PARCOURS DE CYBERSECURITÉ

—

Déploiement des packs initiaux
Guide à destination des prestataires terrain

———

ANSSI

Règles de diffusion du présent document

Une notice explicative construite suite à une phase d'expérimentation et visant à guider les prestataires terrain

Pourquoi une notice explicative ?

- Ce document a pour but de **guider les prestataires terrain** dans le déploiement d'un pack initial et/ou de packs relais auprès des bénéficiaires du volet cyber de France Relance.
- Il a été construit de manière pédagogique afin d'expliciter à la fois **les objectifs et le déroulement de chaque étape du Parcours de cybersécurité.**
- Il est le fruit d'une première phase d'expérimentation, qui a permis de définir les processus et de construire l'intégralité des livrables afin que les prestataires puissent se **focaliser sur le fond et l'analyse dans le cadre de leurs travaux.**

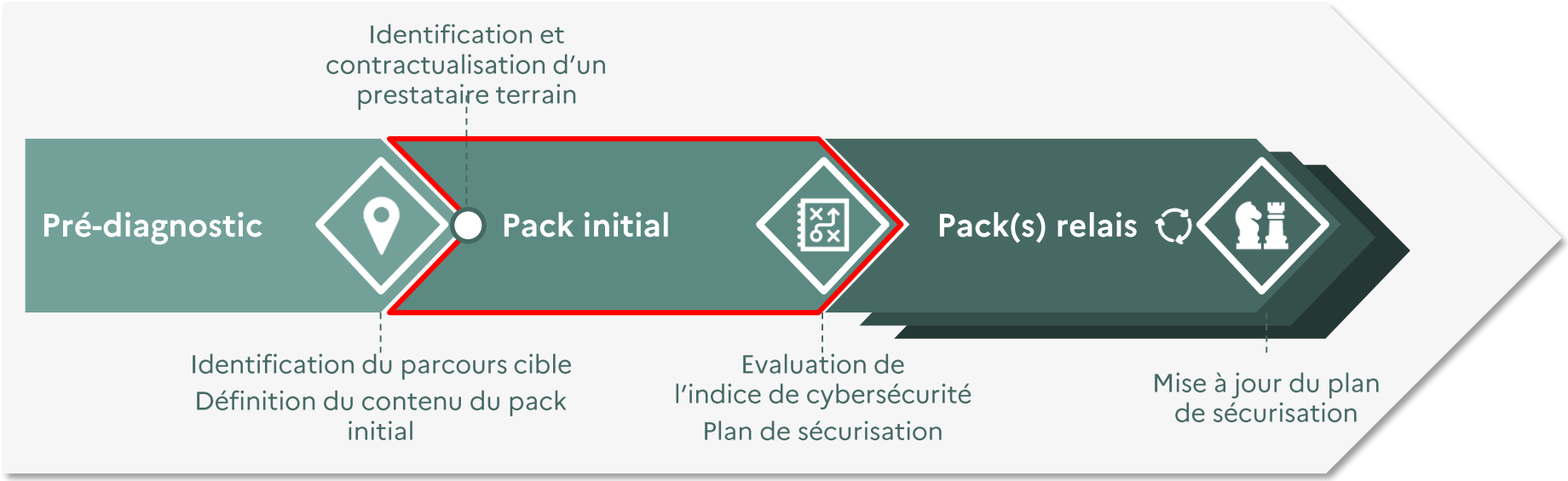
Comment s'en servir ?

- Il est recommandé de consulter l'intégralité de cette notice en amont de la démarche dans le but d'en avoir **une compréhension globale**, puis de s'y référer à chacune des étapes, afin de vérifier qu'elles sont correctement mises en œuvre.
- Si, malgré l'exhaustivité des consignes qui vont suivre, certaines zones d'ombre subsistent, les prestataires terrain peuvent se référer **à leur prestataire accompagnateur** qui les accompagne ainsi que le bénéficiaire durant l'ensemble de la **démarche.**

2

Sommaire

Un dispositif d'accompagnement structuré en trois phases dont le pack initial est le pivot



Le pack initial répond à plusieurs objectifs :

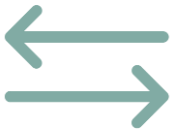
- Formaliser un plan de sécurisation garantissant l'existence de **cibles claires, pertinentes et cohérentes à court et moyen terme**
- Permettre à un prestataire terrain de **maîtriser le contexte et l'existant** d'un bénéficiaire et d'instaurer une **relation de confiance avec lui**, qui pourra notamment se prolonger lors des **packs relais**
- Présenter aux **équipes dirigeantes** du bénéficiaire une synthèse des travaux réalisés ainsi que des éléments de sensibilisation afin de les **convaincre de la nécessité de mettre en œuvre** ce plan de sécurisation et **d'en soutenir** (par des communications ainsi que des arbitrages budgétaires) le déploiement.
- Déterminer de façon argumentée les travaux concrets de sécurisation qui pourront être lancés lors des **packs relais**, **dans les meilleurs délais** suite au pack initial, afin de mettre rapidement le bénéficiaire dans une dynamique d'amélioration de sa sécurité

Une démarche demandant au prestataire terrain d'analyser de façon approfondie le contexte du bénéficiaire en s'appuyant sur un cadre industrialisé

Cadre fourni par le prestataire accompagnateur

- Définition des processus
- Modèles et livrables types

Bénéficiaire



Prestataire terrain

Le pack initial vise à **établir un diagnostic complet permettant de définir un plan de sécurisation personnalisé, adapté au contexte** du bénéficiaire et atteignable en **quelques semestres**, afin d'améliorer de façon **satisfaisante son niveau de sécurité** tout en restant **réaliste vis-à-vis de ses moyens (**humains et budgétaires).

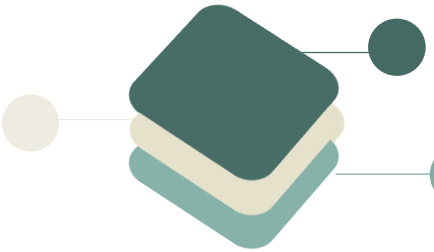
Il est ainsi attendu du prestataire terrain qu'il apporte, dans le cadre du parcours le maximum de valeur ajoutée **sur le fond plutôt que sur la forme** au bénéficiaire**.** La démarche a ainsi été **industrialisée de façon très poussée afin d'éviter aux prestataires terrain de récréer à chaque fois des modèles** de travail et de restitution, permettant de maîtriser les coûts de ces travaux et d'augmenter les ressources utilisées dans le cadre des packs relais.

Cette réflexion de fond se concentrera notamment sur des travaux **d'état des lieux organisationnel et technique** afin d'avoir une **vision claire de la maturité SSI** du bénéficiaire mais également par des travaux de **compréhension du contexte et des enjeux du bénéficiaire** (approche par les risques, priorités métier, projets SI, orientations SSI du bénéficiaire et principales menaces le visant) **afin d'orienter et de prioriser le plan de sécurisation de façon adéquate.**

Ce plan d'action devra trouver un **juste équilibre** entre une cible **ambitieuse** afin d'améliorer durablement le niveau de sécurité du bénéficiaire et une cible estimée **comme réaliste par les équipes SSI, SI et dirigeantes** du bénéficiaire vis-à-vis de **leurs moyens (humains et financiers)** afin de générer une **motivation** dans la mise en œuvre de ce plan de sécurisation qui pourra être **immédiatement exploitée dans le cadre des packs relais**

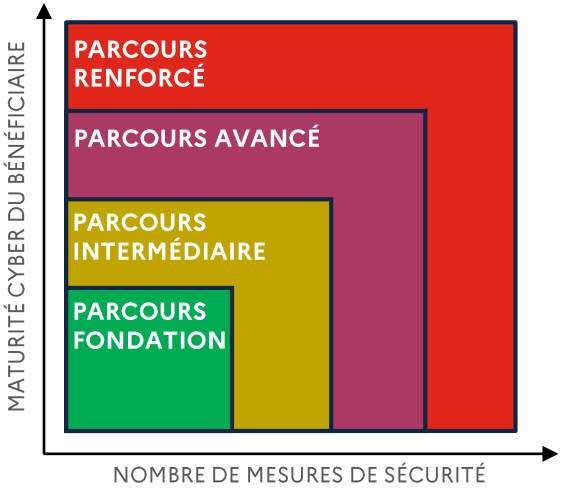
Une démarche s'appuyant sur des parcours de cybersécurité cumulatifs, conçus pour répondre aux enjeux et aux besoins de chaque organisation à travers 120 mesures progressives

☑ Couvre les **mesures d'hygiène de l'ANSSI**

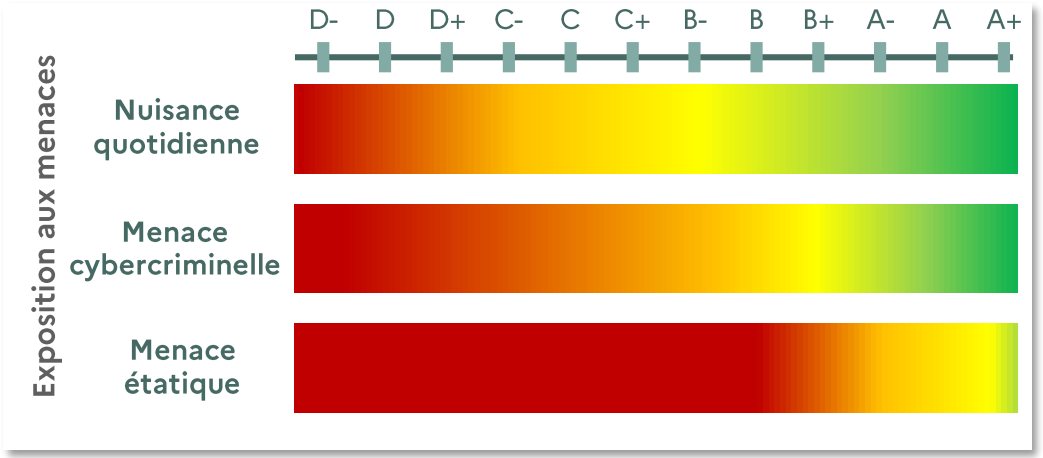


☑ S'inspire du **référentiel ISO 27000**

☑ S'inspire du **NIST Cybersecurity Framework**



L'indice de cybersécurité, basé sur ces parcours cybersécurité, permet de positionner et de suivre la maturité du bénéficiaire de façon comparative



Des démarches de diagnostic et de formalisation du plan de sécurisation à mener sur des périmètres adaptés

État des lieux

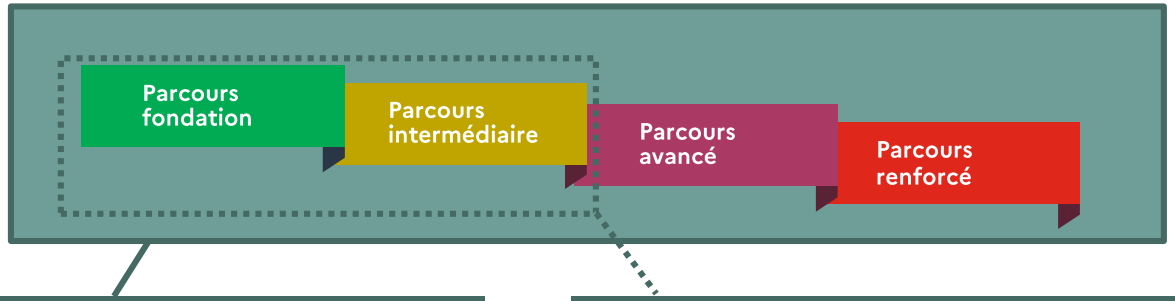
- Identification des enjeux métiers et DSI
- État des lieux SSI organisationnel
- État des lieux SSI technique
- Cartographie des zones de vulnérabilités

Plan de sécurisation

- Identification des chantiers
- Planification du plan de sécurisation
- Présentation aux dirigeants
- Mise en œuvre des mesures urgentes

Autres travaux

- Réalisation d'actions de sensibilisation



UN ÉTAT DES LIEUX GÉNÉRAL…

L'état des lieux est réalisé sur l'ensemble des mesures de sécurité, quel que soit le parcours cible du bénéficiaire, afin de pouvoir établir un **benchmark** entre toutes les entités.

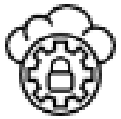
…MAIS UN PLAN DE SÉCURISATION CIBLÉ

Le plan de sécurisation est quant à lui **adossé au parcours cible du bénéficiaire**, identifié suite au pré diagnostic, afin de définir des objectifs de cybersécurité qui soient à la fois **adaptés, raisonnables et atteignables**.

La démarche permettant définir une feuille de route est inspirée de la méthodologie EBIOS Risk Manager

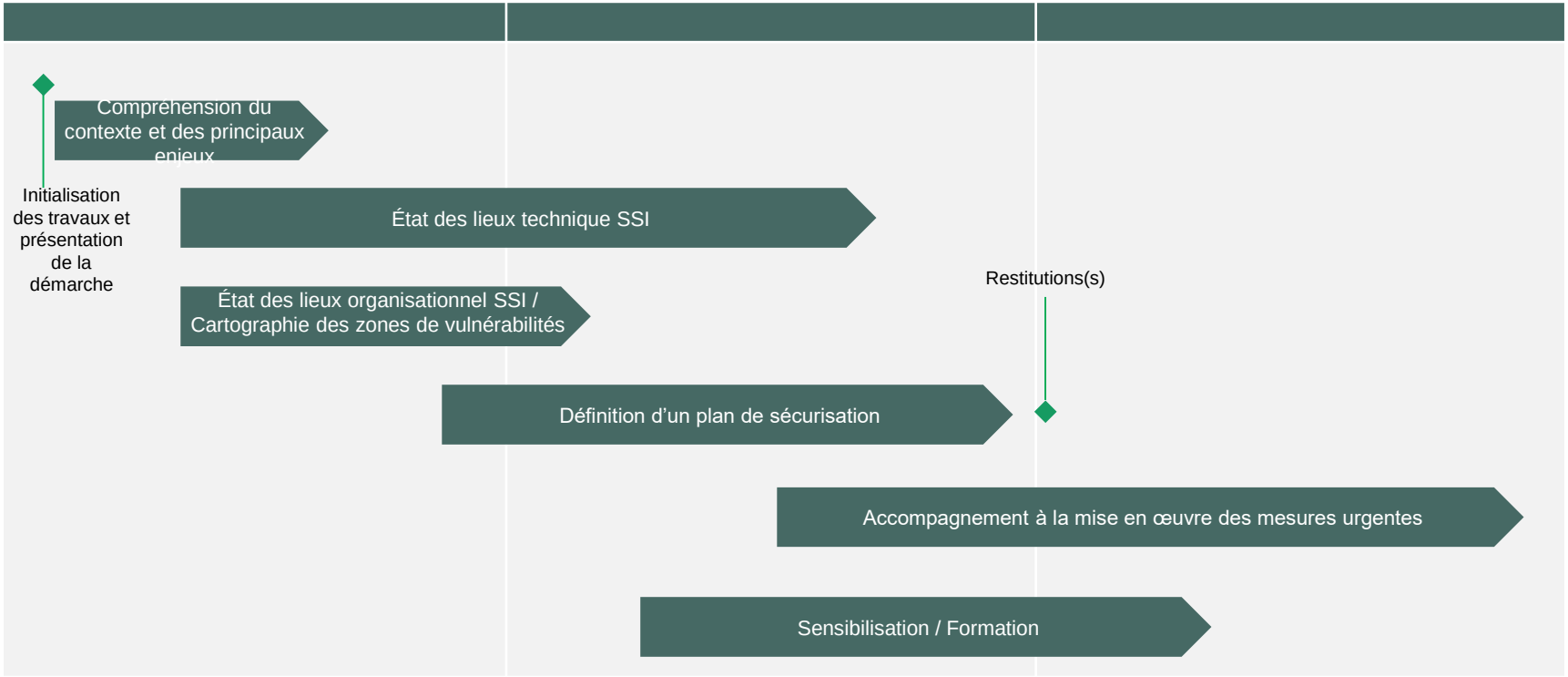
Les travaux liés à **la prise de contexte et l'état des lieux** sont ainsi proches des tâches réalisées dans le cadre **des premiers ateliers** de la démarche EBIOS Risk Manager, en particulier le premier atelier. Les travaux réalisés dans le cadre du **plan de sécurisation** sont quant à similaires à ceux réalisés dans le cadre du **dernier atelier** de la méthodologie. Enfin, aucun travail ne sera lié à l'atelier concernant les scénarios opérationnels.

En particulier, pour l'atelier des scénarios stratégiques, la démarche vise à **définir les principaux évènements redoutés** du bénéficiaire puis à déterminer sa capacité à y **faire face** d'une part **suite à l'état des lieux et** d'autre part **suite à la mise en œuvre du plan de sécurisation.** Cette démarche est le **fil directeur** de la présentation de restitution au RSSI et au DSI.

	Source de menace	Vecteur d'attaque possible	Evènement redouté	Principales vulnérabilités	Niveau d'exposition à la menace estimé avant plan de sécurisation	Niveau d'exposition après plan de sécurisation complet
Menace cybercriminelle	 **Attaque opportuniste**	• Phishing • Interfaces exposées sur Internet	Vol de données de recherche	• Manque de sensibilisation des utilisateurs • Niveau de sécurité de l'AD insuffisant	**Très Fort**	**Moyen**
		Formalisé suite à l'étape 2 (cf slide 11)		Formalisé suite à l'étape 3 (cf slide 11)		Formalisé suite à l'étape 4 (cf slide 11)

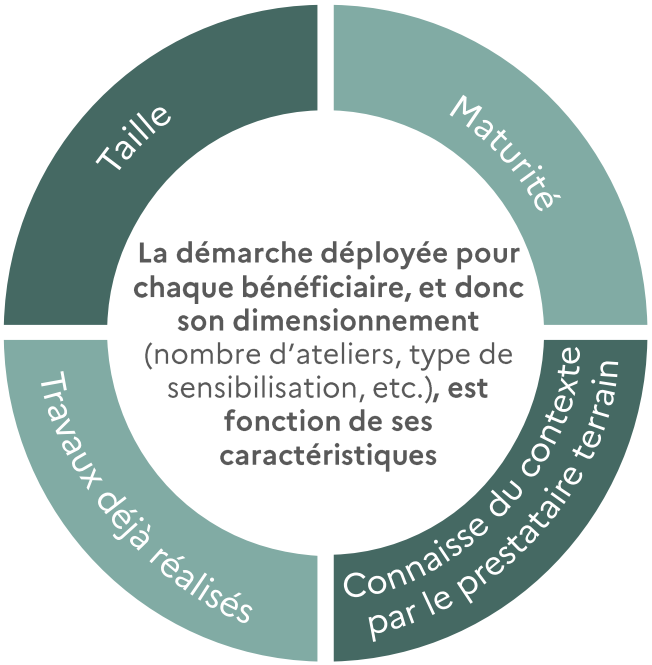
Une démarche devant respecter quelques impératifs calendaires

Afin de conserver une démarche dynamique, il est attendu que la dernière restitution des travaux aie lieu **dans les 3 mois suivant la réunion d'initialisation**. Les travaux de sensibilisation et d'accompagnement à la mise en œuvre des mesures urgentes ne sont pas pris en compte dans cette demande.



Les packs relais ne pourront être lancés qu'après la réalisation de l'ensemble des actions du pack initial

Une démarche adaptée au contexte du bénéficiaire



Les informations et éléments de contexte collectés lors du pré diagnostic permettent de **personnaliser le dimensionnement des différentes étapes du pack initial,** dans une volonté d'utiliser de la manière la plus pertinente possible l'enveloppe de ressources octroyée à chaque bénéficiaire

Exemple 1

Un bénéficiaire réalise déjà de nombreux travaux de sensibilisations auprès de toutes les populations (administrateurs, acheteurs…).

Exemple 2

Un bénéficiaire a récemment défini un plan de sécurisation très détaillé qui est validé par sa direction.

Adaptation

Conservation des ressources pour les packs relais ou renforcement d'autres travaux du pack initial (état des lieux technique ou mesures urgentes)

Réalisation d'une revue du plan de sécurisation existant pour s'assurer qu'il est adapté, plutôt que la création d'un second plan de sécurisation

Synthèse des travaux réalisés dans le cadre du pack initial

ÉTAPE 1

Réunion d'initialisation ou kick-off

- Identification des interlocuteurs et planification des ateliers

ÉTAPE 2

Atelier de compréhension du contexte et des enjeux métiers et DSI

- Support de compréhension du contexte et des enjeux métier *complété*
- Support de compréhension du contexte et des enjeux DSI complété
- Synthèse des enjeux complétée

ÉTAPE 3.A

Atelier d'état des lieux organisationnel

- Questionnaire d'état des lieux organisationnel complété
- Notation de l'ensemble des points de contrôle
- Synthèse de l'état des lieux organisationnel complétée

ÉTAPE 3.B

Etat des lieux techniques

- Rapports SILENE et ADS
- Rapport d'audit technique complété*
- Synthèse de l'état des lieux technique complétée

ÉTAPE 3.C

Cartographie des zones de vulnérabilité du SI

- Cartographie du SI du bénéficiaire mettant en avant les enjeux
- Cartographie du SI du bénéficiaire mettant en avant les vulnérabilités

ÉTAPE 4

Plan de sécurisation

- Plan de sécurisation complété
- Synthèse du plan de sécurisation complétée
- Notation de l'ensemble des points de contrôle après plan de sécurisation P0/P1
- Notation de l'ensemble des points de contrôle après l'ensemble du plan de sécurisation

ÉTAPE 5

Restitutions

- Restitution à la DSI et au RSSI complétée
- Restitution aux dirigeants complétée

ÉTAPE 6

Sensibilisation & actions urgentes

- Supports de sensibilisation types spécifiques aux populations ciblées adaptés
- Stratégie de sensibilisation

Le fond documentaire fourni au lancement des travaux s'applique durant l'ensemble du pack initial. Les éventuelles versions de fonds documentaires qui seraient publiées ensuite ne doivent pas être prises en compte.

Il n'est pas attendu de comptes-rendus Word dans le cadre de la démarche. Les supports PowerPoint et Excel complétés ou mis à jour serviront de compte-rendu des réunions réalisées.

*Utilisation du template non obligatoire

Réunion d'initialisation ou kick-off

Documents fournis

- Support d'initialisation
- Pré diagnostic

Prérequis

/

Livrable(s) de cette étape

- Identification des interlocuteurs et planification des ateliers

Réunion d'initialisation ou kick-off

- La réunion d'initialisation, ou kick-off, a pour but de faire un **premier tour de table entre les prestataires terrain et accompagnateur et le bénéficiaire**, et de présenter le dispositif, **le parcours cible**, le planning, les différentes étapes ainsi que les modalités de travail.
- Cette réunion doit être préparée, notamment à l'aide du support d'initialisation contextualisé et du questionnaire pré diagnostic. Ces documents sont fournis par le prestataire accompagnateur ou le bénéficiaire.
- Dès cette première réunion, le prestataire terrain doit **commencer à planifier les prochains ateliers** et donc identifier, avec le RSSI/référent sécurité, qui seront les **interlocuteurs pertinents à chacune des étapes.**

  Cette identification des interlocuteurs peut s'appuyer sur la liste des 14 thématiques de l'Etat des lieux organisationnel (cf. slide 18) qui doit être partagée avec le bénéficiaire pendant la réunion.
- Les prestataires terrain et accompagnateur doivent également déterminer si des **adaptations** devront être faites à la démarche et, le cas échéant, de quelle manière les mettre en œuvre sans impacter les **hypothèses dimensionnantes.** Ex : *Remplacer un groupe de travail « Enjeux métier » par un groupe de travail sur la construction du plan de sécurisation.*
- A l'issue de cette réunion, le prestataire terrain doit collecter des éléments de **documentation** (organigrammes, référentiels, cartographies, PSSI, feuille de route de la DSI/SSI…) auprès du bénéficiaire, afin de pouvoir en prendre connaissance avant le prochain atelier. Il veillera naturellement à utiliser des moyens adaptés à la sensibilité des données (Ex. conteneur *Zed!*)

⚠ Cette réunion ne doit pas se faire sans le prestataire accompagnateur

Ateliers de compréhension du contexte et des enjeux métiers et DSI

Documents type fournis

- Support de compréhension du contexte et des enjeux métier
- Support de compréhension du contexte et des enjeux DSI
- Synthèse des enjeux type

Prérequis

- Documentation fournie par le bénéficiaire

Livrable(s) de cette étape

- Support de compréhension du contexte et des enjeux métier *complété*
- Support de compréhension du contexte et des enjeux DSI *complété*
- Synthèse des enjeux *complétée*

Ateliers de compréhension du contexte et des enjeux métiers et DSI

Les ateliers de compréhension du contexte et des enjeux doivent permettre au prestataire terrain à la fois de **confronter les visions métier et DSI de la SSI** mais également disposer de tous les éléments nécessaires pour **orienter intelligemment le plan de sécurisation sur les éléments les plus pertinents** en prenant notamment en compte les périmètres métiers critiques, les menaces (approche par les risques) et les évolutions à venir du SI.

Avant les ateliers

- **Envoyer les supports** en amont, pour que les interlocuteurs puissent **préparer les questions**
- Consulter la **documentation** envoyée par le bénéficiaire
- Consulter le **questionnaire de pré-diagnostic** (premier onglet) afin d'avoir des premiers éléments de contexte concernant le SI
- Convier **l'auditeur technique** aux ateliers de compréhension du contexte et des enjeux DSI

Après les ateliers

- Rédiger les **comptes rendus, directement dans les fichiers Powerpoint**
- Envoyer les comptes rendus au bénéficiaire pour **validation**

1. Ateliers de compréhension du contexte et des enjeux métiers

Interlocuteurs : RSSI/référent sécurité et Métiers

Objectifs

- Plonger dans le **contexte** et les **enjeux métiers** du bénéficiaire. : *quels sont les processus métier critiques (messagerie …) ? Quelles sont les activités critiques ? Quelles sont les actifs critiques et leur impact associé en termes DICT ? Y-a-t-il des activités OSE ? Quelles sont les craintes principales ?*
- Prendre le pouls des **interlocuteurs non-SI et non-SSI**
- Comprendre quelles vont être les **principales évolutions** pour orienter le plan de sécurisation et concentrer les efforts sur **les périmètres les plus sensibles**

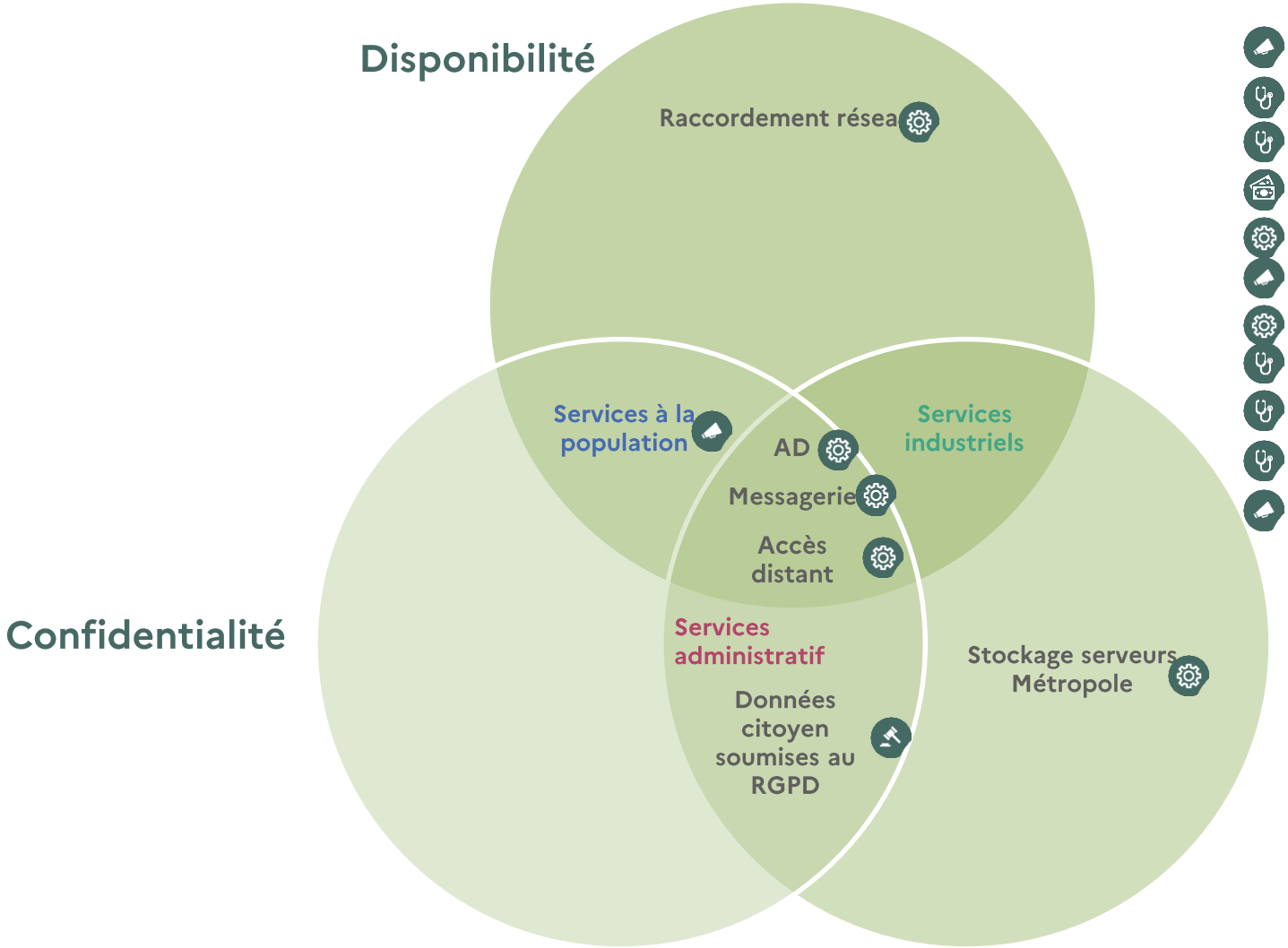
2. Ateliers de compréhension du contexte et des enjeux DSI

Interlocuteurs : RSSI/référent sécurité, DSI et équipe SI

Objectifs

- Comprendre **l'architecture des SI**
- Comprendre quelles sont **les orientations SI** pour les prochaines années : *Full-Cloud ? Externalisation des développements ? Pérennisation du télétravail ?*
- Ex : Si la DSI projette le full-cloud l'année suivante, il faudra déployer des efforts particuliers sur la sécurisation du Cloud dans le plan de sécurisation
- Comprendre les **inquiétudes et attentes de la DSI** vis-à-vis de la sécurisation des SI
- **NB :** La participation de l'auditeur technique peut être intéressante en préparation des tests techniques

Exemple de restitution des principaux enjeux métiers pour une collectivité territoriale



- Services numériques aux usagers
- Gestion de la vaccination
- Activités sociales du CCAS
- Logiciels de gestion financière
- Logiciels RH
- Évènementiel
- Vidéosurveillance
- Gestion du trafic routier
- Traitement des eaux usées
- Approvisionnement en eau
- Cuisine centrale / scolaire

Impact financier | Impact d'image | Impact opérationnel | Impact sur la santé des citoyens ou des agents | Impact juridique

Ateliers d'état des lieux organisationnel

Documents type fournis

- Questionnaire d'Etat des lieux organisationnel
- Synthèse de l'état des lieux organisationnel type

Prérequis

- Thématiques du questionnaire d'Etat des lieux organisationnel réparties par interlocuteurs à interroger

Livrable(s) de cette étape

- Questionnaire d'Etat des lieux organisationnel *complété*
- Notation de l'ensemble des points de contrôle
- Synthèse de l'état des lieux organisationnel *complétée*

Ateliers d'état des lieux organisationnel

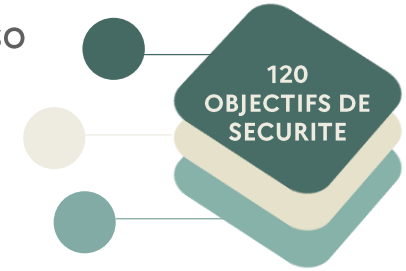
Questionnaire d'état des lieux organisationnel

- L'état des lieux organisationnel est un questionnaire plus de **200 questions** inspirées de différents référentiels et regroupées en **14 thématiques ayant pour objectif de déterminer la maturité SSI du bénéficiaire.**
- Il s'agit d'un état des lieux **déclaratif.** Les questions sont en principe suffisamment complètes pour éviter la majorité des non-dits.
- Pour chacune des questions, **une aide à la notation** a été formalisée. Elle permet à la fois de cadrer la notation de l'indice de cybersécurité et **d'orienter le prestataire** dans la formulation/précision des questions durant les ateliers.

☑ S'inspire du **référentiel ISO 27000**

☑ Contient les **42 mesures d'hygiène informatique essentielles de l'ANSSI**

☑ S'inspire du **NIST Cybersecurity Framework**



Avant les ateliers

- Identifier **quels sont les bons interlocuteurs en fonction des 14 thématiques du questionnaire** puis envoyer à chacun **la liste des questions spécifiques les concernant en amont**, afin qu'ils puissent **les préparer**.
- Consulter le **questionnaire de pré-diagnostic** (second onglet) afin d'avoir des premiers éléments concernant la maturité SSI.

Pendant l'atelier

- Ecrire les réponses du bénéficiaire en séance afin qu'il puisse apporter **corrections et précisions en direct.**
- **Traiter l'ensemble des questions en atelier,** sauf exceptions (ex. absence d'applications dans le Cloud).
- **Ne pas hésiter à approfondir les sujets répondus laconiquement.** Des notes complètes et fiables faciliteront par la suite la **notation.**

Après l'atelier

- **Relire** le questionnaire complété.
- Soumettre le questionnaire complété au bénéficiaire pour **validation** avant de procéder à la **notation.**

⚠ Il sera nécessaire de répondre **à toutes les questions de l'état des lieux organisationnel** (à l'exception des sujets non applicables à cause du contexte SI du bénéficiaire cf. page 20), **quel que soit le parcours retenu** pour le bénéficiaire

Thématiques de l'état des lieux organisationnel SSI

14 grandes thématiques, entre 10 et 25 questions par thème :

Ex : RSSI

- Gouvernance
- Applications
- Protection des données
- Détection
- SI industriels / biomédicaux
- Sensibilisation
- Gestion des fournisseurs et des partenaires
- Gestion des identités et des accès
- Gestion des incidents et Résilience
- Conformité et Audits
- Environnement utilisateur
- Administration
- Réseau
- Cloud

Ex : DSI

Afin d'optimiser le temps passé sur l'Etat des lieux organisationnel, il est important de déterminer **dès la réunion d'initialisation** quels seront les **bons interlocuteurs en fonction des thématiques** (*exemples sur le schéma ci-dessus*) afin d'organiser les ateliers de façon à limiter au mieux le temps d'intervention des différents intervenants (*par exemple, il sera préférable de ne pas solliciter un responsable des postes de travail plus de 30 à 45 minutes*).

Les **questions spécifiques** associées aux thématiques devront être **envoyées aux bons interlocuteurs en amont** afin qu'ils puissent les préparer.

Indice de cybersécurité et consignes de notation de l'état des lieux organisationnel

- L'indice de cybersécurité permet au bénéficiaire de **mesurer sa maturité cyber** et de **se positionner par rapport aux autres entités.**
- Il se construit à travers l'attribution d'une **notation de chaque point de contrôle de l'état des lieux organisationnel** en s'appuyant sur **l'aide à la notation** fournie dans le questionnaire.
- Tous les scores établis doivent être compris **entre 0 et 1.**

  1 devra être considéré comme une note maximale, et sera le plus souvent plutôt **difficile à obtenir**.
- Si le point de contrôle est **non-applicable** à l'organisation étudiée, du fait **de son contexte SI**, noter **"N/A".** Le point de contrôle sera ainsi exclu du calcul de l'indice de cybersécurité dans la suite de la démarche.

  Par exemple, l'absence de SI industriel ou de systèmes dans le Cloud permettra de N/A aux questions associées. Par contre, l'absence de proxy ou de dispositif similaire devra être notée 0 à la question associée. Il ne serait possible de mettre N/A à une question concernant le proxy que si le SI n'avait aucun flux sortant vers l'extérieur.
- Attention, le **mode de notation** indiqué dans l'aide à la notation n'est **pas homogène** et peut varier d'une question à l'autre. En effet, la notation peut être construite **par paliers**, être **cumulative**, comme illustré dans *l'exemple ci-dessous,* voire être une combinaison des deux.

  En cas de notation par paliers, les différents paliers proposés sont regroupés et identifiés **en gras** dans l'aide à la notation.

	Point de contrôle	Aide à la notation
Protection des postes de travail	Les postes de travail et les équipements mobiles (e.g. smartphones, tablettes) sont-ils répertoriés au sein d'un inventaire centralisé qui comprend tous les éléments nécessaires à leur connaissance (e.g. modèle, utilisateur du bien, services /applications locaux associés..) ? Quel outil ou document est utilisé pour ce faire (e.g. fichier Excel, SSCM, Intune,...) ?	0 : Absence d'inventaire des postes de travail et des équipements mobiles +0,4 : Tous les postes de travail sont inventoriés dans un inventaire centralisé +0,3 : Tous les équipements mobiles sont inventoriés dans un inventaire centralisé +0,2 : L'inventaire est mis à jour régulièrement +0,1 : L'inventaire comprend au minimum les éléments suivants : modèle, utilisateur du bien, services / applications locaux associés
Protection des serveurs	Avez-vous mis en œuvre un EDR sur tous les serveurs pour une surveillance et une analyse continue afin d'identifier, de détecter et de prévenir plus facilement les menaces avancées et les signaux faibles ? L'ensemble du parc est-il couvert ?	+0,2 : Au moins 70% des serveurs ont un EDR +0,5 : Au moins 80% des serveurs ont un EDR +0,8 : Au moins 90% des serveurs ont un EDR +1 : Tous les serveurs ont un EDR

*Exemple de notation **cumulative** : pour avoir 1 point, il faut mettre en œuvre les 4 sujets évoqués dans l'aide à la notation*

*Exemple de notation **par paliers** : La note à retenir est celle associées à de l'état du bénéficiaire parmi les propositions effectuées*

Calcul de l'indice cybersécurité

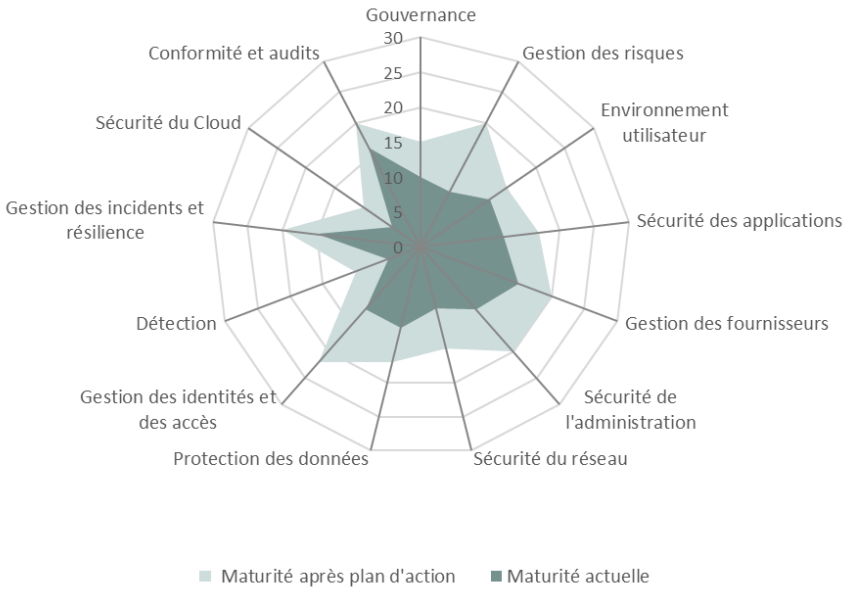
Une fois les notes attribuées, celles-ci doivent être **envoyées au prestataire accompagnateur de façon sécurisée (conteneur Zed) dans un fichier Excel.**

Grâce à un outil interne de traitement des données, celui-ci fournira alors au prestataire terrain les scores totaux avant et après le plan de sécurisation (présenté plus loin lors de ce document) ainsi qu'un détail par catégorie. Un **graphique** représentant l'évolution attendue de la **maturité cyber du bénéficiaire** sera également disponible. *Exemple ci-dessous*

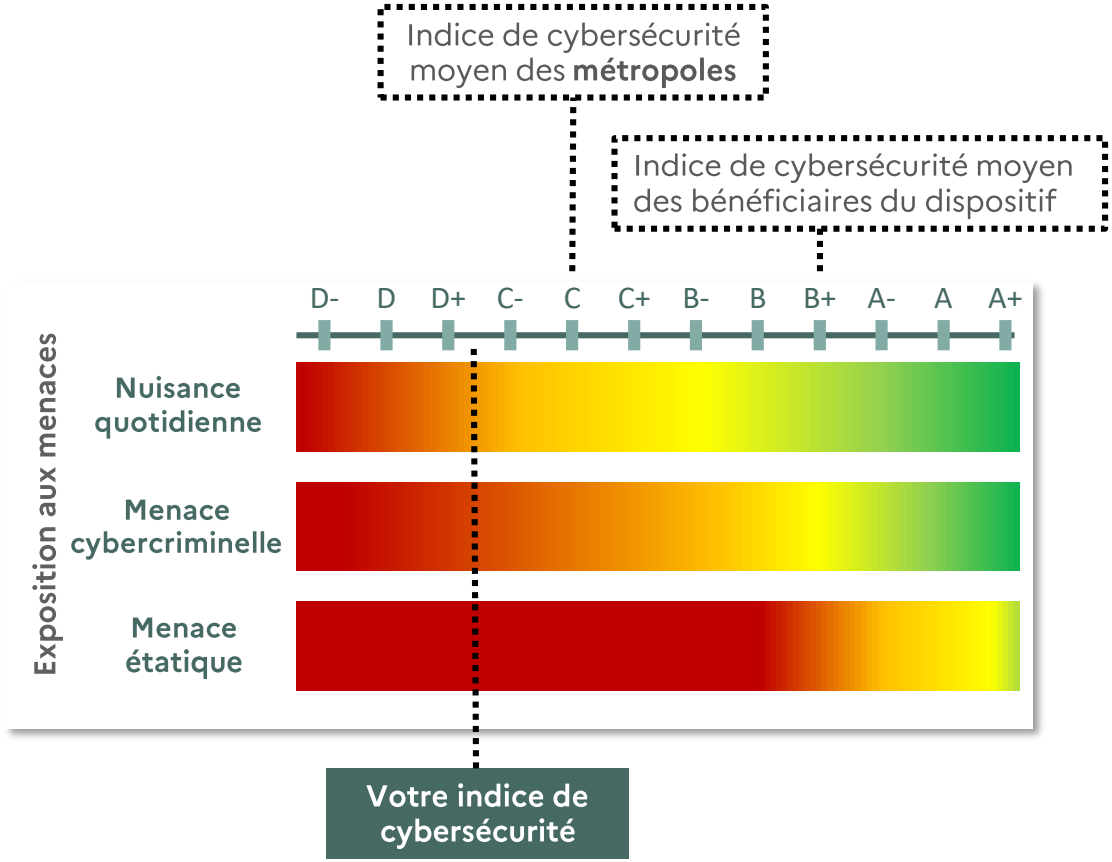
L'indice de cybersécurité ainsi obtenu **correspondra alors à une note en lettre (ex. : A, B-, D+)** qui devra par la suite être reportée dans les **documents de restitution.**

Correspondance de l'indice de cybersécurité	
350 – 400	A+
310 – 349	A
275 – 309	A-
245 – 274	B+
220 – 244	B
200 – 219	B-
180 – 199	C+
155 – 179	C
125 – 154	C-
90 – 124	D+
50 – 89	D
0 – 49	D-

- Il est **indispensable** que **l'intégralité** des questions soit notée **(pas de cases vides).**
- Si un point de contrôle est **non-applicable à l'organisation étudiée,** noter **"N/A".** Le point de contrôle sera ainsi **exclu du calcul de l'indice de cybersécurité.**



Exemple de restitution du benchmark



Etat des lieux technique

Documents type fournis

- Modes opératoires de l'ANSSI pour les services SILENE et ADS
- Rapport d'audit technique type
- Synthèse de l'état des lieux technique type

Prérequis

- Adresses IP publiques, compte d'accès distant, compte utilisateur standard, schéma macroscopique du SI du bénéficiaire…
- Lettre de mission d'audit

Livrable(s) de cette étape

- Rapports SILENE et ADS
- Rapport d'audit technique (format libre) *complété*
- Synthèse de l'état des lieux technique *complétée*

Dans le cadre de cette étape, **les travaux liés à SILENE et ADS sont réalisés par le bénéficiaire** (avec un éventuel support très léger du prestataire terrain). Les résultats des audits SILENE et ADS seront ensuite fournis par le bénéficiaire au prestataire terrain pour alimenter sa réflexion dans le cadre de la formalisation du plan de sécurisation.

Dans le cadre de l'audit technique, **les travaux à réaliser** (scans de vulnérabilités, tests d'intrusion, revue de configuration, revue d'architecture…) **et le périmètre concernés doivent être définis avec le bénéficiaire lors de la**

Etat des lieux technique

L'état des lieux technique **complète ou confirme l'Etat des lieux organisationnel** via la **réalisation de travaux de scans (internes et externes) de vulnérabilités, de tests d'intrusion, de revues de configuration et de revue d'architecture et des processus d'exploitation du SI.**

*Parmi les travaux classiques pouvant être réalisés pour une entité peu mature, on pourra avoir la réalisation d'un **scan des sites exposés sur internet** ainsi que la tentative **d'élévation de privilège sur l'AD depuis un compte utilisateur standard**. Les travaux pourront se concentrer sur la sécurité de quelques serveurs critiques internes ainsi que sur l'accès aux consoles d'administration de solutions de sécurité/des sauvegardes/ des postes de travail*

Pour un bénéficiaire très mature, les travaux pourront se concentrer sur le réseau interne ou mettre en œuvre des revues de configuration plus détaillées.

Avant le lancement des tests

- **Se coordonner avec les équipes techniques** internes - ou externes si un autre prestataire a été assigné à l'état des lieux technique - pour identifier l'auditeur et sa disponibilité.
- Convier l'auditeur technique aux **Ateliers de compréhension du contexte et des enjeux DSI.**
- Demander au bénéficiaire de fournir les **prérequis nécessaires à l'audit,** *a minima* : adresses IP publiques, compte d'accès distant, compte utilisateur standard, schéma macroscopique du SI.
- Planifier une **date de début d'audit.**
- Envoyer une **lettre de mission** au bénéficiaire, avec les **coordonnées des auditeurs,** un **rappel de la démarche** qui va être déployée et une **demande de feu vert** pour le lancement des tests.

En parallèle des tests techniques

En tant qu'interlocuteur technique, l'auditeur doit également demander au bénéficiaire de lui **fournir les scores et rapports suivants** :

- **SILENE :** Scans externes
- **ADS :** Audit AD

Ces scores et rapports sont **générés via les outils automatisés de l'ANSSI** dont les **modes opératoires** doivent être communiqués au **bénéficiaire qui est chargé de les utiliser**.

L'auditeur technique doit simplement **s'assurer que le bénéficiaire réalise ces actions** et lui **porter assistance** s'il rencontre des difficultés dans la compréhension des modes opératoires.

Les rapports ainsi générés pourront compléter et nourrir le rapport d'audit technique. Les scores obtenus seront également partagés sur les **supports**

- Les équipes d'audit **peuvent utiliser leurs propres outils et templates de rapport d'audit.** Le seul document attendu dans un format type du parcours cybersécurité est la **synthèse de l'état des lieux technique**.
- Au-delà du nombre de vulnérabilités identifiées, aucun score spécifique n'est à fournir mais les indicateurs pertinents dans le cadre des périmètre étudiés et des tests réalisés peuvent être restitués

Exemple de synthèse de l'état des lieux technique

Rappel des tests réalisés et des périmètres couverts

- **Tests d'intrusion externes** : Cartographie des informations accessibles sur internet
- **Tests d'intrusion internes** : Cartographie et analyse des vulnérabilités du réseau - et analyse de l'Active Directory
- **Périmètre ciblé** : Les tests ont été menés sur l'environnement de production
- **Approche boite noire** (aucun authentifiant n'est transmis à l'auditeur) pour la phase externe et **approche boite grise** (l'auditeur dispose d'authentifiant utilisateur) pour la phase interne.

Nbre **total** de vuln. identifiées	**20**

Nbre de vuln. **critiques** identifiées	**7**

Score ADS *(audit AD)*	**1** 2 3 4 5

33 pb importants

Score SILENE *(scans externes)*	**1** 2 3 4 5

23 pb importants

Principaux constats réalisés dans le cadre des tests techniques

- Le **système d'information** est **globalement maintenu à jour** : aucun OS obsolète n'a été identifié et aucune vulnérabilité critique impactant les systèmes d'exploitation n'a pu être identifiée.
- Le réseau interne est **correctement cloisonné**. Il n'est pas possible d'accéder qu'à un nombre limité de ressources du réseau depuis un point donné.

- Les **interfaces du système d'information exposées sur Internet ne sont pas maintenues à jour**. De plus, elles exposent des **informations sensibles**.
- Il est d'ailleurs possible d'accéder à **des fichiers contenant des informations techniques sensibles** sans authentification.

Cartographie des zones de vulnérabilités du SI

Documents type fournis

Exemple de cartographie des zones de vulnérabilités du SI du bénéficiaire

Prérequis

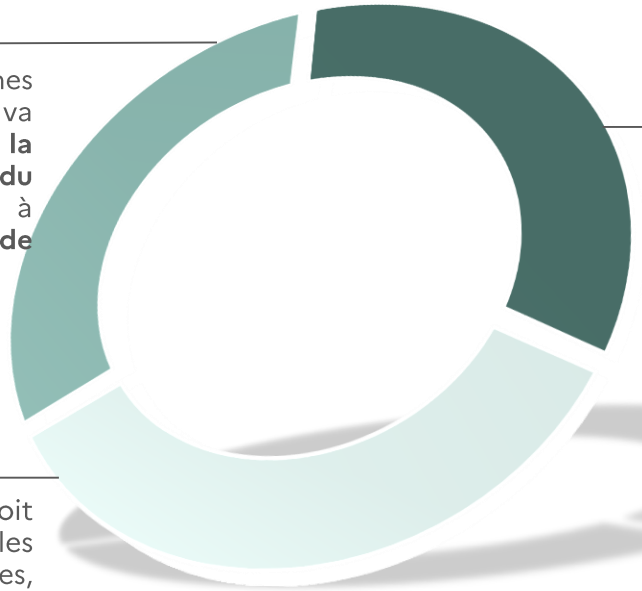
- Etude du contexte
- Etat des lieux organisationnel
- Etat des lieux technique

Livrable(s) de cette étape

- Cartographie du SI du bénéficiaire mettant en avant les enjeux
- Cartographie du SI du bénéficiaire mettant en avant les vulnérabilités

Cartographie des zones de vulnérabilités du SI

La cartographie des zones de vulnérabilités du SI va dans le **prolongement de la compréhension contexte du bénéficiaire** et vise à **orienter le plan de sécurisation.**



Cette cartographie doit représenter les ressources, les utilisateurs, les partenaires, les prestataires, les sites et les interconnexions et **offrir une vue d'ensemble du SI.**

Elle doit être construite comme une **synthèse schématique de l'Etat des lieux technique et de la compréhension des enjeux**, dont le but est de mettre en lumière de manière graphique **dans un premier temps les zones les plus sensibles** du SI du bénéficiaire et **dans un second temps les failles et vulnérabilités majeures** observées, notamment suite à l'état des lieux technique

Ces zones peuvent être représentées par des **éléments graphiques** indiquant les **points**

Exemples de points d'alertes à faire figurer sur la cartographie

Postes de travail non maitrisés

Application Métier critique

Données sensibles exposées sur internet

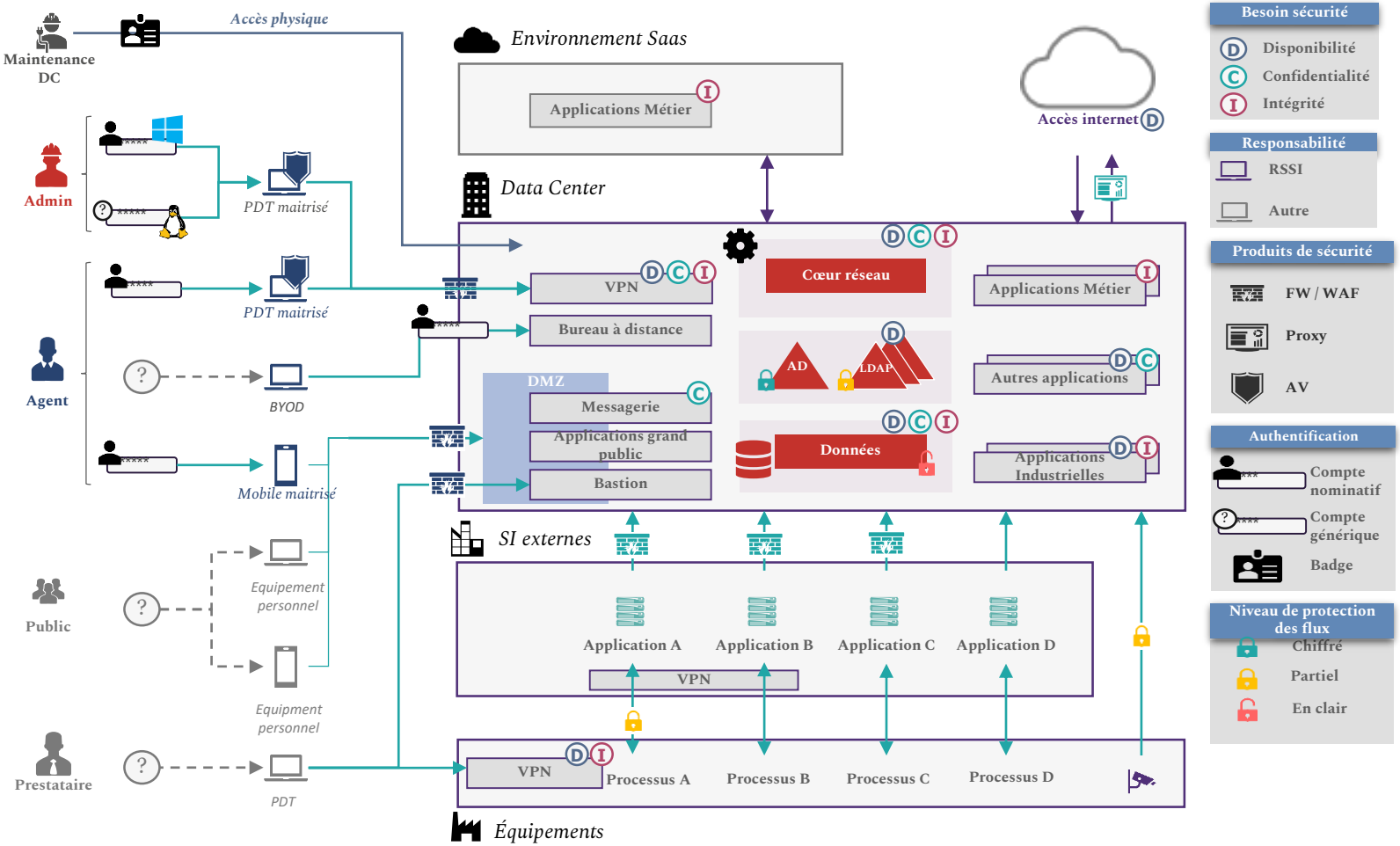
AD

Active Directory non durci

L'objectif de ce schéma est d'illustrer de façon graphique le SI du bénéficiaire afin de faire passer des messages **clairs et impactants sur les zones de vulnérabilité**.
Le temps passé sur cette cartographie dans le cadre du pack initial **ne doit pas dépasser un jour homme**

Exemple de cartographie du système d'information à produire

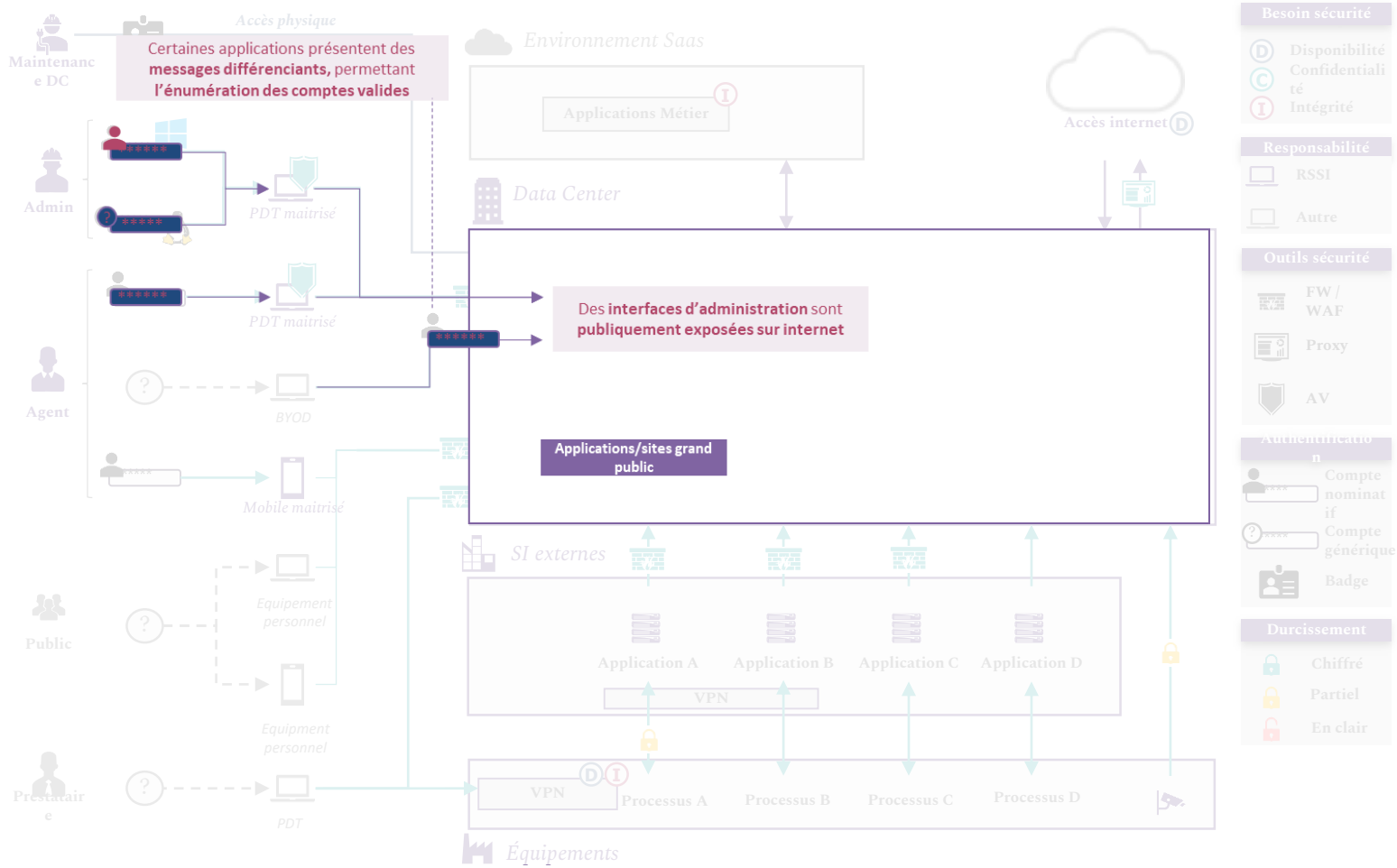
Vue de l'infrastructure technique du système d'information



Il est possible de regrouper des périmètres applicatifs sous une même référence

Exemple de cartographie du système d'information à produire (2/2)

Vue de l'infrastructure technique du système d'information incluant les Vulnérabilités internes suite à l'état des lieux technique



Synthèse de l'analyse de l'existant et détermination des chantiers composant le plan de sécurisation SSI

Documents type fournis

- Modèle de plan de sécurisation
- Synthèse du plan de sécurisation type
- Proposition de pack relais type

Prérequis

- Questionnaire d'Etat des lieux organisationnel *complété*
- Notation de l'ensemble des points de contrôle
- Etat des lieux technique

Livrable(s) de cette étape

- Plan de sécurisation *complété*
- Synthèse du plan de sécurisation *complétée*
- Notation de l'ensemble des points de contrôle après plan de sécurisation P0/P1
- Notation de l'ensemble des points de contrôle après l'ensemble du plan de sécurisation
- Proposition de pack relais

Synthèse de l'analyse de l'existant et détermination des chantiers composant le plan de sécurisation SSI (1/3)

- A partir des constats réalisés lors des états des lieux organisationnel et technique, il faudra définir un plan de sécurisation composé de **10 à 15 macro-chantiers**, déclinés **en 30-50 actions** et **rattachés au parcours cible du bénéficiaire**
    - Un **chantier peut être associé à une catégorie de l'état des lieux organisationnel** (*ex. Sensibilisation du personnel, Protection des données en mouvement, Gestion des sauvegardes etc.*) alors qu'une **action sera plus précise** (*ex. Mise en place de modules de formation à la cybersécurité pour les développeurs et les administrateurs du SI, Mise en place d'une solution de chiffrement des pièces jointes pour les données sensibles, Réalisation de tests de restauration des sauvegardes etc.*)

Les chantiers mis en œuvre devront :

- prendre en compte les constats réalisés suite à l'état des lieux organisationnel et technique,
- être **cohérents** avec les **principaux enjeux SSI** du bénéficiaire et notamment couvrir ses **périmètres métiers plus sensibles**
- couvrir les principales menaces qui visent le bénéficiaire (en particulier le **ransomware**)
- être **cohérents avec les orientations et les évolutions du SI** du bénéficiaire (ex : généralisation du Cloud ou du télétravail)

Actions	Priorité	Complexité	Coûts projet		Coûts récurrrents		Hypothèses de dimensionnement	Budget Validé	Porteur	Planning	
			Charges (j.h)	Invest. (k€)	Charges (j.h)	Invest. (k€)				mai-21	juin-21
	P0	+	30	xx k€	xx j.h.	xx k€		OUI	INTERNE		
	P1	++	40 - 50					NON	EXTERNE		
	P2	+++	5						A ARBITRER		

Synthèse de l'analyse de l'existant et détermination des chantiers composant le plan de sécurisation SSI (2/3)

- L'objectif **n'est pas de traiter tous les points** de contrôle de l'Etat des lieux organisationnel mais de **se concentrer sur le parcours cible du bénéficiaire** afin de construire un plan de sécurisation **raisonnable et atteignable**.
  - Pour ce faire, il faudra d'abord **identifier les points de contrôle à améliorer** en identifiant ceux **rattachés au parcours cible du bénéficiaire (qui inclut les mesures des parcours précédents)**, puis éventuellement **ajouter certains points de contrôle d'un parcours suivant** si cela semble pertinent compte tenu du **contexte** du bénéficiaire identifié lors des échanges sur son contexte **SI et métier**

    La sélection se fait en faisant un tri sur la colonne du parcours cible du bénéficiaire (par exemple, intermédiaire) pour ne retenir que les cases vertes.
  - Une fois les points de contrôle à améliorer identifiés, le prestataire terrain doit formuler, en fonction de l'état des [illegible] **an de sécurisation, ou feuille de route**.

Réf	Catégorie	Question	Fondation	Interm. et -	Avancé et -	Renforcé et -
1	Rôles et les responsabilités en matière de cybersécurité	Qui est le responsable de la Sécurité des Systèmes d'Information au sein de votre organisation ?				
2		A qui est rattaché le RSSI ?				
3		Quelles sont les ressources en ETP (Equivalent Temps Plein) dédiées à la réalisation des activité de cybersécurité ? *(n'inclut pas les administrateurs des infrastructures)*				
4		Avez-vous des ressources dédiées à la sécurité opérationnelle ?				
5		Avez-vous identifié formellement les processus SSI *(e.g. gestion des incidents, gestion des sauvegardes, gestion des exceptions, gestion des vulnérabilités…)* à mettre en œuvre au sein de votre organisation ? Avez-vous déterminé les compétences, les rôles et responsabilités associés ? Les responsabilités ont-elles été réparties entre les équipes (par exemple au travers d'un RACI) ?				

Dans l'exemple ci-contre

- Parcours Fondation : Points 1 et 3 applicables
- Parcours Intermédiaire : Points 1 et 3 applicables
- Parcours Avancé : Points 1, 3, 4 et 5 applicables
- Parcours Renforcé : Points 1 à 5 applicables

Il n'est **pas attendu** que le plan de sécurisation traite **exhaustivement les points du parcours cible** qui ne sont pas encore à un niveau de maturité suffisant. Il s'agira en priorité d'identifier les points permettant d'améliorer sensiblement la capacité du bénéficiaire **à faire face aux principaux risques** qui le menacent (cf page 8)

La majorité des mesures se trouveront dans ce parcours cible. Cependant afin de mieux répondre aux risques, il est possible de manière **marginale de prendre quelques mesures dans les parcours supérieurs**

Synthèse de l'analyse de l'existant et détermination des chantiers composant le plan de sécurisation SSI (3/3)

- Une fois les chantiers identifiés, le prestataire pourra s'atteler à la construction détaillée du plan de sécurisation.

Le plan de sécurisation doit être correctement dimensionné, à la fois financièrement et dans le temps

Chaque action doit comprendre une **estimation des coûts fixes** (*ex. prix de l'acquisition d'une licence*) et de **la charge** (*en J.H*) de mise en œuvre. Si des **coûts récurrents** sont à prévoir, ils doivent également être mentionnés.

Pour que le plan de sécurisation soit raisonnable, il doit pouvoir être **réalisable dans une enveloppe de ressources adaptée** à la taille et des moyens SSI du bénéficiaire (cf. page suivante)

Chaque action doit également être **positionnée dans le temps** et l'ensemble du plan de sécurisation doit pouvoir être **réalisé dans un délai réaliste sans être trop étendu (moins de 3 ans).**

Le plan de sécurisation doit être priorisé

Lors des ateliers de construction du plan de sécurisation, le prestataire et le bénéficiaire doivent **discuter ensemble d'une priorisation des actions**. Chaque action doit être **priorisée en P0, P1, P2 et P3**, en fonction de son **degré d'urgence** et/ou de la **facilité de réalisation** (*quick-win*). Dans cette segmentation, la **réalisation de toutes les actions P0 et P1** doit déjà permettre d'augmenter sensiblement le niveau de sécurité.

Cette priorisation devra notamment intégrer **3 ou 4 actions considérées comme étant les plus importantes** en termes de protection du SI du bénéficiaire. Elles pourront faire l'objet de **packs relais** prévu par le dispositif à l'issu du pack initial.

L'apport du plan de sécurisation au niveau de maturité cyber doit être mesurable

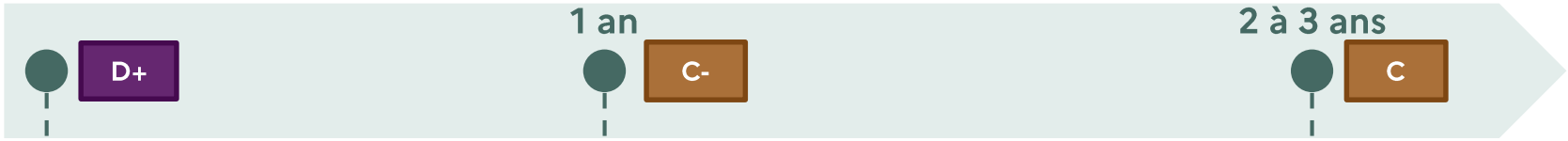
L'indice de cybersécurité permet au bénéficiaire de comparer son niveau de sécurité avec ceux de son secteur, mais aussi de **mesurer sa progression** après la réalisation du plan de sécurisation. Ainsi, la réalisation d'un chantier **induit une augmentation de la note du ou des points de contrôle associés.**

Un **nouvel indice** devra être ainsi calculé suite à la réalisation **de toutes les actions P0 et P1** et suite à la mise en œuvre de **l'ensemble du plan de sécurisation.**

Focus sur le dimensionnement du plan de sécurisation

Lors de la définition du plan de sécurisation, il est important d'afficher 2 temporalités qui correspondent à 2 indices de cybersécurité distincts.

L'objectif est d'avoir une première échéance à **horizon 1 an** qui soit réaliste vis-à-vis de la capacité SSI à faire et à piloter des bénéficiaires et une seconde échéance à 2 ou 3 ans pour l'ensemble des actions du plan de sécurisation (de P0 à P3).



Indice de cybersécurité actuel

Rédaction plan de sécurisation

Indice de cybersécurité à 1 an

Actions P0 et P1

Les actions P0 (quick-wins et actions indispensables à court terme) et P1 (actions à mener dans l'année) :

- Sont **réalisables en 1 an ou moins**
- Représentent **moins de 50% du chiffrage global** du plan de sécurisation
- Ne représentent pas plus de **200 j.h par ETP SSI présent chez le bénéficiaire**

Indice de cybersécurité après le plan de sécurisation

Actions P2 et P3

Les actions P2 (actions à mener dans les 2 à 3 ans) et P3 (chantiers ambitieux pour aller plus loin mais dont les moyens nécessaires ne sont pas garantis) :

- Sont **réalisables en 2 à 3 ans**
- Représentent **plus de 50% du chiffrage global** du plan de sécurisation

bénéficiaire et par an

Ces charges couvrent les travaux **réalisés en interne et externalisés**

Ces estimations budgétaires devront être **partagées avec les décideurs appropriés (DSI, DGS…) en amont des restitutions** pour éviter un effet découverte et une éventuelle réaction de recul voire négative de ces acteurs lors

Focus sur la mise à jour de l'indice de cybersécurité

Une fois l'intégralité des chantiers du plan de sécurisation identifiés, les **scores « après » actions doivent donc être déterminés** dans les colonnes du questionnaire d'état des lieux organisationnel prévues à cet effet. Un **nouvel indice** devra ensuite être calculé suite à la réalisation **de toutes les actions P0 et P1** et suite à la mise en œuvre de **l'ensemble du plan de sécurisation.**

Il s'agira alors de s'assurer que **l'augmentation de l'indice reste réaliste. Vouloir viser une amélioration trop importante de l'indice « pour faire bien » ne pourra se faire qu'au prix d'un plan de sécurisation trop chargé qui n'obtiendra pas in fine l'implication des équipes du bénéficiaire dans sa mise en œuvre.**

Indice de cybersécurité	Actuel	Après plan de sécu P0/P1	Après plan de sécu complet
	135	165	206

Exemple d'évolution de l'indice de cybersécurité pour un bénéficiaire (score sur 400)

Le score d'une question pour laquelle une recommandation a été formulée doit **logiquement augmenter suite au plan de sécurisation.** Néanmoins, la réalisation d'un chantier **n'équivaut pas nécessairement à une notation maximale** sur le ou les points de contrôle associés.

En d'autres termes, **la note 1 ne doit pas être considérée comme** une note « **automatique** » suite à une action. Le prestataire, en s'appuyant sur l'aide à la notation fournie dans l'état des lieux orga, devra ainsi s'assurer que la **progression proposée est réaliste pour chaque point de contrôle.**

Ref	Question	Score actuel	Score après plan d'actions
1	Qui est le responsable de la Sécurité des Systèmes d'Information au sein de votre organisation ?	0.5	0,8
2	A qui est rattaché le RSSI ?	0,2	0,6
3	Quelles sont les ressources en ETP (Equivalent Temps Plein) dédiées à la réalisation des activité de cybersécurité ? *(n'inclut pas les administrateurs des infrastructures)*	1	1
4	Avez-vous des ressources dédiées à la sécurité opérationnelle ?	0,4	0,9

Actions prioritaires : accompagnement à la mise en œuvre des mesures urgentes dans le pack initial et des packs relais

Lors de la construction du plan de sécurisation, le prestataire doit également **identifier quelles sont les 3 ou 4 actions prioritaires en termes de sécurisation du SI**, et sur lesquelles le bénéficiaire aurait éventuellement **besoin d'accompagnement.**

Le dispositif prévoit en effet un accompagnement de quelques jours pour aider le bénéficiaire lors du pack initial. Ce dernier peut également prétendre à un ou plusieurs pack relais co-financés.

Accompagnement à la mise en œuvre des mesures urgentes

Quelques jours sont le plus souvent prévus en fin de pack initial pour **accompagner les équipes du bénéficiaire à la mise en place des actions jugées urgentes**. Cette enveloppe de jours est notamment précisée dans le support d'initialisation.

Cet accompagnement sera essentiellement consacré à de la **sécurité opérationnelle pour corriger les vulnérabilités identifiées lors de l'état des lieux technique** (correction de configuration, fermeture de services inutiles, etc.)

Durant la phase de construction du plan de sécurisation, le prestataire doit donc identifier avec le bénéficiaire les chantiers sur lesquels il pourra **apporter l'expertise nécessaire à leur mise en œuvre rapide.**

Financement de packs relais par l'ANSSI

Le prestataire doit également commencer à **se projeter sur les packs relais** en se demandant sur **quels périmètres** le bénéficiaire pourrait en avoir le plus besoin.

Les packs relais sont des **travaux de sécurisation co-financés par l'ANSSI.** Ils sont **issus du plan de sécurisation** et correspondent aux **actions les plus prioritaires** pouvant idéalement être **menées dans les 12 mois** qui suivent l'obtention de la subvention. Les packs relais doivent favoriser les mesures **opérationnelles** et apporter une amélioration **concrète et rapide** du niveau de cybersécurité du bénéficiaire.

Chaque bénéficiaire peut prétendre au **financement de 2 ou 3 packs relais au maximum**, dans le respect du **plafond du financement accordé au bénéficiaire et de sa contribution en tant que co-financeur.**

Focus sur les mesures urgentes

Les vulnérabilités devant faire l'objet de mesures urgentes de correction sont caractérisées par : **une exploitation triviale et un impact important pour l'activité du bénéficiaire.**

Les bonnes pratiques à adopter :

- ✓ Les vulnérabilités devant faire l'objet de mesures urgentes de correction sont principalement issues de **l'état des lieux technique**
- ✓ La prise en compte des vulnérabilités identifiées dans les rapports SILENE et ADS est également un bon entrant
- ✓ Les actions identifiées suite à l'état des lieux organisationnel sont possibles mais moins fréquentes

Exemples de mesures urgentes

- **Application de correctifs de sécurité** pour pallier à une vulnérabilité importante (permettant par exemple une prise de contrôle immédiate sur des serveurs, ou un grand nombre de postes de travail depuis un accès réseau)
- **Durcissement d'une configuration, ou modification de privilèges** (qui, avant correction, permettent par exemple aisément de réaliser une élévation de privilège sur l'Active Directory)
- **Correction de règles de filtrages réseaux** qui mettraient en danger le SI interne (exposition sur internet d'une grande partie d'un SI par exemple)
- **Procédure de traitement des alertes sécurité**
- **Formalisation d'une politique de mot de passe**
- **Formalisation d'une checklist sécurité pour les projets**
- **Accompagnement à la mise en place d'un WSUS**

Les mesures urgentes sont à mettre en œuvre **au temps passé, sur un nombre limité de jours, défini a priori dans la proposition commerciale.**

Les actions correctives qui nécessiteraient plus de temps d'analyse et de réalisation **ne seront pas pertinentes dans ce cadre**. Par exemple :

- Les changements d'architecture
- La mise en place de cloisonnement

Focus sur le pack relais (1/3)

Une identification à anticiper

L'ambition est **de valider** le contenu des packs relais **lors des restitutions** afin de lancer ensuite ceux-ci **dans les meilleurs délais** pour ne pas perdre l'élan impulsé par le pack initial. Pour cela, les réflexions sur le contenu du/des pack(s) relais doivent **commencer dès les premiers travaux sur le plan de sécurisation**. De même, il sera important d'anticiper les échanges avec les prestataires terrains susceptibles de participer aux packs relais.

Des contenus variés

Lors de la construction du plan de sécurisation, le prestataire terrain et le bénéficiaire doivent identifier quelles sont **les 3 ou 4 actions prioritaires en termes de sécurisation du SI,** et sur lesquelles le bénéficiaire aurait besoin d'accompagnement afin de les sélectionner pour le ou les packs relais. Il peut s'agir de prestations intellectuelles ou d'acquisition de solutions, d'équipements et de services. Ces prestations devront apporter une amélioration **concrète et rapide** du niveau de cybersécurité.

Des travaux financés en partie par l'ANSSI

Le pack relais est co-financé par l'ANSSI dans la limite du montant total de la subvention et sous réserve que le bénéficiaire finance au moins 30% du coût total du pack relais.

Certains projets ne seront pas acceptés dans le cadre d'un pack relais :

- Projet intégrant des achats de composants « IT » courants (postes de travail, serveurs, licences OS, etc.) (DSI)
- Projet ne semblant pas permettre de produire des résultats rapides en matière de relance ou de sécurisation du socle numérique du bénéficiaire
- Projet déjà mis en œuvre ou engagé financièrement (pas de remboursement a posteriori)

Focus sur le pack relais (2/3)

Voici des exemples de packs relais possibles :

- Prestation de sécurisation de la messagerie email
- Acquisition d'une solution de sécurisation des annuaires (ex. Active Directory)
- Prestation d'accompagnement au déploiement d'une solution de sauvegarde sécurisée / Souscription à un service
- Sécurisation des différents composants (logiciels, matériels et processus) assurant l'administration du Datacenter
- Acquisition d'une solution de gestion de vulnérabilités
- Réalisation d'une campagne de Bug bounty
- Déploiement d'une solution de proxy réalisant des actions de sensibilisation en cas de refus de flux
- Optimisation de la configuration du pare-feu / Acquisition d'un Pare-feu ou d'un Pare-feu applicatif web
- Acquisition d'une solution de bastion d'administration
- Acquisition de licences d'un outil d'analyse de risques labellisé par l'ANSSI
- Actions de sensibilisations / formations complémentaires au pack initial
- Acquisition d'une solution industrialisée de tests de phishing
- Etude de cadrage relative à la définition d'une politique et d'une solution d'EDR / Souscription à un service d'EDR
- Réalisation d'une étude de segmentation du réseau
- Prestations de conseil accompagnant la mise en œuvre de projets opérationnels

Les packs relais doivent se concentrer sur quelques actions prioritaires, et se focaliser en particulier sur la **résolution de problématiques concrètes et opérationnelles de sécurisation du SI** (plutôt que de gouvernance, de résilience ou documentaires).

Les packs relais devront permettre en priorité de **renforcer la capacité à détecter et à bloquer en amont les menaces** plutôt que de développer les moyens de résilience suite aux sinistres.

Les packs relais peuvent être réalisés par **tout type de prestataire ou fournisseur de solutions cybersécurité**.

Focus sur le pack relais (3/3)

Voici des exemples de packs relais qui ne seraient très probablement pas validés (*et les raisons de leur non validation*) :

- Acquisition de produits et prestations d'accompagnement pour l'amélioration de la visioconférence (DR)
  - *Projet relevant d'un projet numérique devant assumer sa part cyber*
- Sécurisation des communications téléphoniques
  - *Projet relevant d'un projet numérique devant assumer sa part cyber*
- Projet de réduction de la dette technique
  - *Projet intégrant des achats de composants "IT" courants (Postes de travail, serveurs, licences OS, etc.)*
- Réalisation d'un BIA
  - *Projet lié à des problématiques de résilience*
- Formalisation d'une PSSI
  - *Projet lié à des problématiques de gouvernance*
- Formalisation d'une méthodologie d'ISP
  - *Projet lié à des problématiques de gouvernance*

Un fichier powerpoint permettant de synthétiser les packs relais envisagés est joint au fond documentaire.

Ce fichier sera utilisé pour permette à l'ANSSI de valider le contenu de ces packs relais **en amont de la finalisation du pack initial**, afin de permettre une poursuite des travaux dans les meilleurs délais au travers du déblocage de la seconde partie de la subvention dans le cadre de France relance **dès la fin du pack initial.**

Restitutions

Documents type fournis

- Restitution à la DSI et au RSSI type
- Restitution aux dirigeants type

Prérequis

- Synthèse des enjeux
- Synthèse de l'état des lieux organisationnel
- Synthèse de l'état des lieux technique
- Cartographie du SI
- Synthèse du plan de sécurisation

Proposition de pack relais

Livrable(s) de cette étape

- Restitution à la DSI et au RSSI *complétée*
- Restitution aux dirigeants *complétée*

Présentation des restitutions

Les restitutions clôturent la démarche et visent à présenter au bénéficiaire à la fois une **synthèse de l'existant** (missions, besoins de sécurité, sources de risques, niveau de maturité, …) et une **synthèse du plan de sécurisation et de ses apports en termes de cybersécurité.**

Avant les restitutions :

- Prévoir un **créneau avec le prestataire accompagnateur et le bénéficiaire** pour valider les 2 supports avant les restitutions.

Ce créneau permettra notamment de s'assurer que les restitutions ne provoqueront pas une éventuelle réaction négative des participants ayant un pouvoir de décision lors des présentations (vis-à-vis des constats, des plans d'actions ou de leurs budgets par exemple)

Première restitution : RSSI/DSI/Métiers

1

Objectif :

Présenter une synthèse de l'existant et du plan de sécurisation.

Valider le plan de sécurisation et le contenu des packs relais

Deuxième restitution : Dirigeants

2

Objectif :

Faire prendre conscience aux dirigeants que des menaces pèsent sur leur organisation et que leur soutien aux équipes SI et SSI est nécessaire à la bonne réalisation du plan de sécurisation.

Valider le contenu des packs relais

Focus sur la restitution au RSSI et au DSI

Première restitution : **RSSI/DSI/Métiers**

L'objectif de cette première restitution (1h30-2h) est de **présenter aux équipe SSI et SI et aux interlocuteurs métier qui ont participé à la démarche** une synthèse de l'existant et du plan de sécurisation.

Ainsi, lors de cette première synthèse réalisée sous la forme d'un document PowerPoint, le prestataire doit présenter :

- Une synthèse de **l'analyse du niveau de maturité** (Etats des lieux organisationnels et techniques) et une **comparaison aux autres organisations** tirée du benchmark de l'ANSSI sur le dispositif
- Les **principaux événements redoutés** et les **principaux besoins de sécurité associés**
- La **cartographie macroscopique des vulnérabilités du SI**
- Une restitution et validation du **plan de sécurisation** proposé
- Une liste des **chantiers prioritaires** pouvant faire l'objet de « pack relais » co-financés par l'ANSSI → Ces éléments devront faire **l'objet d'une validation lors de cette réunion**, en amont de la restitution auprès des dirigeants

Focus sur la restitution aux dirigeants (1/2)

Deuxième restitution : **Dirigeants**

La deuxième restitution (1h à 1h30), faite sous la forme d'un document PowerPoint plus court, doit quant à elle être pensée comme une vraie **synthèse managériale, orientée sensibilisation.**

Cette restitution doit faire l'objet d'une attention toute particulière car elle est **incontestablement l'étape la plus importante du pack initial.** En effet, le prestataire doit réussir à **convaincre les dirigeants que des risques cyber importants peuvent menacer leur organisation,** que la bonne mise en œuvre du plan de sécurisation **nécessite des moyens** et qu'il est **essentiel qu'ils soutiennent** ces efforts de renforcement de leur cyber sécurité**.**

Pour ce faire, le prestataire doit notamment présenter aux dirigeants :

- Une synthèse des **principaux enjeux** du bénéficiaire et des **menaces** le visant
- Une synthèse de l'Etat des lieux, une présentation de l'indice de cybersécurité et du **positionnement du bénéficiaire dans le benchmark**
- Une synthèse du plan de sécurisation et de son **impact sur les menaces** visant le bénéficiaire
- **Une proposition de contenu des packs relais pour validation (afin de permettre leur lancement rapide après cette restitution)**
- Une **sensibilisation aux bonnes pratiques** à mettre en œuvre par les équipes dirigeantes dans la prévention et la gestion des cyber attaques

Il sera essentiel de **préparer cette restitution pour garantir son impact.** Il s'agira donc notamment d'identifier en amont de la restitution **quels sont les éléments du support type qu'il sera pertinent de garder,** notamment en fonction de la **maturité et de l'implication historique des dirigeants sur les sujets cyber** (par exemple, il s'agira de réduire les slides et le temps réservé à la sensibilisation en début de présentation si les dirigeants sont déjà bien au fait des menaces cyber qui visent leur organisation)

Focus sur la restitution aux dirigeants (2/2)

Deuxième restitution :
Dirigeants

Répartition du temps de présentation entre les différentes phases pour une présentation d'une heure :

- Première partie de sensibilisation et sur la réglementation : 10 à 15 mn
- Présentation de l'état des lieux et de la feuille de route : 30 mn
- Seconde partie de sensibilisation se concentrant sur le rôle des dirigeants dans le cadre de la cybersécurité : 5 mn
- Temps pour l'échange : 10 à 15 mn

Quelques bonnes pratiques devront être appliquées dans le cadre de cette restitution :

- Présenter un niveau de **synthèse** approprié
- Réduire au maximum les **éléments de jargon liés à la SSI** ou les expliciter au maximum le cas échéant
- Mettre en avant **les éléments financiers** dans le cadre du plan d'action

Enfin, la présentation vise à **générer ou renforcer la relation de confiance** entre les équipes dirigeantes et l'équipe SSI. Il s'agira donc de régulièrement mettre en avant la qualité du travail réalisé par leurs équipes SI et SSI lors des derniers semestres (et ce même si les résultats de l'état des lieux révèlent une maturité faible) afin de s'assurer que les dirigeants leur accorderont la confiance nécessaire pour **accepter de s'engager** dans la réalisation du plan d'action et éventuellement y investir des ressources complémentaires

Sensibilisations ciblées

Documents type fournis

- Supports de sensibilisation types spécifiques aux populations ciblées

Prérequis

- Contexte métier et SI
- Etats des lieux technique et organisationnel

Livrable(s) de cette étape

- Supports de sensibilisation types spécifiques aux populations ciblées *adaptés*

Sensibilisations ciblées

En fin de démarche, des **sessions de sensibilisation SSI** pourront être réalisées.
Le **nombre de sessions** de sensibilisation, leur durée (entre 1h et 1 journée) ainsi que les **publics ciblés** sont définis en amont par le prestataire accompagnateur, et précisés dans les **supports d'initialisation.**

Ces sessions se composent le plus souvent d'une **présentation des menaces** visant le bénéficiaire ainsi que des **bonnes pratiques à mettre en œuvre.**

Par exemple, une session de sensibilisation des *équipes achats* permettra d'aborder les bonnes pratiques de sécurité dans les appels d'offre ou les renouvellements de contrats. Alors qu'une session de sensibilisation du Référent SSI permettra de former ce dernier sur certains sujets cyber afin de le faire monter en compétences.

Cible	Format / Durée	Contenu
Référent SI / Nouveau RSSI	Une journée / 2 demi-journées	Bases de la sécurité des systèmes d'informations, activités classiques d'un RSSI
Administrateurs SI	Une demi-journée (3h)	Bonnes pratiques d'administration du SI
Développeurs	Une journée / 2 demi-journées	Bonnes pratiques pour le développement d'applications **web**
Acheteurs	1h à 1h30	Bons réflexes à avoir & bonnes pratiques pour la sécurisation des prestations (clauses contractuelles, formation des équipes…)
Equipes RH	1h à 1h30	Bons réflexes à avoir au quotidien & focus sur la sensibilité des données traitées
SI industriels / biomédicaux	Une demi-journée (3h)	Bonnes pratiques d'administration et de maintien en conditions de sécurité des SI industriels/biomédicaux

Préparation des sensibilisations ciblées

Lors de la préparation des supports, **certaines slides devront être adaptées** (conservées ou supprimées) **selon le type de bénéficiaire** : collectivité territoriale, établissement de santé etc. afin de personnaliser la sensibilisation.

Par ailleurs, il faudra également revoir le contenu des supports pour s'assurer que les recommandations qu'ils contiennent sont **pertinentes avec l'existant au sein du bénéficiaire** (par exemple : la recommandation de se connecter via un VPN n'aura de sens que si le bénéficiaire dispose d'un VPN)

Stratégie de sensibilisation

Documents type fournis

Support d'animation de la stratégie de sensibilisation

Prérequis

/

Livrable(s) de cette étape

Stratégie de sensibilisation

Démarche proposée

La démarche proposée est constituée de 4 étapes présentées ci-dessous, traitées **lors de 2 réunions de travail**. L'essentiel sera, comme pour le plan de sécurisation, de viser une cible **réaliste vis-à-vis des capacités humaines et financières du bénéficiaire**. Il faudra par ailleurs envoyer le support en amont des réunions aux participants du bénéficiaire à la réflexion pour accélérer les travaux.

A traiter/initier lors de la **première** réunion

A finaliser/traiter lors de la **seconde** réunion

- **1 - Comprendre l'historique, les moyens et les attentes en termes de sensibilisation**
  - Identification des moyens humains et financiers alloués et/ou sur lesquels il sera possible de s'appuyer dans le cadre de la démarche (dispositifs RH, de communication…)
  - Compréhension des attentes concernant la sensibilisation
  - Identification des actions de sensibilisation déjà réalisées et des supports utilisés

- **2 - Identifier les familles de population au sein de l'organisation (métier, IT, fonction support, management, direction…) et déterminer celles devant être visées prioritairement**
  - Segmentation des populations au sein de l'organisation*
  - Définition de leur niveau de priorité (P1, P2, Non retenu)
    - Il sera ici essentiel de **s'assurer que le nombre de typologie de populations identifiées comme prioritaires reste limité** (pas plus de 3 à 4 P1 et de 3 à 4 P2) pour que l'étape suivante de la démarche soit maîtrisée

- **3 - Pour chaque population prioritaire identifiée, décliner une démarche type permettant de définir les moyens de la sensibiliser**
  - Formalisation de la fiche identité de la population ciblée (périmètre et niveau de maturité)
  - Définition des objectifs de sensibilisation de la population*
  - Détermination des activités et supports de sensibilisation à mettre en œuvre* et moyens humains et matériels associés

- **4 - Elaborer un planning prévisionnel**
  - Planification, par cible identifiée, des actions de sensibilisation
  - Validation d'un planning prévisionnel global*

* Des éléments types/exemples se trouvent en annexe du support d'animation pour accompagner à la réflexion

Pilotage : Rôle du prestataire accompagnateur dans le cadre d'un parcours

Le prestataire accompagnateur est en charge de :

A l'initialisation du pack initial

- **Prendre contact avec le prestataire terrain pour planifier et réaliser la réunion préparatoire en amont de la réunion d'initialisation**
- Prendre contact avec le bénéficiaire pour planifier et réaliser la réunion de rappel de la démarche en amont de la réunion d'initialisation
- **Participer à la réunion d'initialisation**

Pendant l'exécution du pack initial

- Réaliser un point d'étape avec le bénéficiaire à l'issue de l'état des lieux
- **Apporter un support méthodologique au prestataire terrain**
- **Remonter au fil de l'eau les points de vigilance et les points d'alerte, dont ceux communiqués par le prestataire terrain**

Lors de la rédaction du plan de sécurisation

- **Echanger avec le prestataire terrain sur une V0 du plan de sécurisation préalablement établi avec le bénéficiaire afin d'aboutir à une V1**
- **Participer aux échanges sur l'identification des packs relais puis les transmettre à l'ANSSI pour validation**
- **Participer à une pré restitution tripartite avec le prestataire terrain et le bénéficiaire**

A l'issue du pack initial

- Participer à la réunion de clôture avec le bénéficiaire après la restitution aux dirigeants
- Attester ou non la bonne réalisation du pack initial
- Transmettre et suivre la complétion du questionnaire de satisfaction
- Suivre le cadrage et l'engagement du pack relais

Pendant l'exécution du/des pack(s) relais

- Suivre le bon déroulement du/des pack(s) relais

Pilotage : Rôle du prestataire terrain vis-à-vis du pilotage et du prestataire accompagnateur

Le prestataire terrain doit :

Pendant toute l'exécution du pack initial

- **Faire appel** au prestataire accompagnateur pour toute question **méthodologique**
- Remonter au fil de l'eau **les points de vigilance et les points d'alerte** au prestataire accompagnateur (décalages projet, points de blocage, difficulté à converger sur la feuille de route, ….)

A l'initialisation du pack initial

- **Participer à la réunion de préparation** organisée par le prestataire accompagnateur (2h)
- **Organiser la réunion d'initialisation** avec le bénéficiaire et y convier le prestataire accompagnateur (1h)

A l'issue de l'état des lieux organisationnel

- **Partager les scores issus de l'état des lieux organisationnel** au prestataire accompagnateur pour le calcul de l'indice de cybersécurité

Lors de la rédaction du plan de sécurisation

- Organiser un point avec le prestataire accompagnateur afin de **revoir la V0 du plan de sécurisation** préalablement établi avec le bénéficiaire afin d'aboutir à une V1 (2h). Les éléments du plan d'actions seront communiqués **la veille de la réunion**
- Echanger avec le bénéficiaire sur les **actions à mettre en œuvre dans le cadre d'un pack relais**

A la restitution du pack initial

- Organiser une **pré-restitution tripartite** avec le prestataire accompagnateur et le bénéficiaire (1h). Le support de la réunion de restitution au RSSI et au DSI sera communiqué **la veille de la réunion**
- Intégrer le prestataire accompagnateur aux **réunions de restitution DSI** (2h) **puis DG** (1h)

Pilotage : Modalités de contact avec le prestataire accompagnateur

Destinataire du mail	Type d'information traité dans le mail	Règles de partage
Votre prestataire accompagnateur dédié	• ~~Demande de calcul de l'indice de~~ cybersécurité (dans un conteneur sécurisé) • Questions méthodologiques (sur le fond documentaire, …) • Remontée des points de vigilance et d'alerte (demandes du bénéficiaire hors cahier des charges, décalage du planning, indisponibilité des interlocuteurs côté bénéficiaire….) • Communication du support de restitution (dans un conteneur sécurisé)	1. Objet du mail : **[Parcours cyber] Nomclient Sujet** (Sujet au choix : Indice de cybersécurité ; Pilotage ; Question méthodologique ; Point de vigilance) 2. Mettre en copie l'adresse générique (en fonction de l'entreprise à laquelle appartient le prestataire accompagnateur) • francerelance@evabssi.com • accompagnateurs.ssi.fr@formind.fr • prestataireaccompagnateur.cyber.francerelance@wavestone.com
	• Organisation des différentes réunions auxquelles les prestataires accompagnateurs doivent être conviés (réunion de lancement,…) • Echanges concernant le plan de sécurisation	1. Objet du mail : **[Parcours cyber] Nomclient Sujet** (Sujet au choix : Planification réunion ; Plan d'action)