

Rapport d'évaluation de la maturité numérique *Etablissement de référence*

Bruce Banner – *Auditeur*

4 janvier 2021

Résumé

Ce rapport décrit le résultat de l'évaluation réalisée à *Etablissement de référence* en 2020. L'évaluation initiale a été contrôlée le 4 janvier 2021 par Bruce Banner. Cette évaluation repose sur un questionnaire établi conformément aux règles d'hygiène de l'ANSSI.

- Directeur de l'établissement : *Benjamin GRIMM*
- RSSI de l'établissement : *Donald BLAKE*

Rapport validé

Original signé

Ce document, réservé à votre seul usage interne, est émis en application du contrat convenu entre nous. Il a été établi sur la base des informations que vous nous avez préalablement communiquées, par référence à votre contexte et en tenant compte de vos éléments d'analyse. L'émetteur du présent document apporte tout le soin possible à la préparation des informations et des conclusions qui y sont présentées, à partir de notre méthodologie et de nos expertises. La décision de mettre en oeuvre ou non ces conclusions, ainsi que les modalités de mise en oeuvre relèvent de la seule responsabilité du lecteur.

Table des matières

| | | |
|----------|---|-----------|
| 1 | Analyse de l'évaluation pour l'année 2020 | 5 |
| 1.1 | Introduction | 5 |
| 1.1.1 | Le modèle PDCA et la roue de Deming | 5 |
| 1.1.2 | Le modèle PDCA appliqué au SMSI | 5 |
| 1.2 | Explications préliminaires | 6 |
| 1.2.1 | Mode de calcul des notes | 6 |
| 1.2.2 | Détails des cotations | 6 |
| 1.3 | Notes obtenues par l'établissement | 6 |
| 1.4 | Graphes de synthèses de l'établissement | 8 |
| 1.5 | Commentaires et conclusion | 9 |
| 1.5.1 | Commentaires de l'établissement | 9 |
| 1.5.2 | Conclusion des évaluateurs | 9 |
| 2 | Résultats de l'audit pour l'année 2020 | 10 |
| 2.1 | Sensibiliser et former | 10 |
| 2.1.1 | Former les équipes opérationnelles à la cybersécurité | 10 |
| 2.1.2 | Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique | 11 |
| 2.1.3 | Maîtriser les risques de l'infogérance | 12 |
| 2.2 | Connaître le système d'information | 13 |
| 2.2.1 | Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau | 13 |
| 2.2.2 | Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour | 15 |
| 2.2.3 | Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs | 16 |
| 2.2.4 | Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés | 18 |
| 2.3 | Authentifier et contrôler les accès | 18 |
| 2.3.1 | Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur | 18 |
| 2.3.2 | Attribuer les bons droits sur les ressources sensibles du système d'information | 19 |
| 2.3.3 | Définir et vérifier des règles de choix et de dimensionnement des mots de passe | 20 |
| 2.3.4 | Protéger les mots de passe stockés sur les systèmes | 21 |
| 2.3.5 | Changer les éléments d'authentification par défaut sur les équipements et services | 22 |
| 2.3.6 | Privilégier lorsque c'est possible une authentification forte | 22 |
| 2.4 | Sécuriser les postes de travail | 23 |
| 2.4.1 | Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique | 23 |
| 2.4.2 | Se protéger des menaces relatives à l'utilisation de supports amovibles | 24 |
| 2.4.3 | Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité | 25 |
| 2.4.4 | Activer et configurer le parefeu local des postes de travail | 26 |
| 2.4.5 | Chiffrer les données sensibles transmises par voie Internet | 26 |
| 2.5 | Sécuriser le réseau | 27 |
| 2.5.1 | Segmenter le réseau et mettre en place un cloisonnement entre ces zones | 27 |
| 2.5.2 | S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages | 27 |
| 2.5.3 | Utiliser des protocoles réseaux sécurisés dès qu'ils existent | 28 |
| 2.5.4 | Mettre en place une passerelle d'accès sécurisé à Internet | 29 |
| 2.5.5 | Cloisonner les services visibles depuis Internet du reste du système d'information | 30 |

| | | |
|----------|--|-----------|
| 2.5.6 | Protéger sa messagerie professionnelle | 31 |
| 2.5.7 | Sécuriser les interconnexions réseau dédiées avec les partenaires | 31 |
| 2.5.8 | Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques | 32 |
| 2.6 | Sécuriser l'administration | 33 |
| 2.6.1 | Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information | 33 |
| 2.6.2 | Utiliser un réseau dédié et cloisonné pour l'administration du système d'information | 33 |
| 2.6.3 | Limitier au strict besoin opérationnel les droits d'administration sur les postes de travail | 34 |
| 2.7 | Gérer le nomadisme | 35 |
| 2.7.1 | Prendre des mesures de sécurisation physique des terminaux nomades | 35 |
| 2.7.2 | Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable | 36 |
| 2.7.3 | Sécuriser la connexion réseau des postes utilisés en situation de nomadisme | 36 |
| 2.7.4 | Adopter des politiques de sécurité dédiées aux terminaux mobiles | 37 |
| 2.8 | Maintenir le système d'information à jour | 37 |
| 2.8.1 | Définir une politique de mise à jour des composants du système d'information | 37 |
| 2.8.2 | Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles | 38 |
| 2.9 | Superviser, auditer, réagir | 39 |
| 2.9.1 | Activer et configurer les journaux des composants les plus importants | 39 |
| 2.9.2 | Définir et appliquer une politique de sauvegarde des composants critiques | 40 |
| 2.9.3 | Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées | 41 |
| 2.9.4 | Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel | 41 |
| 2.9.5 | Définir une procédure de gestion des incidents de sécurité | 42 |
| 2.10 | Gérer la sécurité par les risques | 43 |
| 2.10.1 | Mener une analyse de risques formelle | 43 |
| A | Le SMSI | 44 |
| A.1 | Exigences générales | 44 |
| A.2 | Établissement et management du SMSI | 44 |
| A.2.1 | Établissement du SMSI | 44 |
| A.2.2 | Mise en œuvre et fonctionnement du SMSI | 45 |
| A.3 | Surveillance et réexamen du SMSI | 46 |
| A.4 | Mise à jour et amélioration du SMSI | 46 |

Rapport imprimé par l'établissement le 4 janvier 2021.

1. Analyse de l'évaluation pour l'année 2020

1.1. Introduction

1.1.1. Le modèle PDCA et la roue de Deming

La roue de Deming est une illustration de la méthode qualité PDCA (Plan-Do-Check-Act). Son nom vient du statisticien William Edwards Deming. Ce dernier n'a pas inventé le principe du PDCA, mais il l'a popularisé dans les années 50 en présentant cet outil au Nippon Keidanren.

La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux. Sa mise en place doit permettre d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service...

Plan Préparer, Planifier (ce que l'on va réaliser) ;

Do Développer, réaliser, mettre en œuvre ;

Check Contrôler, vérifier ;

Act Agir, réagir

1.1.2. Le modèle PDCA appliqué au SMSI

Appliqué au Système de Management de la Sécurité de l'Information, le PDCA se traduit selon le schéma suivant :

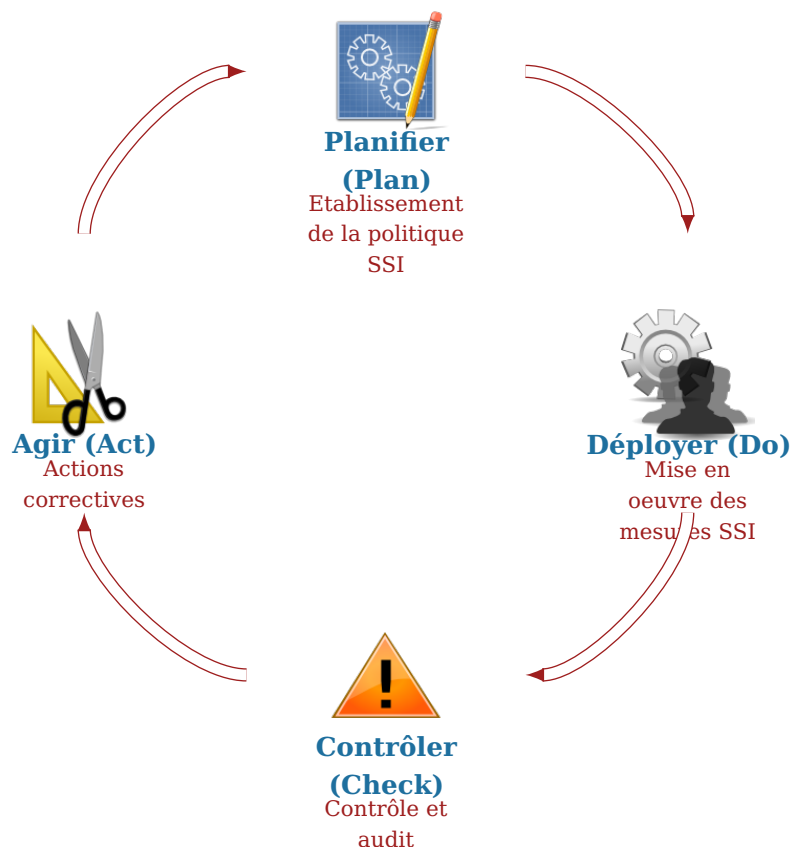


Figure 1 – Le PDCA appliqué au SMSI

Planifier Établir la politique, les objectifs, les processus et les procédures du SMSI relatives à la gestion du risque et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformément aux politiques et aux objectifs globaux de l'organisme ;

Déployer Mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures du SMSI ;

Contrôler Évaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique et rendre compte des résultats à la direction pour réexamen ;

Agir Entreprendre les actions correctives et préventives, sur la base des résultats de l'audit interne du SMSI et la revue de direction, ou d'autres informations pertinentes, pour une amélioration continue dudit système.

1.2. Explications préliminaires

1.2.1. Mode de calcul des notes

Chacune des questions possède une pondération permettant de les hiérarchiser. La note de chaque thème est calculée en réalisant une moyenne pondérée de ses questions. Les thèmes sont indépendants entre eux et possèdent tous une note représentative des problématiques qu'ils abordent.

Formule de calcul de la note de chaque thème :

$$N = \frac{\sum_{i=1}^n (P_Q \times E_Q)}{\sum_{i=1}^n P_{Q_i}}$$

Avec, N désignant la note finale du thème, P_Q la pondération de la question Q , E_Q la valeur de l'évaluation pour la question Q .

1.2.2. Détails des cotations

Pour chaque question, une cotation est définie. Il existe sept choix possible de cotation :

Non Applicable La règle est non applicable ou à fait l'objet d'une dérogation (à préciser dans le commentaire) ;

Inexistant et investissement important La disposition proposée n'est pas appliquée actuellement et ne le sera pas avant un délai important (mesure non planifiée, mesure nécessitant une étude préalable importante, mesure nécessitant un budget important, etc.) ;

Inexistant et investissement peu important La disposition proposée n'est pas appliquée actuellement, mais le sera rapidement, car sa mise en oeuvre est facile et/ou rapide ;

En cours et demande un ajustement La disposition proposée est en cours de réalisation (état d'avancement à 30% au minimum), mais des difficultés sont rencontrées et les plans prévus de réalisation doivent être modifiés ;

En cours La disposition proposée est en cours de réalisation (état d'avancement à 60% au minimum) et se déroule sans encombre ;

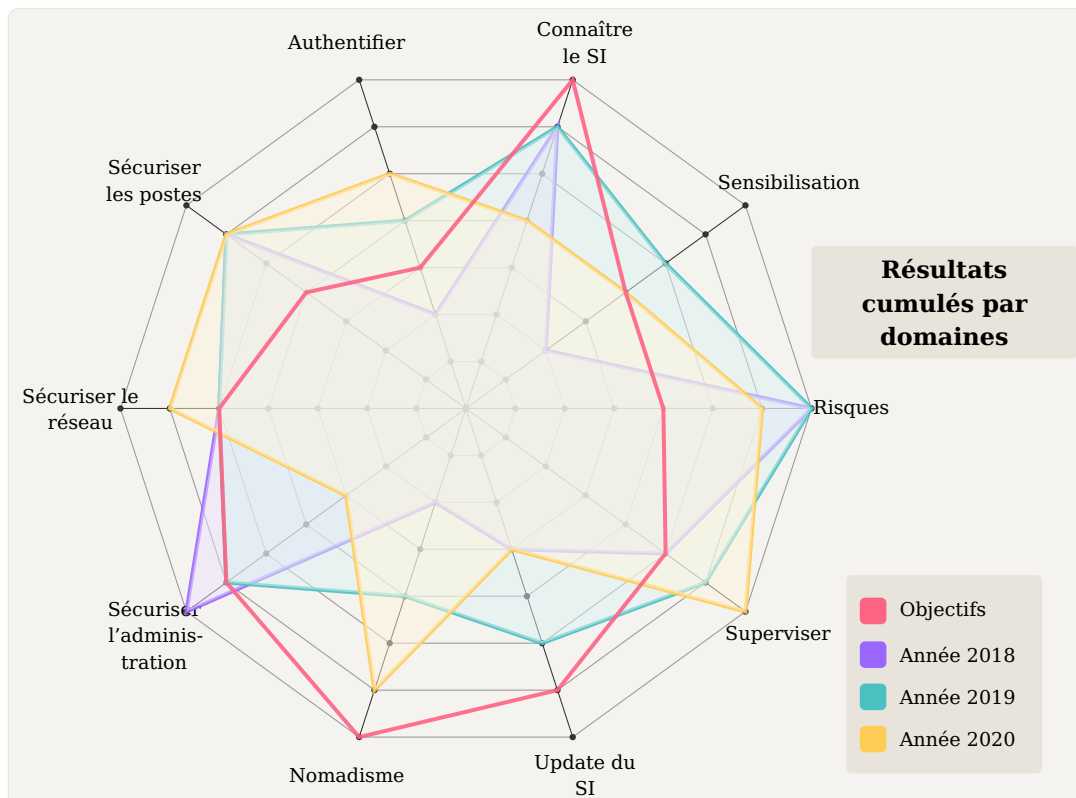
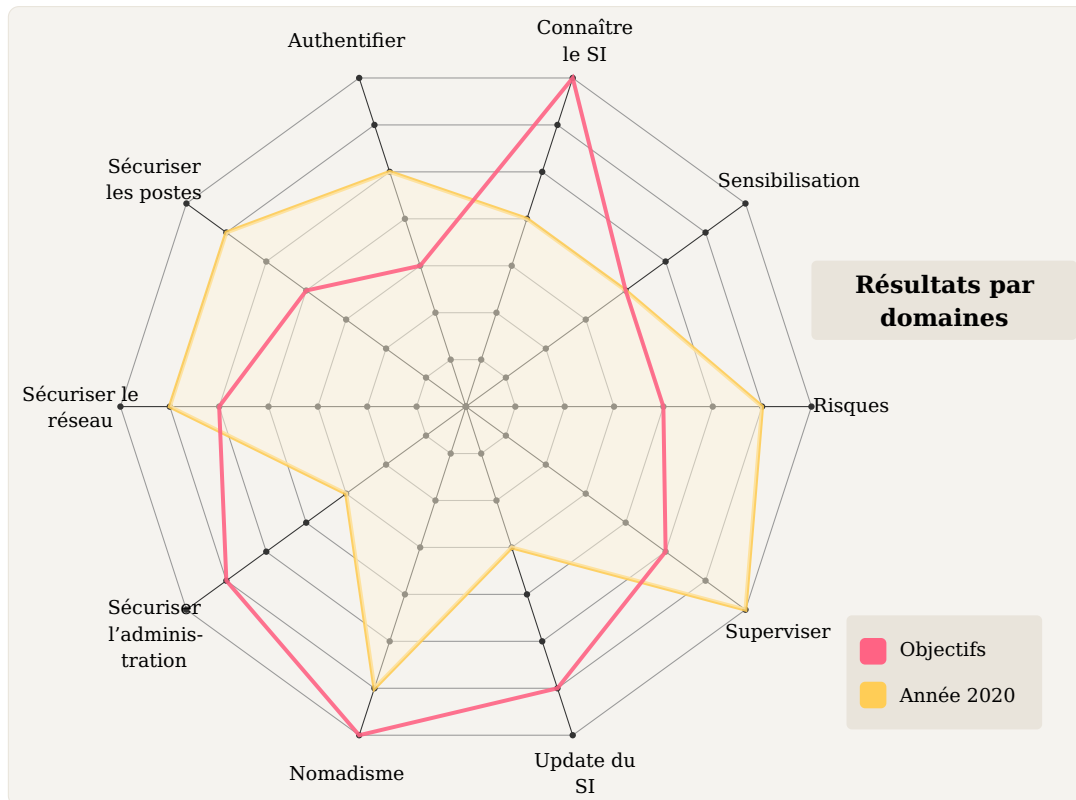
Existant et demande un ajustement La disposition est mise en place et il reste quelques ajustements à réaliser pour la rendre totalement opérationnelle (état d'avancement à 90% au minimum) ;

Opérationnel La disposition est opérationnelle et remplit entièrement les besoins demandés.

1.3. Notes obtenues par l'établissement

| Notes finales de l'établissement | | |
|----------------------------------|---------------------------------------|-------------|
| Établissement | Détail des notes | Note finale |
| Etablissement de référence | Sensibilisation → 12, 43/20 | 14, 05/20 |
| | Connaître le SI → 11, 63/20 | |
| | Authentifier → 13, 03/20 | |
| | Sécuriser les postes → 16, 80/20 | |
| | Sécuriser le réseau → 18, 20/20 | |
| | Sécuriser l'administration → 9, 71/20 | |
| | Nomadisme → 16, 54/20 | |
| | Update du SI → 7, 34/20 | |
| | Superviser → 18, 57/20 | |
| | Risques → 16, 20/20 | |
| | | |

1.4. Graphes de synthèses de l'établissement



1.5. Commentaires et conclusion

1.5.1. Commentaires de l'établissement

En progression par rapport à 2019.

1.5.2. Conclusion des évaluateurs


Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

2. Résultats de l'audit pour l'année 2020

2.1. Sensibiliser et former

2.1.1. Former les équipes opérationnelles à la cybersécurité


Question n°1.1.1 Un plan de formation à la cybersécurité au profit des équipes opérationnelles existe et est budgétisé.

| Évaluation de l'établissement | Commentaire |
|--|-------------------------------------|
|  En cours (5/7) | Le plan de formation est à l'étude. |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°1.1.2 Le plan de formation des équipes opérationnelles est spécifique à chaque métier (administrateur, chef de projet, développeur,...)

| Évaluation de l'établissement | Commentaire |
|---|--------------|
|  Existant et demande un ajustement (6/7) | toto tata |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°1.1.3 La formation à la cybersécurité des équipes opérationnelles couvre le volet juridique.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°1.1.4 La formation à la cybersécurité des équipes opérationnelles détaille les principaux risques et menaces.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°1.1.5 La formation à la cybersécurité des équipes opérationnelles couvre les notions de maintien en condition de sécurité.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°1.1.6 La formation à la cybersécurité des équipes opérationnelles détaille les principes et règles de l'authentification et du contrôle d'accès.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°1.1.7 La formation à la cybersécurité des équipes opérationnelle traite du paramétrage et du durcissement des systèmes d'information.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°1.1.8 La formation à la cybersécurité des équipes opérationnelle traite de l'architecture sécurisée des systèmes et des réseaux.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°1.1.9 Les contrats d'externalisation et d'infogérance contiennent une clause garantissant la formation à la cybersécurité du personnel.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.1.2. Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique


Question n°1.2.1 Un plan de sensibilisation à la cybersécurité au profit des utilisateurs existe et est budgétisé.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Le plan de sensibilisation des utilisateurs est intégré au dossier de cybersécurité de l'entité. | |


Question n°1.2.2 La sensibilisation à la cybersécurité des utilisateurs est systématique et renouvelée régulièrement.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Il est recommandé de sensibiliser les utilisateurs lors de leur arrivée dans l'entité et de renouveler cette sensibilisation tous les 3 ans. La liste des agents sensibilisés à la cybersécurité est conservée dans un registre dédié. Ce registre est intégré au dossier de cybersécurité de l'entité. | |


Question n°1.2.3 La sensibilisation à la cybersécurité des utilisateurs détaille les règles de la politique de sécurité des systèmes d'informations.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°1.2.4 L'entité a élaboré une charte des moyens informatiques précisant les règles et consignes que doivent respecter les utilisateurs.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| L'entité peut s'inspirer du guide d'élaboration publié par l'ANSSI (https://bit.ly/2sy5N7e). La charte des moyens informatiques doit être présentée au CHSCT et intégrée au règlement intérieur de l'entité. | |

Question n°1.2.5 Chaque utilisateur signe la charte des moyens informatiques.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| La signature de la charte des moyens informatiques est conservées dans un registre dédié. Ce registre est intégré au dossier de cybersécurité de l'entité. | |

2.1.3. Maîtriser les risques de l'infogérance


Question n°1.3.1 Une liste d'exigences précises a été contractualisée avec le prestataires.

| Évaluation de l'établissement | Commentaire |
|--|------------------------------|
|  Inexistant et investissement peu important (3/7) | Difficile à mettre en oeuvre |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| L'entité peut s'inspirer du guide sur l'externalisation publié par l'ANSSI (https://bit.ly/2V8e4It) | |


Question n°1.3.2 La liste d'exigences fixe les modalités de réversibilités du contrat.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | OK |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°1.3.3 La liste d'exigence détaille les modalités de réalisation d'audits.

| Évaluation de l'établissement | Commentaire |
|--|---|
|  Inexistant et investissement peu important (3/7) | Fait pour la majorité des prestataires. |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°1.3.4 La liste d'exigence détaille les modalités de sauvegarde et de restitution des données dans un format ouvert normalisé.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°1.3.5 La liste d'exigence détaille la mise en oeuvre du maintien à niveau de la sécurité dans le temps.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°1.3.6 Pour chaque contrat d'externalisation, le prestataire a fourni un plan d'assurance sécurité (PAS).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


2.2. Connaître le système d'information

2.2.1. Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau


Question n°2.1.1 La liste des données sensibles existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette liste est intégrée au dossier de cybersécurité de l'entité. | |


Question n°2.1.2 La liste des données sensibles précise sur quels composants elles sont stockées ou traitées.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.1.3 Les composants traitants ou hébergeant des données sensibles sont considérés comme critiques.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.1.4 Des mesures de sécurité spécifiques sont décrites pour les composants critiques (sauvegarde, mise à jour, contrôle d'accès)

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.1.5 Un schéma du réseau existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Le schéma du réseau est intégré au dossier de cybersécurité de l'entité. | |


Question n°2.1.6 Le schéma du réseau précise le positionnement des équipements réseaux et de sécurité.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.1.7 Le schéma du réseau identifie les points d'interconnexion avec Internet et avec les partenaires.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.1.8 Le schéma du réseau détaille l'emplacement des composants critiques.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°2.1.9 Le schéma du réseau détaille le plan d'adressage IP.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°2.1.10 Le schéma du réseau est considéré comme une donnée sensible.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

2.2.2. Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour


Question n°2.2.1 La liste des comptes à privilèges existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | test |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°2.2.2 La liste des comptes à privilèges référence les utilisateurs ayant un compte administrateur sur le système d'information.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°2.2.3 La liste des comptes à privilèges référence les utilisateurs ayant suffisamment de droits pour accéder aux données des responsables.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.2.4 La liste des comptes à privilèges référence les utilisateurs utilisant un poste non administré par le service informatique.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°2.2.5 La revue périodique des droits d'accès au système d'information est effectuée régulièrement.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°2.2.6 La revue périodique des droits d'accès au système d'information permet de supprimer les comptes obsolètes.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.2.3. Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs


Question n°2.3.1 Une procédure d'arrivée des utilisateurs existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|------------------|
|  En cours et demande un ajustement (4/7) | Projet en cours. |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette procédure est intégrée au dossier de cybersécurité de l'entité. | |


Question n°2.3.2 La procédure d'arrivée précise les modalités de création des comptes et des boîtes de messagerie.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.3.3 La procédure d'arrivée précise les modalités d'affectation des équipements informatiques (ordinateur, smartphone, tablette,...).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.3.4 La procédure de d'arrivée est régulièrement mise à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°2.3.5 Une procédure de départ des utilisateurs existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°2.3.6 La procédure de départ précise les modalités de fermeture des comptes et des boîtes de messagerie.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°2.3.7 La procédure de départ précise les modalités de restitution des équipements informatiques (ordinateur, smartphone, tablette,...).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°2.3.8 La procédure de départ est régulièrement mise à jour.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.2.4. Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés

Question n°2.4.1 Une politique fixant les règles d'usage des équipements personnels existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement important (2/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette politique est intégrée au dossier de cybersécurité de l'entité. | |


Question n°2.4.2 Une politique fixant les règles d'usage des équipements prestataires et visiteurs externes existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette politique est intégrée au dossier de cybersécurité de l'entité. | |

Question n°2.4.3 Un réseau WiFi dédié aux visiteurs existe.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement important (2/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°2.4.4 Des mesures techniques (802.1x) sont en place pour authentifier les postes de travail.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


2.3. Authentifier et contrôler les accès

2.3.1. Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur


Question n°3.1.1 Une politique de gestion des comptes existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°3.1.2 Chaque utilisateur dispose d'un compte d'accès au système d'information personnel et nominatif.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°3.1.3 Chaque administrateur du système d'information dispose d'un compte d'administration nominatif différent de son compte d'utilisateur.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°3.1.4 Les comptes d'administration sont exclusivement dédié aux opérations d'administration du système d'information.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°3.1.5 Les comptes d'administration sont utilisée sur des environnements dédiés à l'administration.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°3.1.6 Les actions d'administrations sont journalisées.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.3.2. Attribuer les bons droits sur les ressources sensibles du système d'information


Question n°3.2.1 Une liste des ressources sensibles existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette liste est intégrée au dossier de cybersécurité de l'entité. | |


Question n°3.2.2 Pour chaque ressource, la liste des ressources sensibles précise quelle population peut y avoir accès.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°3.2.3 Les accès aux ressources sensibles sont journalisées.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°3.2.4 Une revue régulière des droits d'accès aux ressources sensibles est effectuée.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

2.3.3. Définir et vérifier des règles de choix et de dimensionnement des mots de passe


Question n°3.3.1 Une politique des mots de passe existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°3.3.2 La longueur minimale des mots de passe est définie.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°3.3.3 Le niveau de complexité des mots de passe est défini.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Les mots de passe doivent contenir, au minimum, un mélange de lettres minuscules, majuscules et chiffres. | |


Question n°3.3.4 La durée de validité des mots de passe est définie.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°3.3.5 Les modalités de blocage des comptes à l'issue de plusieurs échecs de connexion sont définies.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°3.3.6 Les connexions anonymes sont désactivées.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°3.3.7 La robustesse des mots de passe est auditée.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Pour cela l'entité peut faire appel à un prestataire spécialisé dans la cadre d'un test technique. | |

2.3.4. Protéger les mots de passe stockés sur les systèmes

Question n°3.4.1 L'entité met à disposition de ses utilisateurs un mécanisme de coffre-fort numérique pour protéger leurs mots de passe.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Le logiciel opensource et gratuit KeePass (https://bit.ly/2CmCyVY) est une solution recommandée pour cet usage. | |

Question n°3.4.2 Les mots de passe des comptes génériques sont obligatoirement stockés dans un coffre-fort numérique.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

2.3.5. Changer les éléments d'authentification par défaut sur les équipements et services


Question n°3.5.1 Les éléments d'authentification par défaut des composants du système d'information sont modifiés dès leur installation.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°3.5.2 Les éléments d'authentification des composants du système d'information sont stockés dans un coffre-fort numérique.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°3.5.3 Lorsque les éléments d'authentification par défaut des composants du système d'information ne peuvent pas être modifiés, ces composants font l'objet de mesures de sécurité renforcées.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.3.6. Privilégier lorsque c'est possible une authentification forte


Question n°3.6.1 L'entité met en oeuvre une authentification forte pour ses systèmes sensibles.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°3.6.2 L'entité met en oeuvre une authentification forte pour ses comptes d'administration.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°3.6.3 L'entité met en oeuvre une authentification forte pour l'ensemble de ses utilisateurs.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


2.4. Sécuriser les postes de travail

2.4.1. Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique


Question n°4.1.1 Une politique de sécurisation des postes existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement important (2/7) | OK |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette politique est intégrée au dossier de cybersécurité de l'entité. | |


Question n°4.1.2 Une liste d'applications autorisées sur les postes de travail existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.1.3 Une liste d'applications autorisées sur les smartphones et tablettes existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette liste est intégrée au dossier de cybersécurité de l'entité. | |


Question n°4.1.4 Une liste des modules autorisés sur les navigateurs web existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette liste est intégrée au dossier de cybersécurité de l'entité. | |


Question n°4.1.5 Les postes utilisateurs sont dotés d'un pare-feu local.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Non applicable (1/7) | toto |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°4.1.6 Les postes des utilisateurs sont dotés d'un antivirus à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°4.1.7 Les disques durs des postes des utilisateurs sont chiffrés.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.1.8 Les espaces de stockages des smartphones et tablettes sont chiffrés.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | test |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.1.9 Les fonctions d'exécution automatique (autorun) sont désactivées.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.4.2. Se protéger des menaces relatives à l'utilisation de supports amovibles


Question n°4.2.1 Le branchement de périphériques amovibles inconnus est interdit.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°4.2.2 Une solution permettant d'interdire l'exécution de programme sur les périphériques amovibles est mise en oeuvre.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.2.3 Le rechargement électrique des smartphones et tablettes est interdit sur les postes utilisateurs.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.2.4 Les supports amovibles ayant contenus des informations sensibles sont détruit en fin de vie.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.4.3. Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité


Question n°4.3.1 L'entité met en oeuvre un outil de gestion centralisée de type Active Directory.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°4.3.2 L'ensemble des postes de travail est intégré dans l'outil de gestion centralisé.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°4.3.3 L'ensemble des serveur est intégré dans l'outil de gestion centralisé.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.3.4 Une politique de durcissement des postes de travail est définie et appliquée via l'outils de gestion centralisé.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.3.5 Une politique de durcissement des serveurs est définie et appliquée via l'outils de gestion centralisé.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.4.4. Activer et configurer le parefeu local des postes de travail


Question n°4.4.1 Un pare-feu est activé sur les postes de travail.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.4.2 La liste des flux réseaux autorisés existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.4.3 Seuls les ports correspondants aux flux autorisés sont ouverts sur les postes de travail.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.4.4 Les tentatives de connexion sur les ports bloqués par les pare-feu des postes de travail sont journalisées.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | v |
| Commentaire évaluateurs | |
| Avis conforme | |

2.4.5. Chiffrer les données sensibles transmises par voie Internet


Question n°4.5.1 Les emails transitant via Internet sont transmis en utilisant des protocoles assurant le chiffrement (IMPAS, POPS, SMTPS).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°4.5.2 Les données transitant via Internet sont transmises en utilisant des protocoles assurant le chiffrement (HTTPS).

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°4.5.3 Les données sensibles sont chiffrées avant transmission via Internet.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


2.5. Sécuriser le réseau

2.5.1. Segmenter le réseau et mettre en place un cloisonnement entre ces zones


Question n°5.1.1 Le réseau de l'entité est segmenté en plusieurs zones matérialisées par des VLAN spécifiques.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.1.2 Un pare-feu assure le filtrage des flux entre les différentes zones du réseau.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.1.3 Un segment du réseau est spécifiquement dédié aux tâches d'administration.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.2. S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages


Question n°5.2.1 Le réseau Wi-Fi met en oeuvre un chiffrement des flux robuste (mode WPA2 avec AES CCMP).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.2.2 Le mot de passe par défaut des points d'accès Wi-Fi est changé lors de l'installation.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.2.3 L'authentification des équipements au réseau Wi-Fi se fait par certificat délivré par une infrastructure de gestion des clefs centralisée.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.2.4 Si l'authentification des équipements au réseau Wi-Fi se fait par mot de passe, celui-ci est robuste et changé régulièrement.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.2.5 Le réseau Wi-Fi est placé dans un VLAN distinct.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.2.6 Le réseau Wi-Fi dédié aux terminaux personnels ou visiteurs est séparé du réseau Wi-Fi des terminaux de l'entité (SSID et VLAN différents).


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.3. Utiliser des protocoles réseaux sécurisés dès qu'ils existent


Question n°5.3.1 Sur les serveurs Web de l'entité, le protocole HTTP est désactivé au profit de HTTPS.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.3.2 Sur les serveurs de messagerie de l'entité, les protocoles IMAP, POP3 et SMTP sont désactivés au profit de IMAPS, POP3S et SMTPS.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.3.3 Sur les serveurs de transfert de fichiers de l'entité, le protocole FTP est désactivé au profit de FTPS ou SFTP.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.3.4 Les protocoles TELNET et RLOGIN sont désactivés au profit de SSH.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.3.5 L'implémentation de TLS sur les serveurs de l'entité n'autorise que les versions 1.2 et 1.3 du protocole.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.4. Mettre en place une passerelle d'accès sécurisé à Internet


Question n°5.4.1 L'accès à Internet se fait au travers d'un proxy authentifiant (type Alcasar - www.alcasar.net)

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.4.2 Le proxy d'accès à Internet comporte une fonctionnalité de filtrages des flux réseaux (pare-feu).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.4.3 Le proxy d'accès à Internet comporte une fonctionnalité d'analyse anti-virale.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.4.4 Le proxy d'accès à Internet comporte une fonctionnalité de filtrages des URLs.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.4.5 Le proxy d'accès à Internet conserve les journaux d'activité des usagers conformément à la loi française.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.4.6 Un équipement de détection d'intrusion est déployé au point d'interconnexion entre le réseau de l'entité et internet.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.5. Cloisonner les services visibles depuis Internet du reste du système d'information


Question n°5.5.1 Dans le cas d'un hébergement interne de services accessibles sur internet, ces services sont isolés des autres systèmes d'information de l'entité.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.5.2 Dans le cas d'un hébergement interne de services accessibles sur internet, les flux liés à ces services sont filtrés (pare-feu).

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.5.3 Dans le cas d'un hébergement interne de services accessibles sur internet, les flux entrants passent par un serveur mandataire (proxy).

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.5.4 Dans le cas d'un hébergement externe, l'entité s'assure que son prestataire est conforme à ses exigences de sécurité (plan d'assurance sécurité).


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.6. Protéger sa messagerie professionnelle


Question n°5.6.1 La redirection de messages professionnels vers une messagerie personnelle est interdite.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.6.2 Afin de se prémunir des escroqueries aux faux ordres de virement, des mesures organisationnelles sont décrites et appliquées.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.6.3 L'entité dispose d'un système d'analyse antivirus des boîtes de messagerie des utilisateurs.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.6.4 L'entité dispose d'un service anti-spam.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.7. Sécuriser les interconnexions réseau dédiées avec les partenaires


Question n°5.7.1 Les interconnexions réseaux avec une entité externe se font au travers d'un réseau privé virtuel de site à site (VPN).

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.7.2 Les réseaux privés virtuels (VPN) mis en oeuvre utilisent le standard IPSEC.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.7.3 Un filtrage IP à l'aide d'un pare-feu est mis place au plus près de l'entrée des flux VPN sur le réseau de l'entité.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.7.4 La matrice des flux (entrants et sortants) circulant au travers du VPN existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.7.5 Un point de contact à jour chez le partenaire est identifié pour pouvoir réagir en cas d'incident de sécurité.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.5.8. Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques


Question n°5.8.1 Les accès aux salles serveurs et aux locaux techniques sont contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.8.2 Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont interdit.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.8.3 Une revue des droits d'accès est réalisée régulièrement afin d'identifier les accès non autorisés.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°5.8.4 Lors du départ d'un collaborateur ou d'un changement de prestataire ses droits d'accès sont supprimés.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°5.8.5 Les prises réseau se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) sont désactivées.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


2.6. Sécuriser l'administration

2.6.1. Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information


Question n°6.1.1 Les postes utilisés pour l'administration des systèmes d'information de l'entité sont physiquement déconnecté d'internet.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| L'entité peut s'inspirer des recommandations de l'ANSSI (https://bit.ly/2vPE8O8). | |

Question n°6.1.2 Les administrateurs de l'entité disposent d'un deuxième poste de travail pour les activités hors administration.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°6.1.3 Les mises à jour des équipements administrés se font via une zone d'échange sécurisée ou en mode déconnecté (via un support amovible).


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

2.6.2. Utiliser un réseau dédié et cloisonné pour l'administration du système d'information


Question n°6.2.1 L'entité utilise un réseau dédié aux activités d'administration de ses systèmes d'information.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| L'entité peut s'inspirer des recommandations de l'ANSSI (https://bit.ly/2vPE8O8). | |

Question n°6.2.2 L'entité met en oeuvre un cloisonnement logique ou physique de son réseau d'administration.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°6.2.3 Dans le cas d'un cloisonnement logique, un filtrage IP (pare-feu) contrôle les flux réseaux.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

2.6.3. Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail


Question n°6.3.1 Par défaut, les utilisateurs ne dispose pas de privilèges d'administration sur leur poste de travail.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°6.3.2 L'entité met en oeuvre un magasin d'applications validées du point de vue de la sécurité.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°6.3.3 Seuls les agent chargés de l'administration des postes disposent de ces droits lors de leurs interventions.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  En cours et demande un ajustement (4/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


Question n°6.3.4 Si une délégation de privilèges sur un poste de travail est nécessaire elle est tracée, limitée dans le temps et retirée à échéance.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


2.7. Gérer le nomadisme

2.7.1. Prendre des mesures de sécurisation physique des terminaux nomades


Question n°7.1.1 Les utilisateurs sont sensibilisés aux risques spécifiques liés aux équipements informatiques lors d'un déplacement.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°7.1.2 Les terminaux nomades de l'entité sont équipés d'un filtre de confidentialité.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°7.1.3 Les terminaux nomades de l'entité ne portent pas de signe distinctifs liés à l'entité.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.7.2. Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable

Question n°7.2.1 Les données stockées sur supports amovibles (disques durs externes, clefs USB) de l'entité sont chiffrées.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°7.2.2 Les supports de stockages des terminaux nomades (ordinateurs, tablettes, smartphones) de l'entité sont chiffrés.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.7.3. Sécuriser la connexion réseau des postes utilisés en situation de nomadisme


Question n°7.3.1 L'entité met en oeuvre un réseau privé virtuel (VPN) entre son système d'information et les terminaux nomades.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°7.3.2 Le VPN à destination des terminaux nomades utilise le standard IPSEC.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°7.3.3 Le tunnel VPN est automatiquement activé et non débrayable dès que le terminal est en situation de nomadisme.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°7.3.4 Une procédure de révocation identifiants de connexion en cas de perte de vol existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°7.3.5 Une plainte est systématiquement déposée en cas de vol d'un terminal nomade.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°7.3.6 L'entité met en oeuvre un mécanisme d'authentification forte pour les ordinateurs nomades. La démarche est formalisée dans une procédure interne à l'entité.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.7.4. Adopter des politiques de sécurité dédiées aux terminaux mobiles


Question n°7.4.1 L'entité met en oeuvre une solution de gestion centralisée de sa flotte de terminaux nomades.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°7.4.2 La configuration de sécurité des terminaux nomades est homogène.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°7.4.3 L'entité déploie un magasin d'applications limitant l'accès à des applications validées du point de vue de la sécurité.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


2.8. Maintenir le système d'information à jour

2.8.1. Définir une politique de mise à jour des composants du système d'information


Question n°8.1.1 L'entité dispose d'un dispositif de veille concernant les vulnérabilités et les mises à jours des composants de son système d'information.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement important (2/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Le centre gouvernemental de veille, d'alerte et de réponses aux attaques informatiques fournit gratuitement cette prestation (https://www.cert.ssi.gouv.fr/) | |


Question n°8.1.2 Une procédure de mise à jour des composants du système d'information existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Cette procédure est intégrée au dossier de cybersécurité de l'entité. | |

Question n°8.1.3 La procédure de mise à jour des composants du SI précise les sources d'information relatives à la publication des mises à jour.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement important (2/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°8.1.4 La procédure de mise à jour des composants du SI précise les outils utilisés pour déployer les correctifs de sécurité.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

2.8.2. Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles


Question n°8.2.1 L'entité assure un suivi des mises à jour et des dates de fin de support des logiciels.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement important (2/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°8.2.2 L'entité dispose d'un plan de renouvellement des composants matériels et logiciels obsolètes.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |

Question n°8.2.3 Les contrats avec les prestataires et fournisseurs intègrent des clauses garantissant le suivi des correctifs de sécurité et la gestion des obsolescences

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Inexistant et investissement peu important (3/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |
| Recommandations | |
| Néant | |


2.9. Superviser, auditer, réagir

2.9.1. Activer et configurer les journaux des composants les plus importants


Question n°9.1.1 Les journaux des pare-feu sont activés et intègrent notamment la liste des paquets bloqués.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.1.2 Les journaux des applications métiers sont activés et contiennent notamment les informations d'authentifications et d'autorisations (échecs et succès).

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.1.3 Les journaux des systèmes d'exploitation des postes de travail sont activés et contiennent notamment les informations d'authentifications et d'autorisations (échecs et succès).

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.1.4 L'entité dispose d'un serveur de temps (NTP) utilisé pour synchroniser les horloges des composants critiques du son système d'information.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.1.5 L'entité dispose d'une collecte centralisée des journaux d'activités des composants critiques de son système d'information.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.9.2. Définir et appliquer une politique de sauvegarde des composants critiques


Question n°9.2.1 Une politique de sauvegarde existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.2.2 La politique de sauvegarde précise la liste des données jugées vitales pour l'entité et les serveurs concernés.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.2.3 La politique de sauvegarde précise le type et la fréquence des sauvegardes.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.2.4 La politique de sauvegarde précise la procédure d'administration et d'exécution des sauvegardes.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.2.5 La politique de sauvegarde précise les procédures de test et de restauration.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.2.6 Un exercice de restauration des données est planifié au moins une fois par an.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.9.3. Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées


Question n°9.3.1 Un audit interne de la sécurité du système d'information est réalisé au moins une fois par an.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.3.2 Un audit externe de la sécurité du système d'information est réalisé régulièrement.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.3.3 Les actions correctives, identifiées lors des audits internes et externes, sont planifiées et des points de suivi organisés à intervalles réguliers.


| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

2.9.4. Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel

Question n°9.4.1 L'entité a formellement désigné un référent en sécurité des systèmes d'information.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.4.2 Le référent en sécurité des systèmes d'information dispose d'une lettre de mission validée par la direction de l'entité.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.4.3 Le référent en sécurité des systèmes d'information est connu de tous les utilisateurs.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.4.4 Le référent en sécurité des systèmes d'information est en charge de la définition des règles de sécurité et de la vérification de leur application.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.4.5 Le référent en sécurité des systèmes d'information est en charge de la sensibilisation des utilisateurs.


| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

2.9.5. Définir une procédure de gestion des incidents de sécurité


Question n°9.5.1 Une procédure de gestion des incidents de sécurité existe et est à jour.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.5.2 Le référent en sécurité des systèmes d'information centralise et traite les incidents de sécurité.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.5.3 La procédure de gestion des incidents de sécurité impose la déconnexion du réseau du composant concerné.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.5.4 La procédure de gestion des incidents de sécurité impose le maintien sous tension du composant concerné.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.5.5 La procédure de gestion des incidents de sécurité fixe les modalités d'information de la hiérarchie et du référent en sécurité des systèmes d'information.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°9.5.6 La procédure de gestion des incidents de sécurité précise les modalités de collecte des informations sur le composant concerné.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


Question n°9.5.7 La procédure de gestion des incidents de sécurité précise les modalités de plainte auprès du service judiciaire compétent.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  Opérationnel (7/7) | RAS |
| Commentaire évaluateurs | |
| Avis conforme | |


2.10. Gérer la sécurité par les risques

2.10.1. Mener une analyse de risques formelle


Question n°10.1.1 L'entité met en oeuvre une démarche d'analyse des risques informationnels (EBIOS).

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°10.1.2 Une analyse des risques est réalisée pour chaque système d'information critique de l'entité.

| Évaluation de l'établissement | Commentaire |
|--|-------------|
|  En cours (5/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

Question n°10.1.3 L'analyse des risques permet d'exprimer les besoins de sécurité, d'identifier les objectifs de sécurité et de déterminer les exigences de sécurité.

| Évaluation de l'établissement | Commentaire |
|---|-------------|
|  Existant et demande un ajustement (6/7) | Néant |
| Commentaire évaluateurs | |
| Avis conforme | |

A. Le SMSI

A.1. Exigences générales

L'établissement doit établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI documenté dans le contexte des activités d'ensemble de l'établissement et des risques auxquels elles sont confrontées. Le processus utilisé est basé sur le modèle PDCA.

A.2. Établissement et management du SMSI

A.2.1. Établissement du SMSI

L'organisme doit effectuer les tâches suivantes :

1. définir le domaine d'application et les limites du SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, de sa technologie, ainsi que des détails et de la justification de toutes exclusions du domaine d'application ;
2. définir une politique pour le SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, et de sa technologie, qui :
 - (a) inclut un cadre pour fixer les objectifs et indiquer une orientation générale et des principes d'action concernant la sécurité de l'information ;
 - (b) tient compte des exigences liées à l'activité et des exigences légales ou réglementaires, ainsi que des obligations de sécurité contractuelles ;
 - (c) s'aligne sur le contexte de management du risque stratégique auquel est exposé l'organisme, dans lequel se dérouleront l'établissement et la mise à jour du SMSI ;
 - (d) établit les critères d'évaluation future du risque ;
 - (e) a été approuvée par la direction.
3. définir l'approche d'appréciation du risque de l'organisme :
 - (a) identifier une méthodologie d'appréciation du risque adaptée au SMSI, ainsi qu'à la sécurité de l'information identifiée de l'organisme et aux exigences légales et réglementaires ;
 - (b) développer des critères d'acceptation des risques et identifier les niveaux de risque acceptables. La méthodologie d'appréciation du risque choisie doit assurer que les appréciations du risque produisent des résultats comparables et reproductibles.
4. identifier les risques :
 - (a) identifier les actifs relevant du domaine d'application du SMSI, ainsi que leurs propriétaires¹ ;
 - (b) identifier les menaces auxquelles sont confrontés ces actifs ;
 - (c) identifier les vulnérabilités qui pourraient être exploitées par les menaces ;
 - (d) identifier les impacts que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs ;
5. analyser et évaluer les risques c'est :
 - (a) évaluer l'impact sur l'activité de l'organisme qui pourrait découler d'une défaillance de la sécurité, en tenant compte des conséquences d'une perte de confidentialité, intégrité ou disponibilité des actifs ;
 - (b) évaluer la probabilité réaliste d'une défaillance de sécurité de cette nature au vu des menaces et des vulnérabilités prédominantes, des impacts associés à ces actifs et des mesures actuellement mises en œuvre ;
 - (c) estimer les niveaux des risques ;
 - (d) déterminer si les risques sont acceptables ou nécessitent un traitement, en utilisant les critères d'acceptation des risques ;

1. Le terme "propriétaire" identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des actifs. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur l'actif.

6. identifier et évaluer les choix de traitement des risques. Les actions possibles comprennent :
 - (a) l'application de mesures appropriées ;
 - (b) l'acceptation des risques en connaissance de cause et avec objectivité, dans la mesure où ils sont acceptables au regard des politiques de l'organisme et des critères d'acceptation des risques ;
 - (c) l'évitement ou le refus des risques ;
 - (d) le transfert des risques liés à l'activité associés, à des tiers, par exemple assureurs, fournisseurs ;
7. sélectionner les objectifs de sécurité et les mesures de sécurité proprement dites pour le traitement des risques.

Les objectifs de sécurité et les mesures de sécurité proprement dites doivent être sélectionnés et mis en œuvre pour répondre aux exigences identifiées par le processus d'appréciation du risque et de traitement du risque. Cette sélection doit tenir compte des critères d'acceptation des risques ainsi que des exigences légales, réglementaires et contractuelles.

Les objectifs de sécurité et les mesures de sécurité proprement dites doivent être sélectionnés comme partie intégrante de ce processus, dans la mesure où ils peuvent satisfaire à ces exigences.

Les objectifs de sécurité et les mesures de sécurité proprement dites ne sont pas exhaustifs et des objectifs de sécurité et des mesures de sécurité proprement dites additionnels peuvent également être sélectionnés.

Le questionnaire utilisé pour cette évaluation contient une liste complète d'objectifs de sécurité et des mesures de sécurité proprement dites qui se sont révélés communément appropriés aux organismes. Les utilisateurs peuvent se reporter à ce questionnaire comme point de départ de sélection des mesures de sécurité, afin de s'assurer qu'aucune option importante de sécurité n'est négligée.
8. obtenir l'approbation par la direction des risques résiduels présentés ;
9. obtenir l'autorisation de la direction pour mettre en œuvre et exploiter le SMSI ;
10. préparer une déclaration d'acceptabilité (DdA). Une DdA² doit être élaborée et inclure les informations suivantes :
 - (a) les objectifs de sécurité et les mesures de sécurité proprement dites et les raisons pour lesquelles ils ont été sélectionnés ;
 - (b) les objectifs de sécurité et les mesures de sécurité proprement dites actuellement mis en œuvre ;
 - (c) l'exclusion des objectifs de sécurité et des mesures de sécurité proprement dites spécifiés dans le questionnaire et la justification de leur exclusion.

A.2.2. Mise en œuvre et fonctionnement du SMSI

L'organisme doit effectuer les tâches suivantes :

1. élaborer un plan de traitement du risque qui identifie les actions à engager, les ressources, les responsabilités et les priorités appropriées pour le management des risques liés à la sécurité de l'information ;
2. mettre en œuvre le plan de traitement du risque pour atteindre les objectifs de sécurité identifiés, ce plan prévoyant le mode de financement et l'affectation de rôles et de responsabilités ;
3. mettre en œuvre les mesures de sécurité sélectionnées afin de répondre aux objectifs de sécurité ;
4. définir la méthode d'évaluation de l'efficacité des mesures ou groupes de mesures sélectionnés et spécifier comment ces évaluations doivent être utilisées pour évaluer l'efficacité des mesures, de manière à obtenir des résultats comparables et reproductibles.
5. mettre en œuvre des programmes de formation et de sensibilisation ;

2. La DdA fournit un résumé des décisions concernant le traitement du risque. La justification des exclusions prévoit une contre-vérification qui permet d'assurer qu'aucune mesure n'a été omise par inadvertance

6. gérer les opérations du SMSI ;
7. gérer les ressources consacrées au SMSI ;
8. mettre en œuvre les procédures et les autres mesures permettant de détecter rapidement et de répondre tout aussi rapidement aux incidents de sécurité.

A.3. Surveillance et réexamen du SMSI

L'organisme doit effectuer les tâches suivantes :

1. exécuter les procédures de surveillance et de réexamen, ainsi que les autres mesures afin :
 - (a) de détecter rapidement les erreurs dans les résultats des traitements ;
 - (b) d'identifier rapidement les failles et les incidents de sécurité ;
 - (c) de permettre à la direction de déterminer si les activités de sécurité confiées au personnel ou mises en œuvre par les technologies de l'information sont exécutées comme prévu ;
 - (d) de faciliter la détection des événements de sécurité, et par conséquent, de prévenir les incidents de sécurité par l'utilisation d'indicateurs ;
 - (e) de déterminer si les actions entreprises pour résoudre une faille de sécurité se sont révélées efficaces.
2. réaliser des réexamens réguliers de l'efficacité du SMSI (y compris le respect de la politique et des objectifs du SMSI, et le réexamen des mesures de sécurité) en tenant compte des résultats des audits de sécurité, des incidents, des mesures de l'efficacité, des propositions et du retour d'information de toutes les parties intéressées ;
3. d'évaluer l'efficacité des mesures afin de vérifier que les exigences de sécurité ont été satisfaites ;
4. réexaminer les appréciations du risque à intervalles planifiés et réexaminer le niveau de risque résiduel et le niveau de risque acceptable identifié, compte tenu des changements apportés à l'organisme, à la technologie, aux objectifs métiers et aux processus de l'organisme, aux menaces identifiées, à l'efficacité des mesures œuvre et aux événements extérieurs (modifications apportées à la législation ou à la réglementation, aux obligations contractuelles et au climat social) ;
5. mener des audits internes du SMSI à intervalles fixés ;
6. effectuer une revue de direction du SMSI de manière régulière afin de s'assurer du caractère toujours adéquat du domaine d'application du système et de l'identification des améliorations apportées au processus d'application du SMSI ;
7. mettre à jour les plans de sécurité afin de tenir compte des résultats des activités de surveillance et de réexamen ;
8. consigner les actions et les événements qui pourraient avoir un impact sur l'efficacité ou les performances du SMSI.

A.4. Mise à jour et amélioration du SMSI

L'organisme doit effectuer les tâches suivantes de manière régulière :

1. mettre en œuvre les améliorations identifiées du SMSI ;
2. entreprendre les actions correctives et préventives appropriées. Appliquer les leçons tirées des expériences de sécurité des autres organismes, ainsi que de celles de l'organisme concerné ;
3. informer toutes les parties prenantes des actions et améliorations, avec un niveau de détail approprié aux circonstances et, le cas échéant, convenir de la méthode à adopter ;
4. s'assurer que les améliorations permettent d'atteindre leurs objectifs prévus.