AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

# Audit exposition sur internet

## Cahier des charges

*Statut : A valider* | *Classification : Public* | *Version : 0.94*

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

# SOMMAIRE

**1 Introduction ..... 2**
**1.1 Contexte du programme « cyber-accélération et résilience des établissements » (CaRE) ..... 2**
**1.2 Objet du document ..... 2**
**2 Déroulement de l'audit ..... 3**
**2.1 Prérequis ..... 3**
**2.2 Cartographie ..... 3**
**2.3 Activités exclues de l'audit ..... 3**
**2.4 Analyse ..... 3**
*2.4.1 Services exposés ..... 3*
*2.4.2 Configuration ..... 4*
*2.4.3 Obsolescence / CVE ..... 4*
*2.4.4 Exposition de données sensibles ..... 4*
**2.5 Elaboration du rapport de l'audit ..... 4**
*2.5.1 Contenu du rapport ..... 4*
*2.5.2 Cotation des vulnérabilités et des risques ..... 5*
**3 Restitution des résultats de l'audit ..... 6**
**3.1 Les parties prenantes de l'audit ..... 8**
*3.1.1 L'auditeur officiel ..... 8*
*3.1.2 Le prestataire ..... 8*
**3.2 L'audit ..... 9**
*3.2.1 L'ES audité ..... 9*
*3.2.2 La nature de l'audit ..... 10*
*3.2.1 La date de l'audit ..... 10*
*3.2.1 Le périmètre cible audité ..... 10*
*3.2.1 Le score, le niveau et la somme des vulnérabilités ..... 11*
**4 Clauses de sécurité ..... 12**
**4.1 Devoir d'information du prestataire d'audit ..... 12**
**4.2 Collaboration du prestataire d'audit ..... 12**
**4.3 Sécurité et confidentialité ..... 12**
**4.4 Limitation d'utilisation des données, conservation et transfert hors UE ..... 13**
**ANNEXE 1 : Schéma de la structure d'échange des messages d'audit ..... 14**

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

# 1 INTRODUCTION

## 1.1 Contexte du programme « cyber-accélération et résilience des établissements » (CaRE)

Le programme CaRE a pour objectif de renforcer la sécurité des systèmes d'information des établissements de santé. Ainsi, Le programme CaRE a identifié 4 domaines techniques prioritaires pour répondre à la menace de rançongiciel et d'exfiltration de donnée.

- Domaine 1 : Audits techniques – Annuaire technique & exposition sur internet ;
- Domaine 2 : Poste de travail et détection ;
- Domaine 3 : sécurisation des accès de télémaintenance
- Domaine 4 : stratégie de sauvegarde.

Nous allons, dans ce document, nous concentrer sur le domaine 1. En effet, les cyberattaques récentes montrent que l'exposition internet est l'un des vecteurs principaux de pénétration par les attaquants dans le système d'information des établissements de santé. L'Active Directory (annuaire technique) est ensuite le principal moyen de propagation, par lequel les attaquants obtiennent des privilèges élevés, leur permettant d'infliger plus de dégâts.

Dans le cadre du programme CaRE, il est demandé aux établissements de santé de réaliser régulièrement des audits pour évaluer leur niveau d'exposition sur Internet.

Par ailleurs, les établissements de santé doivent également effectuer des audits réguliers pour évaluer la robustesse de leurs annuaires techniques. Un score d'audit annuaire technique (AD) supérieur à 2 sur 5 est nécessaire pour répondre aux exigences.

## 1.2 Objet du document

Ce document constitue un cahier des charges du service pour la réalisation d'une cartographie de la surface d'exposition sur Internet des établissements de santé et l'identification des vulnérabilités et des risques de sécurité associés.

Ce service vise à donner de la visibilité à ces établissements sur leur niveau d'exposition et à les accompagner par l'application progressive de mesures adéquates pour le réduire. Il permet également aux établissements de réduire leur surface d'attaque, d'adopter une démarche sécurisée et de la maintenir dans le temps.

Les requêtes effectuées dans le cadre de ce service sont similaires à celles auxquelles les équipements sont régulièrement exposés sur Internet.

Les résultats sont rendus disponibles dans un rapport qui détaille et classe les vulnérabilités, les risques de sécurité et les recommandations afférentes. Lors de l'audit, le niveau de sécurité des services exposés sur Internet est traduit par une appréciation globale (VERT/ORANGE/ROUGE) en fonction de la nature et de la gravité des vulnérabilités et des risques identifiés.

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

# 2 DEROULEMENT DE L'AUDIT

Un audit de l'exposition internet doit être réalisé tous les 2 mois à la demande de l'établissement de santé sur tous les services exposés.

## 2.1 Prérequis

L'établissement doit transmettre au prestataire ses adresses IP, les noms de domaine publics utilisés, ainsi que toute information nécessaire à la bonne tenue de l'audit, notamment sur les infrastructures type cloud utilisées.

## 2.2 Cartographie

Il faut identifier l'ensemble des scans de ports réalisés (TCP, UDP, ICMP, SNMP, …) et des interfaces exposées (base de données, web services, APIs, …). Le scan doit s'effectuer sur une liste de ports/services la plus exhaustive possible, notamment afin de découvrir des services et équipements spécifiques à la santé et qui pourraient être exposés.

Une analyse des informations publiquement accessibles et qui auraient pu être exposées par le passé sur les 6 mois précédant la date de l'audit sur les IP et noms de domaine doit être réalisée au travers des services Shodan, Onyphe, Censys, etc…

La découverte de données, informations, vulnérabilités exposées temporairement, ou de nouvelles adresses IP ou noms de domaine n'étant pas connus ou n'ayant pas été fourni par l'audité permettra d'estimer le niveau de maturité du système d'information audité.

Il n'est pas demandé de réaliser une recherche de fuite d'identifiants tel que proposés par les services de type « Have I Been Pawned ».

## 2.3 Activités exclues de l'audit

L'audit n'a pas pour objet de vérifier l'exploitabilité des vulnérabilités ou risques de sécurité identifiés et leur impact, dans les conditions réelles d'une attaque sur le système.

Aussi, l'audit réalisé ne couvre pas les tests suivants :

- la sécurité des mots de passe des interfaces (mot de passe par défaut ou fuités sur les interfaces administrateurs par exemple) ;
- identification et exploitation des vulnérabilités Web (injection SQL, bypass d'authentification, etc…).

## 2.4 Analyse

### 2.4.1 Services exposés

Un certain nombre de services techniques ne doivent pas être exposés sur Internet, comme les services de prise en main à distance (par exemple : SSH, RDP, service d'administration de routeurs/boitiers de sécurité, NetBIOS, DICOM, APIs, …), des outils liés à la gestion du SI, des accès à des services de

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

bases de données (SQL, NoSQL), ou tout accès n'ayant pas nécessité d'être exposé publiquement sans un filtrage affiné des flux.

### 2.4.2 Configuration

Une revue de configurations doit être menée sur des services spécifiques, tels que DNS (vérification du transfert de zone, TTLs, redirections, résolutions récursives), l'accès à des APIs d'administration ou d'interrogation (cloud), ainsi que les configurations de certificats et services TLS (ordre des suites cryptographiques proposées, noms de domaine non fournis et potentiellement utilisés, shadow IT).

### 2.4.3 Obsolescence / CVE

Chaque service exposé doit faire l'objet d'une analyse précise des vulnérabilités non corrigées, comme les CVE et vulnérabilités associées aux équipements et logiciels.

Une analyse des versions de services, applicatifs ou matériels doit être conduite afin de mettre en avant une potentielle dette technique (par exemple une version de service qui n'est plus maintenue sans toutefois faire l'objet de vulnérabilité connue).

### 2.4.4 Exposition de données sensibles

Chaque service, équipement, applicatif, exposé doit faire l'objet d'analyses complémentaires notamment des versions de ces actifs, du type d'accès (public, administration, interne) et des données exposées (données sensibles, données de santé).

## 2.5 Elaboration du rapport de l'audit

Une fois les tests finalisés, le prestataire produit un rapport de l'audit pour le bénéficiaire de l'audit. Il peut être généré automatiquement.

### 2.5.1 Contenu du rapport

Le rapport fourni doit présenter :

- Le périmètre de l'évaluation avec la liste des domaines et sous-domaines, avec une cartographie des systèmes détectés ;
- Une synthèse managériale permettant de prendre rapidement connaissance du niveau de sécurité constaté (VERT/ORANGE/ROUGE), de la typologie des vulnérabilités comprenant une liste non exhaustive des vulnérabilités publiques de niveau critique et haute et des risques de sécurité de niveau critique liés aux services exposés, à la configuration ou à l'exposition de données sensibles tels que précisés ci-après ;
- Une synthèse technique présentant :
    - Les vulnérabilités détectées par niveau de criticité et les risques de niveau critique,
    - Un plan d'actions de remédiation hiérarchisé ;
- Le détail des vulnérabilités et des risques identifiés avec pour chacun :
    - La criticité ;
    - Le type de vulnérabilité ou de risque (ou catégorie, telle que l'exposition d'un service admin, défaut de configuration, …) ;

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- L'impact sur le SI ;
- La description de la vulnérabilité ;
- La recommandation associée en vue de sa correction.

### 2.5.2 Cotation des vulnérabilités et des risques

#### 2.5.2.1 Vulnérabilités liées aux outils sur étagère

Pour définir le niveau de criticité des vulnérabilités publiques identifiées (CVE), l'auditeur se base sur le standard CVSS (3.1 puis 4.0 lorsque cette nouvelle version sera utilisée par une majorité d'éditeurs) et la cotation de l'éditeur. Ce score va de 0 à 10 et correspond aux quatre niveaux faible, moyen, haut et critique. Un calculateur est disponible en ligne : https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N.

#### 2.5.2.2 Risques critiques liés aux services exposés, à la configuration ou à l'exposition de données sensibles

La criticité des risques de sécurité liés aux services exposés et à la configuration ou l'exposition de données sensibles ne peut pas faire l'objet d'une cotation « automatique » selon les 4 niveaux présentés ci-dessus.

Cependant, ce document donne la liste des risques qui doivent être considérés comme critiques dans le cadre de cet audit :

- Exposition d'une base de données contenant des données à caractère personnel ;
- Exposition de protocoles n'utilisant pas de chiffrement nativement (Telnet, FTP, WMI) ;
- Exposition d'accès à distance avec une authentification login-mot de passe :
  - administration technique ou applicative (SSH, applications Web) ;
  - protocole SMB ;
  - serveur Windows RDP.
- Exposition d'un serveur avec des composants logiciels obsolescents et concernés par des vulnérabilités critiques (CVSS > 9) ;
- Exposition d'outils liés à la gestion du SI : redis, elasticsearch, memcached et autres ;
- Configurations DNS vulnérables :
  - absence de vérification de transfert de zone ;
  - autorisation des requêtes DNS récursives.

#### 2.5.2.3 Appréciation des résultats

L'appréciation de l'audit est définie selon les trois niveaux VERT, ORANGE et ROUGE selon les règles suivantes :

- [VERT] : Aucune vulnérabilité publique de niveau critique (CVE supérieur ou égal à 9) ou risque critique lié aux services exposés ou vulnérabilité publique de niveau haute avec un score CVSS entre 7 et 9 n'ayant pas été identifié lors du précédent audit ;

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- [ORANGE] : Vulnérabilités de niveau haute avec un score CVSS entre 7 et 9 devant être corrigées avant le prochain audit ou présence de composants obsolètes devant être soit mis à jour, soit protégés par un équipement de sécurité (VPN, parefeu, etc.…) soit décommissionnés ;
- [ROUGE] : présence d'au moins une vulnérabilité de niveau critique (CVE supérieur ou égal à 9) ou d'un risque critique lié aux services exposés tels que référencés dans le chapitre 2.5.

Seul l'obtention du niveau VERT permet d'être conforme à l'objectif associé du Domaine D1.

# 3 RESTITUTION DES RESULTATS DE L'AUDIT

Certains éléments devront être précisés, le schéma enrichi et certaines règles requises revues (ces cas sont surlignés en jaune dans ce qui suit)

Le format, la fréquence et le canal de remontée des résultats des audits seront précisés dans une version ultérieure du cahier des charges.

La liste des données que le prestataire en charge de l'audit doit transmettre est la suivante :

| Data | Type | Description |
|---|---|---|
| ID de l'auditeur officiel | Identifiant (liste de références à définir et intégrer au schéma) | Identification de la partie prenante qui pilote l'audit (ANSSI, CERT, …) |
| ID du prestataire | SIREN | Identifiant de la partie prenant qui procède à l'audit |
| ID ES | FINESS EG (/ EJ voir le niveau de granularité attendu ?) | Identifiant de l'établissement audité |
| ID GHT | Identifiant à définir (voir si cette donnée ne peut être reconsolidée au niveau du hub ?) | Identifiant du regroupement d'établissements audité |
| Nature de l'audit | Référence (liste de références à définir et intégrer au schéma) | Référence de la nature de l'audit (CaRE-D1, ADS, …) |
| Date de l'audit | Datetime (yyyymmdd-hhmmss) | |
| Périmètre cible audité | Liste d'éléments | FQDN ou IP |
| Score de l'audit | Nombre | CVE ? |
| Niveau évalué | Référence (liste de références red, orange, green à intégrer au schéma) | Couleur en fonction des règles définies au paragraphe « Appréciation des résultats » |
| Vulnérabilités et risques critiques | Nombre (Elément à définir dans le schéma) | |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Le schéma de la structure du format json OPSSIES BI V2 est dans sa version actuelle : ng-msp-opssies-schema-anssi-v5 (voir en ANNEXE 1 la description du schéma). Celui-ci doit être enrichi en fonction des besoins à venir.

Par convention et pour les premiers échanges, ce schéma se base sur une synthèse reprenant les « événements » audités (events) comme objet principal d'association aux systèmes d'appréciation ainsi que les parties prenantes en lien à ces systèmes. L'objet `Stakeholders` permet de définir les parties prenantes qui auditent, le tableau `event` la partie auditée, les périmètres cibles et les résultats.

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

## 3.1 Les parties prenantes de l'audit

### 3.1.1 L'auditeur officiel

L'auditeur officiel correspond à l'institution qui est porteuse de l'audit. La liste de références ou des identifiants reste à définir et intégrer au schéma.

"stakeholderId": {

"_stakeholderIdType": "x",

"__text": " identifiantxxx "

},

"_stakeholderType": "3", ("thirdParty =3")

"_stakeholderRoleType": "3" ("auditor=3")

### 3.1.2 Le prestataire

Le prestataire correspond à l'industriel réalisant l'audit

"stakeholderId": {

"_stakeholderIdType": "4", ("id_siren=4")

"__text": "NumeroSIREN"

},

"_stakeholderType": "3", ("thirdParty=3")

"_stakeholderRoleType": "2" ("serviceProvider=2")

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

## 3.2 L'audit

Il s'agit de définir l'ES audité, la date et le statut de l'action effectuée, le périmètre de l'audit, le résultat de l'audit

### 3.2.1 L'ES audité

Il s'agit ainsi de définir chaque identifiant de l'audité

Voir quelle serait la règle d'usage des identifiants et s'il faut rajouter un stakeholderIdType pour identifier les GHT.

"stakeholderId": [

{

"_stakeholderIdType": "2", ("id_finess_geo =2")

"__text": "identifiantxxx"

},

{

"_stakeholderIdType": "3", ("id_finess_jur =3")

"__text": "identifiantxxx"

},

{

"_stakeholderIdType": "5", ("id_siret =5")

"__text": "identifiantxxx"

}

]

Version de tra



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

### 3.2.2 La nature de l'audit

Il faudrait prévoir un nouveau type, la nature de l'audit `OperationNatureType` et le référencer dans une liste

- ADS
- SILENE
- CaRE-D1
- …

"_OperationNatureType": "CaRE-D1"

### 3.2.1 La date de l'audit

Il s'agit de définir la date de l'audit (au format yyyymmdd-hhmmss)

```
"dates":{
        "date":[
                {
                    "__text":"20231205-152050"
                    }
        ]
}
```

### 3.2.1 Le périmètre cible audité

Il s'agit de définir le périmètre cible et dans ce cas les Fqdn et IP (vérifier si `forestDnsHostName` convient pour le champ IP)

```
"scope":{
        "forest":{
                "forestFqdn":"www.example-ght.fr",
                "forestDnsHostName":"8.8.8.8"
                }
},
```

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

### 3.2.1 Le score, le niveau et la somme des vulnérabilités

Il s'agit de définir le score cible, le niveau et le nombre de vulnérabilités et risques critique. Un champ `CriticalVulnerability` comprenant le nombre de vulnérabilités et risques devrait être rajouté dans le schéma.

```
"outcome":{
        "score":"7780",
        "level":"red",
        "CriticalVulnerability":"17"
        },
```

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

# 4 CLAUSES DE SECURITE

Le prestataire d'audit est tenu de respecter la confidentialité et d'assurer la sécurité des données, notamment celles à caractère personnel dont le bénéficiaire de l'audit a la charge.

Le prestataire d'audit doit ainsi être conforme au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après « RGPD ») ainsi qu'à la Loi Informatique et Libertés n° 78-17 du 7 janvier 1978 modifiée (ci-après « LIL »).

## 4.1 Devoir d'information du prestataire d'audit

Dans la mesure où la prestation d'audit est susceptible de permettre la collecte, l'enregistrement, la saisie, le transfert, l'hébergement, la conservation ou tout autre traitement de données à caractère personnel, le prestataire doit être parfaitement informé des exigences légales qui s'imposent au bénéficiaire de l'audit, responsable de traitement, d'une part et aux éventuels sous-traitants, d'autre part, au sens de la législation en vigueur mentionnée ci-dessus et du caractère essentiel que revêt la conformité des prestations à la réglementation relative à la protection des données personnelles.

## 4.2 Collaboration du prestataire d'audit

Le prestataire d'audit s'engage à apporter son concours en tant que sous-traitant à la réalisation des obligations dont il est tenu en tant que tel et dont est tenu le bénéficiaire de l'audit, en tant que responsable de traitement et notamment à lui fournir tout document et information nécessaire à la réalisation d'une analyse d'impact sur la protection des données personnelles traitées.

## 4.3 Sécurité et confidentialité

A cet égard, et conformément à l'exigence essentielle de sécurité des données, le prestataire d'audit s'engage, dans le cadre de l'exécution de sa prestation et dans le cadre d'une obligation de résultat, à prendre toutes mesures techniques et organisationnelles utiles afin de préserver la sécurité et la confidentialité des données et notamment d'empêcher qu'elles ne soient déformées, endommagées, perdues, détournées, corrompues, divulguées, transmises ou communiquées à des personnes non autorisées et conformément aux exigences de la LIL et du RGPD pour les données à caractère personnel.

Le prestataire d'audit doit notamment respecter les obligations suivantes et les faire respecter par son personnel :

- ne prendre aucune copie des données qui lui sont confiées, à l'exception de celles nécessaires à l'exécution des prestations, l'accord préalable du bénéficiaire de l'audit étant nécessaire ;
- ne pas utiliser les données traitées à des fins autres que celles limitativement spécifiées au marché ;
- ne pas divulguer ces données à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales quelles qu'elles soient ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution des prestations ;

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- plus généralement, le prestataire d'audit doit impérativement traiter, stocker et transmettre les données à caractère personnel susceptibles de figurer parmi les données du bénéficiaire de l'audit de manière parfaitement conforme à la législation relative à la protection des données à caractère personnel.

## 4.4 Limitation d'utilisation des données, conservation et transfert hors UE

Le Titulaire est dûment informé et entend systématiquement appliquer les principes et exigences suivants conformément à la LIL et au RGPD :

- ne traiter les données à caractère personnel que par stricte application des finalités en lien avec l'objet des prestations, telles qu'elles sont indiquées par le bénéficiaire de l'audit selon ses instructions, notamment en cas de demande d'accès, de rectification, de suppression, de limitation ou de portabilité émanant d'une personne physique ;
- ne conserver les données que pendant la durée qui sera indiquée par le bénéficiaire de l'audit et en cas de rupture contractuelle quelle qu'en soit la raison, sans possibilité de rétention des données quelle qu'elle soit, et sans conservation au-delà de la demande de restitution ou de destruction émanant du bénéficiaire de l'audit.

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

# ANNEXE 1 : Schéma de la structure d'échange des messages d'audit

Source du schéma de la structure du format json OPSSIES BI V2 : ng-msp-opssies-schema-anssi-v5

Par convention et pour les premiers échanges, ce schéma se base sur une synthèse reprenant les « événements » audités (events) comme objet principal d'association aux systèmes d'appréciation ainsi que les parties prenantes en lien à ces systèmes.

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

## A. Racine événements

**events Object §**

Résultat de l'audit

| Field Name | Type | Description |
|---|---|---|
| stakeholders | stakeholders Object | Identification des parties prenantes qui auditent |
| Event | event Array | Données de l'audit |

## B. Parties prenantes Audits

Il s'agit de définir les parties prenantes qui font procéder ou procèdent à l'audit.

**stakeholders Object §**

Parties prenantes

| Field Name | Type | Description |
|---|---|---|
| stakeholder | stakeholder Array | Liste des parties prenantes |

**stakeholder Array §**

Partie prenante



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

| Field Name | Type | Description |
|---|---|---|
| stakeholderId | stakeholderId Object | Identifiant de la partie prenante |
| stakeholderName | stakeholderName Object | Nom de la partie prenante |
| _stakeholderType | Integer | Type de la partie prenante |
| _stakeholderRoleType | Integer | Rôle de la partie prenante |

**stakeholderId Object §**

Partie prenante : référence

| Field Name | Type | Description |
|---|---|---|
| _stakeholderIdType | Integer | Référence identifiante de la partie prenante (exemple 4 pour indiquer qu'il s'agit d'un identifiant Siren)<br>"stakeholderIdType":{<br>"type":"integer",<br>"enum":[<br>1, 2, 3, 4, 5<br>],<br>"referenceList":[<br>"1;id_finess_plage",<br>"2;id_finess_geo",<br>"3;id_finess_jur",<br>"4;id_siren",<br>"5;id_siret"<br>]<br>} |
| __text | String | Valeur textuelle |

**stakeholderName Object §**



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Partie prenante : nom

| Field Name | Type | Description |
|---|---|---|
| _stakeholderNameType | Integer | Libellé court ou long de la partie prenante (exemple 1 pour indiquer le libellé court)<br>"stakeholderNameType":{<br>"type":"integer",<br>"enum":[<br>1, 2<br>],<br>"referenceList":[<br>"1;shortLabel",<br>"2;longLabel"<br>]<br>} |
| __text | String | Valeur textuelle |

**_stakeholderType §**

Partie prenante type

| Field Name | Type | Description |
|---|---|---|
| _stakeholderType | Integer | Liste du type de partie prenante (exemple 1 pour indiquer qu'il s'agit d'un site)<br>"referenceList":[<br>"1;site",<br>"2;incorporatedGroup",<br>"3;thirdParty"<br>]<br>"site" = structure auditée (ES EG)<br>"incorporatedGroup" = structure englobante de celle auditée (GHT / ES EJ)<br>"thirdParty" = tiers participant à l'audit (ANSSI, …) |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**_stakeholderType §**

Partie prenante rôle

| Field Name | Type | Description |
|---|---|---|
| _stakeholderRoleType | Integer | Liste du rôle de la partie prenante (exemple 3 pour indiquer qu'il s'agit d'un auditeur)<br>"referenceList":[<br>"1;requester",<br>"2;serviceProvider",<br>"3;auditor",<br>"4;recipient"<br>]<br>"requester" = structure auditée (EG / EJ / GHT, …)<br>"serviceProvider" = Industriels ou prestataires opérant l'audit<br>"auditor" = Auditeur officiel (ANSSI<br>"recipient" = bénéficiaires des résultats de l'audit (ANS, …) |

Version



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

### C. ES audités

Il s'agit de définir l'ES audité, le contexte d'activité professionnelle couvert, la date et le statut de l'action effectuée, le périmètre de l'audit, le résultat de l'audit

**event Array** §

Les Audits

| Field Name | Type | Description |
|---|---|---|
| Stakeholders | stakeholders Object | Parties prenantes auditées |
| Contexts | contexts Object | Les contextes d'activités professionnelles couverts |
| Dates | dates Object | Les dates et statuts de l'audit |
| Scope | scope Object | Le périmètre de l'audit |
| Outcome | outcome Object | Le résultat de l'audit |
| _eventType | Integer | Le type d'événement de référence de l'audit |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**stakeholders Object §**

Parties prenantes

| Field Name | Type | Description |
|---|---|---|
| stakeholder | stakeholder Object | Liste des parties prenantes |

Point de vigilance `stakeholder` est ici un Object et non plus un Array comme dans le chapitre précédent.

**stakeholder Object §**

Partie prenante auditée

| Field Name | Type | Description |
|---|---|---|
| stakeholderId | stakeholderId Array | Tableau des Identifiants de la partie prenante auditée |

**stakeholderId Array §**

Partie prenante : identifiants

| Field Name | Type | Description |
|---|---|---|
| _stakeholderIdType | Integer | Référence identifiante de la partie prenante (exemple 4 pour indiquer qu'il s'agit d'un identifiant Siren)<br>"referenceList":[<br>"1;id_finess_plage",<br>"2;id_finess_geo",<br>"3;id_finess_jur",<br>"4;id_siren",<br>"5;id_siret"<br>] |
| __text | String | Valeur de l'identifiant |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**contexts Object** §

Contextes d'activité

| Field Name | Type | Description |
|---|---|---|
| Context | context Array | Tableau décrivant les contextes d'activités professionnelles auditées |

**context Array** §

Contextes d'activités

| Field Name | Type | Description |
|---|---|---|
| _contextType | Integer | Référence identifiante du type de contexte<br>"1;Fonctionnel",<br>"2;Technique",<br>"3;Technico-fonctionnel" |
| _contextCategory | Integer | Référence identifiante des contextes voir le tableau ci-dessous) |
| _text | String | Valeur |

| Description List |
|---|
| "referenceList":[<br>"1;Pilotage médico-économique", |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**Description List**

"2;Production des soins cliniques",

"3;Production de soins médico-techniques",

"4;Recherche",

"5;Support",

"6;Infrastructures",

"7;Gestion Administrative du Patient",

"8;Gestion des actes et consultations externes",

"9;Facturation",

"10;Bureautique médicale",

"11;Gestion du dossier médical du patient",

"12;Gestion des dossiers d'anesthésie",

"13;Gestion des dossiers de réanimation",

"14;Gestion des dossiers transfusionnels",

"15;Gestion des dossiers RCP",

"16;Gestion des dossiers de dialyse",

"17;Gestion des dossiers HAD",

"18;Gestion du dossier de soins",

"19;Gestion des lits (planification)",

"20;Gestion des rendez vous et planification",

"21;Prescription de Médicaments",

"22;Médicaments - BDM",

"23;Prescription de  Produits Sanguins Labiles",

"24;Prescription de Chimiothérapies",

"25;Prescription d'Analyses médicales",

"26;Prescription d' Examens d'Imagerie",

"27;Prescription de Soins",

"28;Gestion des Blocs opératoires",

"29;Gestion de laboratoire de biologie",

"30;Serveur de résultats - biologie",

"31;Gestion de Laboratoire d'anatomocytopathologie",

"32;Pharmacie",

"33;Chimiothérapie",

"34;Traçabilité des DMI",

"35;Stérilisation",

"36;Médecine Nucléaire",

"37;Imagerie Médicale - SIR",

"38;Imagerie Médicale - PACS",

"39;Dépôt de produit sanguins labiles",



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**Description List**

```
    "40;Hémovigilance",
    "41;Gestion des urgences",
    "42;SAMU",
    "43;PMSI MCO",
    "44;PMSI SSR",
    "45;PMSI PSY",
    "46;Recueil d'activité et aide au codage",
    "47;Outil de contrôle qualité",
    "48;Constitution du FICHCOMP - MO",
    "49;Constitution du FICHCOMP - DMI",
    "50;Constitution du FICHCOMP - PIE",
    "51;Constitution du FICHCOMP - PO",
    "52;Constitution du FICHCOMP - PIP",
    "53;Constitution du fichier VIDHOSP",
    "54;Constitution du RSF / ACE",
    "55;Constitution du RSS groupé",
    "56;Gestion Economique et financière",
    "57;Comptabilité analytique",
    "58;GMAO - biomédical",
    "59;Restauration",
    "60;Transport des patients",
    "61;GMAO - Services techniques",
    "62;SSO",
    "63;Système de Gestion des Ressources Humaines",
    "64;Médecine du travail",
    "65;Gestion des Vigilances",
    "66;Gestion des Risques - Evenements indésirables",
    "67;Gestion Documentaire",
    "68;Questionnaires - Enquetes",
    "69;Système décisionnel",
    "70;Messagerie Sécurisée PS",
    "71;Portail Extranet PS",
    "72;Télémédecine"
]
```



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**dates Object** §

Dates et statuts de l'audit

| Field Name | Type | Description |
|---|---|---|
| date | date Array | Tableau décrivant les dates et statuts de l'audit |

**date Array** §


```
"dates": {
   "date": [
      {
         "_dateType":"4",
         "__text":"20231205-152050"
      },
      {
         "_dateType":"7",
         "__text":"20240115-141742"
      }
   ]
```


Dates et statuts de l'audit

| Field Name | Type | Description |
|---|---|---|
| _dateType | Integer | Référence identifiante des statuts "referenceList" : [ "1;Demande effective", "2;Demande prévisionnelle", "3;Demande annulée", "4;Inscription effective", "5;Inscription prévisionnelle", "6;Inscription annulée", "7;Réalisation effective", "8;Réalisation prévisionnelle", "9;Réalisation annulée" |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

| Field Name | Type | Description |
|---|---|---|
| | | ] |
| _text | DateTimme | Date au format aaaammjj-hhmmss |

Version de travail



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**scope Object** §

Périmètre de l'audit

| Field Name | Type | Description |
|---|---|---|
| forest | forest Object | Objet décrivant les différents périmètres d'audit |

**forest Object** §


```
"forest":{
   "forestFqdn":"corp1.example-
   ght.fr",
   "forestGuid":"556c5d2e-e75d-4d20-
   8a45-033d96465f70",
   "forestDnsHostName":"dnsserver.exa
   mple-ght.fr",
   "forestNetBiosName":"corp1"
}
```

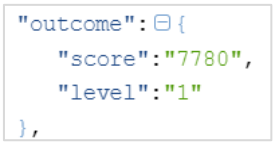

Périmètres d'audit

| Field Name | Type | Description |
|---|---|---|
| forestFqdn | String | Fully Qualified Domain Name |
| forestGuid | String | ID utilisateur ? |
| forestDnsHostName | String | IP ou NDM ? |
| forestNetBiosName | String | Nom de machine |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

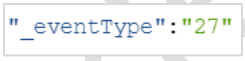
**outcome Object** §




Résultats de l'audit

| Field Name | Type | Description |
|---|---|---|
| score | Integer | Résultat chiffré |
| isConform | true\|false | Conforme ou non (pas dans le schéma actuel) |
| level | String | Niveau peut être déterminé par une couleur (rouge, orange, vert) |

**eventType** §




Résultats de l'audit

| Field Name | Type | Description |
|---|---|---|
| _eventType | Integer | Le type d'événement de référence de l'audit (voir la liste ci-dessous) |

| Description List |
|---|
| "referenceList":[<br>"1;IDENTIFIER/Gestion des actifs/Connaissance des actifs physiques et logiciels",<br>"2;IDENTIFIER/Gestion des actifs/Messagerie et protocoles",<br>"3;IDENTIFIER/Gestion des actifs/Gestion des identités et des accès",<br>"4;IDENTIFIER/Gestion des actifs/Mots de passe",<br>"5;IDENTIFIER/Gestion des actifs/Sauvegarde",<br>"6;IDENTIFIER/Gestion des actifs/Téléphonie",<br>"7;IDENTIFIER/Gestion des actifs/Chiffrement et protection des secrets, hachage",<br>"8;IDENTIFIER/Environnement métier/Connaissance écosystème",<br>"9;IDENTIFIER/Gouvernance/Connaissance des normes et standards", |



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**Description List**

"11;IDENTIFIER/Gouvernance/Obligations du prestataire-risques client",

"10;IDENTIFIER/Gouvernance/Connaissance juridique et réglementaire",

"12;IDENTIFIER/Gouvernance/Recommandations de base",

"13;IDENTIFIER/Appréciation des risques/Identification",

"14;IDENTIFIER/Appréciation des risques/Typologie des attaquants",

"15;IDENTIFIER/Appréciation des risques/Gestion des vulnérabilités",

"16;IDENTIFIER/Stratégie de gestion des risques/Gestion de crise",

"17;IDENTIFIER/Gestion des risques de la chaîne approvisionnement/Relation client",

"18;IDENTIFIER/Gestion des risques de la chaîne approvisionnement/Anticipation",

"19;PROTÉGER/Gestion des identités et contrôle accès/Chiffrement et protection des secrets, hachage",

"20;PROTÉGER/Gestion des identités et contrôle accès/Sécurisation",

"21;PROTÉGER/Sensibilisation et formation/Recommandations de base",

"22;PROTÉGER/Sensibilisation et formation/Relation client",

"23;PROTÉGER/Sécurité des données/Sécurité physique",

"24;PROTÉGER/Sécurité des données/Téléphonie",

"25;PROTÉGER/Sécurité des données/Architecture",

"26;PROTÉGER/Sécurité des données/Sécurisation",

"27;PROTÉGER/Sécurité des données/Sécurisation/Audit technique/AD/ADS",

"28;PROTÉGER/Sécurité des données/Sécurisation/Audit technique/Exposition Internet/Cybersurveillance",

"29;PROTÉGER/Sécurité des données/Sécurisation/Audit technique/Next-Gen",

"60;PROTÉGER/Sécurité des données/Sécurisation/Audit technique/Exposition Internet/SILENE",

"61;PROTÉGER/Sécurité des données/Sécurisation/Audit technique/Messagerie",

"30;PROTÉGER/Sécurité des données/Antivirus",

"31;PROTÉGER/Sécurité des données/Administration systèmes",

"32;PROTÉGER/Sécurité des données/Disponibilité",

"33;PROTÉGER/Processus et procédures de protection des informations/Procédure interne",

"34;PROTÉGER/Maintenance/MCO-MCS",

"35;PROTÉGER/Technologie de protection/Connaissance des solutions et technologies de sécurisation existantes",

"36;DETECTER/Anomalies et événements/Identification",

"37;DETECTER/Anomalies et événements/Gestion des vulnérabilités",

"38;DETECTER/Surveillance continue de la sécurité/Analyse",

"39;DETECTER/Surveillance continue de la sécurité/Supervision SSI",

"40;DETECTER/Surveillance continue de la sécurité/Attaques",

"41;DETECTER/Processus de détection/Détection",

"42;RÉPONDRE/Plan intervention/Gestion de crise",

"43;RÉPONDRE/Plan intervention/Gestion de crise/Simulation-Exercice",

"44;RÉPONDRE/Plan intervention/Réponse à incidents",



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

**Description List**

```
    "45;RÉPONDRE/Communication/Connaissance juridique et réglementaire",
    "46;RÉPONDRE/Analyse/Identification",
    "47;RÉPONDRE/Analyse/Conservation de la preuve",
    "48;RÉPONDRE/Analyse/Analyse",
    "49;RÉPONDRE/Analyse/Analyse matérielle",
    "50;RÉPONDRE/Atténuation/Accompagnement",
    "51;RÉPONDRE/Atténuation/Remédiation",
    "52;RÉPONDRE/Amélioration/Procédure interne",
    "53;RÉTABLIR/Planification de la récupération/Gestion de crise",
    "54;RÉTABLIR/Planification de la récupération/Sauvegarde",
    "55;RÉTABLIR/Planification de la récupération/PCA-PRA",
    "56;RÉTABLIR/Amélioration/Procédure interne",
    "57;RÉTABLIR/Amélioration/Veille technologique-Exploitation",
    "58;RÉTABLIR/Communication/Relation client",
    "59;RÉTABLIR/Communication/Gestion de crise"
]
```

Version de



Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.