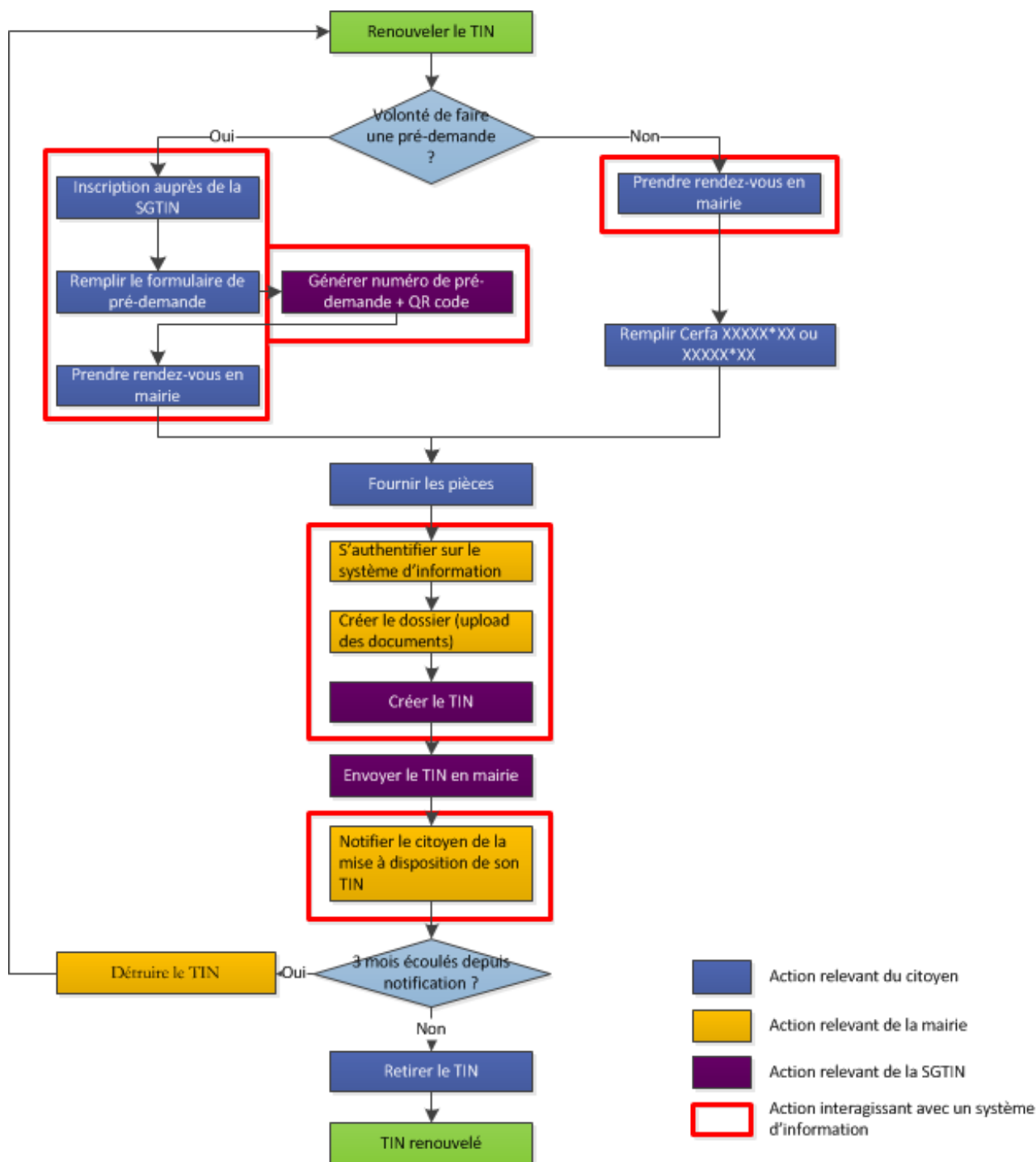


FIGURE 1 : DIAGRAMME DE FLUX DE LA DÉMARCHE DE RENOUVELLEMENT DE TITRES D'IDENTITÉ NUMÉRIQUE

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.



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

2.2.1.4.1 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.

2.2.1.4.2 Les systèmes d'information en présence

À 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 :

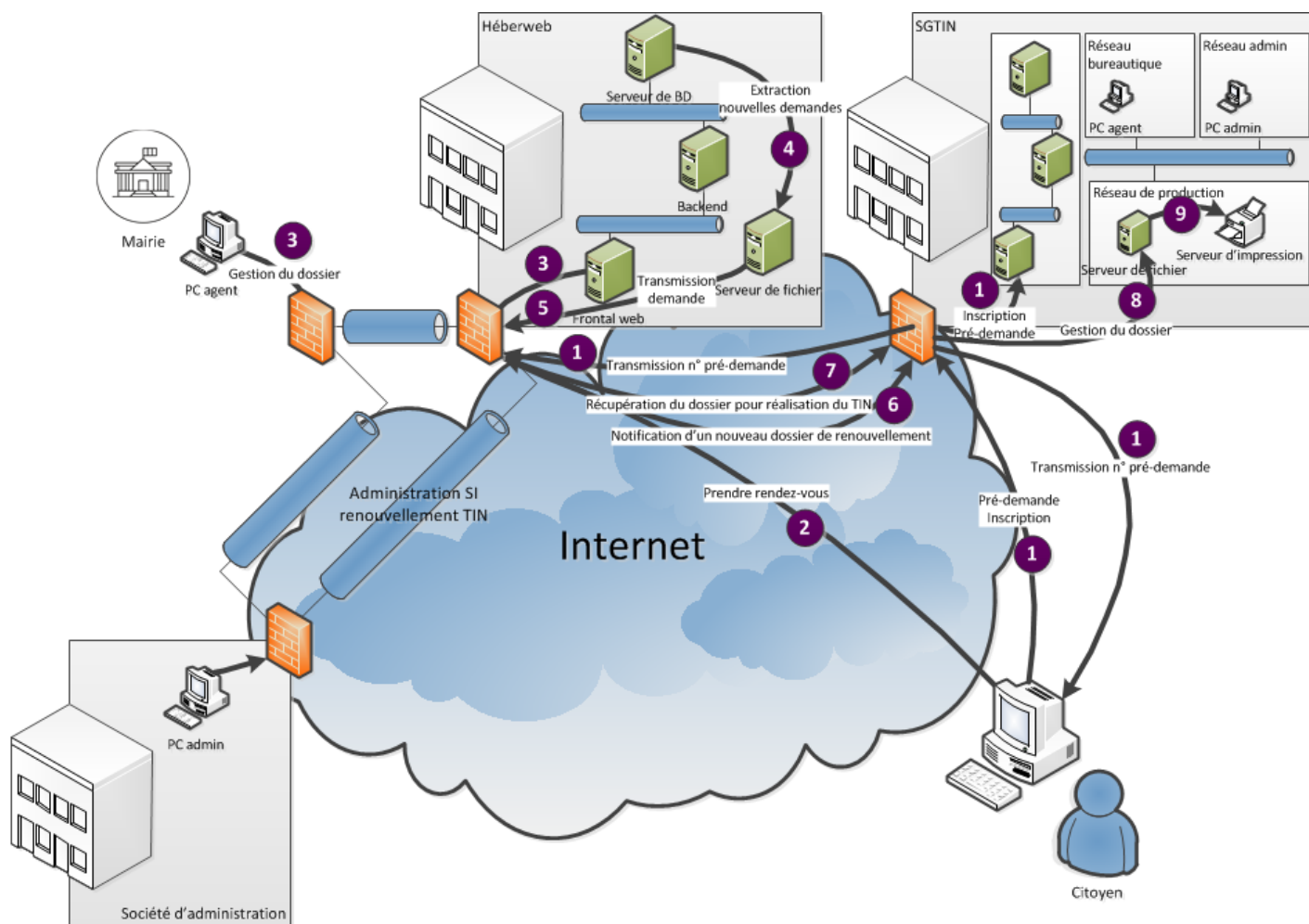


FIGURE 2 : SCHÉMA D'INFRASTRUCTURE RÉSEAU



2.2.2 CONCLUSIONS D'UN AUDIT

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

2.2.2.1 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).

2.2.2.2 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,
- 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

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.

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)



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.

2.2.2.3 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.

2.2.2.4 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 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.

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

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.)



2.3 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 en charge de la mise en œuvre					



2.4 Identifier les événements redoutés (ER)

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	
<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/perde 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 prématurée 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'utilisateurs.

FIGURE 4 : CATÉGORIES D'IMPACTS PROPOSÉES DANS EBIOS RISK MANAGER



Valeur métier	Évènement redouté	Conséquences (« impacts »)	Gravité	Commentaires / Justification



2.5 Évaluer les couples sources de risques / objectifs visés (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

Source de risques	Objectif visé	Motivation	Ressources	Pertinence



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

SR/OV les plus pertinents		ER les plus graves	
Source de risques	Objectif visé	Événement redouté	Valeur métier

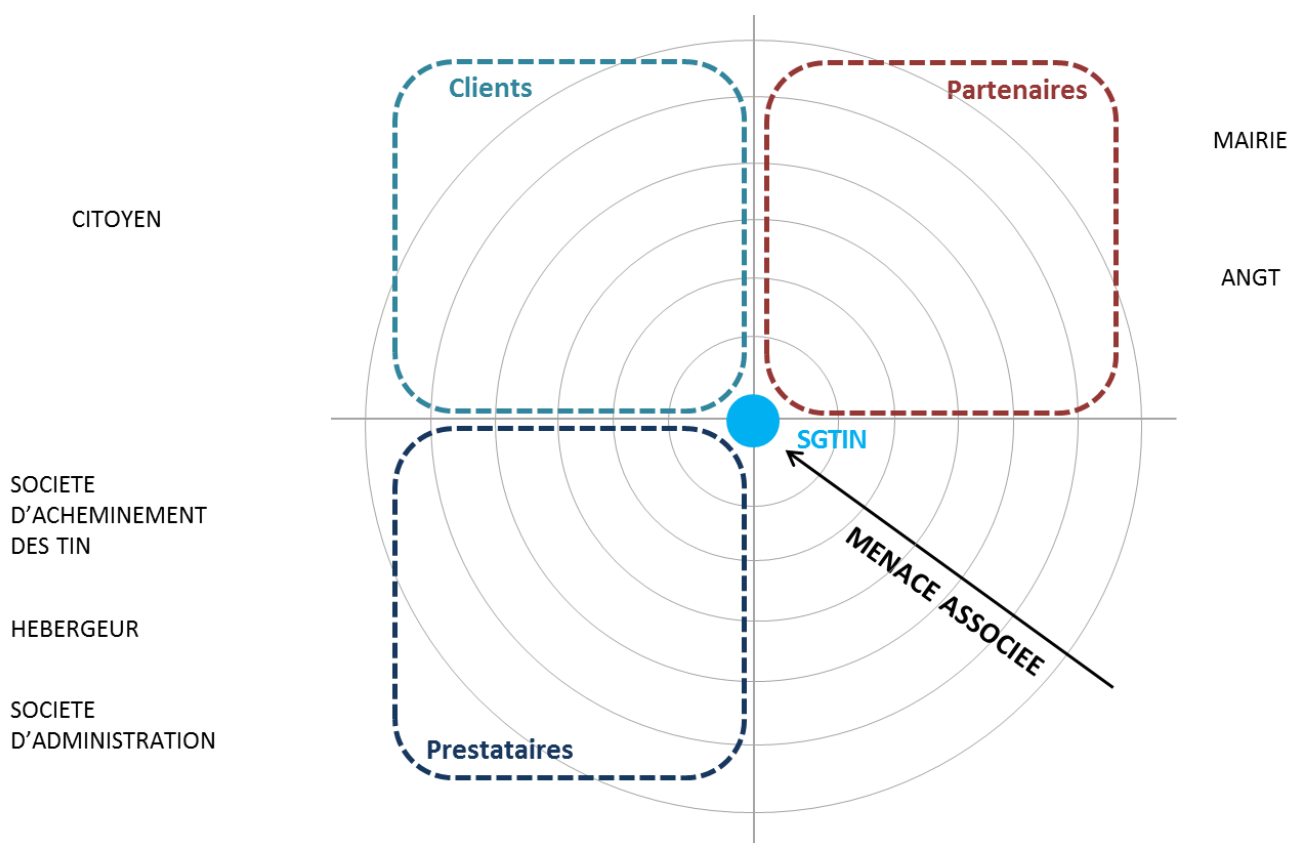


2.7 Construire la cartographie de l'écosystème

	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	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)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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	Partie prenante	Dépendance	Pénétration	Maturité cyber	Confiance	Dangerosité



2.8 Élaborer des scénarios stratégiques

Sources de risque

Écosystème

SGTIN



2.9 Élaborer des scénarios opérationnels

Scénario stratégique	Chemin d'attaque	Gravité

Connaitre

Rentrer

Trouver

Exploiter



Scénario stratégique	Chemin d'attaque	Gravité

Connaitre

Rentrer

Trouver

Exploiter



Scénario stratégique	Chemin d'attaque	Gravité

Connaitre

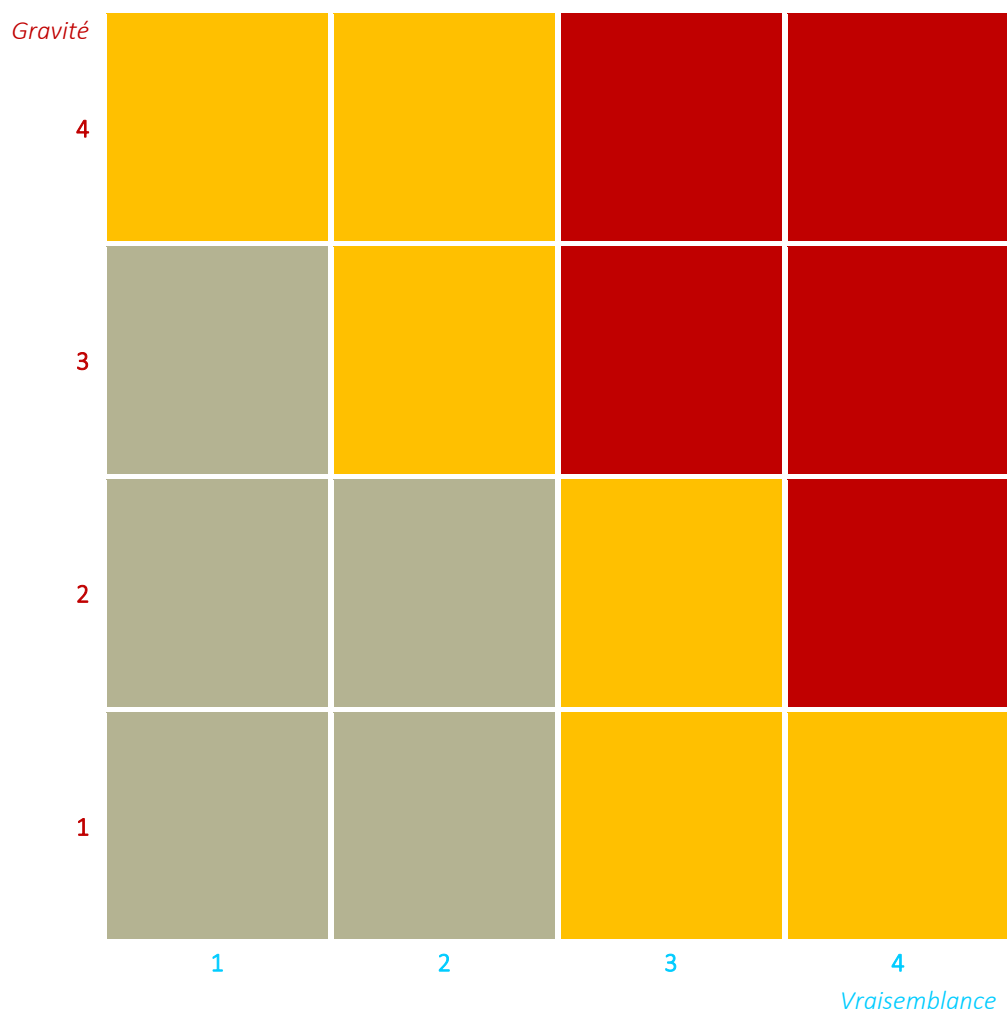
Rentrer

Trouver

Exploiter



2.10 Réaliser une synthèse des risques





2.11 Définir le plan de traitement des risques

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficulté de mise en œuvre	Coût / Complexité	Échéance	Statut