Rapport d'audit de Ornisec

1.Audit

ID	Question	Score	Commentaire
1	Qui est le responsable de la Sécurité des Systèmes d'Information au sein de votre organisation ?	0	RAS
2	A qui est rattaché le RSSI ?	0	RAS
3	Quelles sont les ressources en ETP (Equivalent Temps Plein) dédiées à la réalisation des activité de cybersécurité ? (n'inclut pas les administrateurs des infrastructures)	0	RAS
4	Avez-vous des ressources dédiées à la sécurité opérationnelle ?	0	RAS
5	Avez-vous identifié formellement les processus SSI (e.g. gestion des incidents, gestion des sauvegardes, gestion des exceptions, gestion des vulnérabilités...) à mettre en œuvre au sein de votre organisation ? Avez-vous déterminé les compétences, les rôles et responsabilités associés ? Les responsabilités ont-elles été réparties entre les équipes (par exemple au travers d'un RACI) ?	0	RAS
6	Par quels moyens la disponibilité des ressources compétentes liées à la SSI est-elle garantie (e.g. redondance des ressources internes, appel à des prestations...) ? Y a-t-il des périodes sans compétences SSI au sein de l'organisation (suite à des congés par exemple) ? Des astreintes sont-elles mises en place en heures non ouvrées ?	0	RAS
7	Quels rôles sont couverts par une fiche de poste ? (e.g. RSSI, équipe du RSSI, sécurité opérationnelle, security champion pour l'Agile…)	0	RAS
8	Avez-vous une PSSI ? De quand date la dernière mise à jour ?	0	RAS
9	La PSSI est-elle validée par la direction ? Sa mise en œuvre est-elle appuyée par la direction ?	0	RAS
10	La PSSI est-elle mise à disposition des collaborateurs et de quelle façon ?	0	RAS
11	Disposez-vous d'un référentiel documentaire inventoriant les éléments (e.g. politiques, processus, procédures, plans…) formalisés par votre organisation ? Une version de ces documents est-elle centralisée ? Une copie de ces documents isolée du SI (par exemple sur clé USB) existe-elle ?	0	RAS
12	Une analyse des risques numériques est-elle réalisée de façon transverse pour toute l'entité ? Quel est son niveau d'exhaustivité ? A quelle fréquence est-elle mise à jour?	0	RAS
13	Un schéma directeur / une feuille de route est-il défini pour traiter les risques numériques ? Une priorité est-elle définie pour chaque chantier ?	0	RAS
14	Quels indicateurs sont suivis dans le cadre du pilotage de la sécurité ? (e.g. % de serveurs à jour des correctifs, % postes de travails avec antivirus…) Les résultats des indicateurs sont-ils utilisés pour déterminer des objectifs opérationnels et stratégiques pour l'organisation ?	0	RAS
15	Des comités de pilotage dédiés à la cybersécurité sont-ils organisés ? A quelle fréquence ? Qui y participe ?	0	RAS
16	Un plan de sensibilisation (populations cibles, messages pour chaque population, outils & planning) est-il défini et mis en œuvre?	0	RAS
17	Des communications de sensibilisation par e-mail sont-elles effectuées de façon périodique ? A quelle fréquence ? Sont-elles appuyées par la direction ?	0	RAS
18	Réalisez-vous des présentations de sensibilisation sur l'intranet et des rappels physiques sur la cybersécurité (e.g. goodies, posters dans les salles imprimantes, messages sur écrans, etc.) ?	0	RAS
19	Réalisez-vous des sessions de sensibilisation en présentiel ?	0	RAS
20	Réalisez-vous de la sensibilisation à la cybersécurité spécifique auprès des dirigeants ?	0	RAS
21	Réalisez-vous de la sensibilisation à la cybersécurité spécifique pour les membres des équipes achats ?	0	RAS

ID	Question	Score	Commentaire
22	Réalisez-vous de la sensibilisation à la cybersécurité spécifique pour les administrateurs du SI (et pour les ingénieurs biomédicaux pour les établissements de santé) ?	0	RAS
23	Réalisez-vous de la sensibilisation à la cybersécurité spécifique pour les développeurs SI ?	0	RAS
24	Réalisez-vous de la sensibilisation à la cybersécurité spécifiques pour les référents métier et les maitrises d'ouvrage des projets SI ?	0	RAS
25	Réalisez-vous des tests de phishing ?	0	RAS
26	Avez-vous défini une charte utilisateur des systèmes d'information ? Est-elle signée par la population cible des utilisateurs ou annexée au règlement interne ?	0	RAS
27	Avez-vous défini une charte spécifique pour les utilisateurs à privilèges de la DSI (e.g. administrateurs, helpdesk, développeurs…) ? Est-elle signée par la population cible ?	0	RAS
28	Réalisez-vous des formations à la cybersécurité ? Sous quel format ? (e.g. e-learning, formations présentielles, etc.) Auprès de quelles populations ?	0	RAS
29	Les postes de travail et les équipements mobiles (e.g. smartphones, tablettes) sont-ils répertoriés au sein d'un inventaire centralisé qui comprend tous les éléments nécessaires à leur connaissance (e.g. modèle, utilisateur du bien, services /applications locaux associés..) ? Quel outil ou document est utilisé pour ce faire (e.g. fichier Excel, SSCM, Intune,...) ?	0	RAS
30	Chiffrez-vous les postes de travail portables (e.g. BitLocker) ? L'ensemble du parc est-il couvert ? Quel est le mécanisme de chiffrement utilisé et d'authentification associé (e.g. authentification par code Pin+TPM) ? Les clés de chiffrement sont-elles stockées de façon sécurisée ?	0	RAS
31	Avez-vous déployé sur les postes de travail une protection anti-malwares/anti-virus basée sur les signatures ? Quelle solution est mise en place ? L'ensemble du parc est-il couvert ? Quelle est la fréquence et quelles sont les modalités de mise à jour ?	0	RAS
32	Une solution de sandboxing est-elle utilisée pour tester des fichiers ou programmes non vérifiés (pièces jointes de mails…) qui peuvent contenir un virus ou un autre code malveillant ?	0	RAS
33	Avez-vous mis en œuvre un EDR sur tous les postes de travail pour une surveillance et une analyse continues afin d'identifier, de détecter et de prévenir plus facilement les menaces avancées et les signaux faibles ? L'ensemble du parc est-il couvert ?	0	RAS
34	Une solution de prévention de la fuite des données (DLP) est-elle déployée sur les postes de travail ? Fonctionne-t-elle en mode détection ou blocage ?	0	RAS
35	Un processus de déploiement des correctifs de sécurité sur les postes de travail est-il mis en œuvre ? Avec quel outillage (e.g. WSUS) ? Est-il automatisé ? Est-il formalisé ? Une veille sécurité est-elle réalisée concernant la gestion des vulnérabilités (e.g. abonnement newsletter CSIRT…) sur les postes de travail ?	0	RAS
36	Quel est le délai défini pour la mise en œuvre des correctifs standards et des correctifs critiques ?	0	RAS
37	Quel est le taux d'application des correctifs sur les postes de travail ?	0	RAS
38	Avez-vous déployé une stratégie de sécurité (GPO) sur les postes de travail ? Quels paramètres sont modifiés par ces GPO (e.g. temps de veille de l'écran, logiciels téléchargeables, stratégies de mot de passe…) ?	0	RAS
39	Des outils de gestion (e.g. SCCM ou Intune) sont-ils implémentés sur les postes de travail connectés au SI de l'entreprise ? Quelles actions sont réalisées au travers de ces outils (e.g. installation de la configuration initiale de sécurité, déploiement de correctifs, contrôle de la conformité des configurations, déploiement de plan d'actions automatique pour les dispositifs non conformes (e.g. alerte, blocage, etc.) etc.) ?	0	RAS
40	Quels dispositifs d'effacement sécurisé/destruction sont mis en œuvre dans le cadre du cycle de vie des postes de travail (réattribution, maintenance externalisée, fin de vie,…) ?	0	RAS
41	Les droits d'administration sur les postes de travail sont-ils interdits par défaut, et accordés seulement pour des profils aux besoins spécifiques (selon un processus de gestion des exceptions tracé) ? Un dispositif est-il mis en place afin de ne pas avoir de compte d'administration locale identique sur tous les postes (e.g. avec la solution LAPS) ?	0	RAS

ID	Question	Score	Commentaire
42	Des comptes dédiés sont-ils utilisés pour l'administration des postes de travail (par exemple dans le cadre des activités de support) ? Les droits de ces comptes sont-ils uniquement dédiés à l'administration des postes ?	0	RAS
43	Les appareils à distance se connectent-ils au réseau via un VPN chiffré standard ?	0	RAS
44	Les appareils à distance se connectent-ils systématiquement au réseau par le biais d'une authentification utilisateur et d'un mot de passe ? Une authentification multi-facteurs est-elle requise ? (e.g. par certificats, carte à puce, biométrie,…)	0	RAS
45	La configuration de sécurité est-elle vérifiée lors de la connexion de l'appareil ? (e.g. NAC pour la connexion physique, VPN pour la connexion à distance…)	0	RAS
46	Une solution de contrôle d'accès au réseau empêchant à un poste de travail ou un équipement externe de se connecter au SI interne (par exemple basée sur du contrôle par adresse mac, sur des certificats / du Network Acces Control (NAC)) est-elle implémentée sur tout le réseau) ?	0	RAS
47	Un contrôle d'accès (e.g. par mot de passe, par badge…) est-il mis en place sur les imprimantes ?	0	RAS
48	Comment les fichiers scannés sont-ils traités ? (stockage sur un répertoire partagé, stockage temporaire sur un répertoire individuel, envoi par mail…)	0	RAS
49	Une politique est-elle formalisée pour définir les règles de sécurité à respecter sur les smartphones et tablettes ? Est-elle appliquée ? Est-elle contrôlée ?	0	RAS
50	Des outils de gestion de type MDM sont-ils implémentés sur les téléphones mobiles et tablettes ? Quelles actions sont réalisées au travers de ces outils ? (e.g. configurer l'appareil lors de l'inscription, chiffrement de l'appareil, déploiement de correctifs, installer une politique de sécurité , effacer l'appareil à distance, etc.)	0	RAS
51	Un document est-il communiqué aux utilisateurs expliquant les bonnes pratiques d'usage à mettre en œuvre sur les smartphones et tablettes (e.g. charte dédiée aux équipements mobiles) ?	0	RAS
52	Une politique d'authentification est-elle appliquée aux téléphones mobiles et tablettes ? Quelle est cette politique ? (e.g. code PIN à 4 chiffres, 6 chiffres, biométrie, etc.) Est-elle appliquée à l'ensemble du parc ?	0	RAS
53	Les activités sensibles effectuées à partir des appareils mobiles sont-elles protégées par une authentification à deux facteurs (e.g.: U2F Bluetooth, jeton NFC...) ?	0	RAS
54	Les applications de l'organisation sont-elles répertoriées au sein d'un inventaire centralisé (e.g. CMDB) qui comprend tous les éléments nécessaires à leur connaissance (e.g. propriétaire du bien, niveau de sensibilité,...) ? Quel outil ou document est utilisé pour ce faire ?	0	RAS
55	La sensibilité cybersécurité et les exigences de sécurité des applications de l'organisation sont-elles identifiées ? Sont-elles déterminées selon des critères communs à toute l'organisation ? Quel outil ou document est utilisé pour ce faire ?	0	RAS
56	Une méthodologie d'intégration de la sécurité dans les projets informatiques (durant les phases de cadrage, définition de l'architecture, développement, recette...) est-elle formalisée et communiqué aux différentes parties prenantes ? Comment est-elle outillée ? Est-elle adaptée aux différentes typologies de projets (e.g. cycle en V, agile) ?	0	RAS
57	Une revue de conformité à un référentiel de mesures minimales de sécurité est-elle réalisée pour les projets (ce travail peut aussi être réalisé dans le cadre d'une analyse de risques) ?	0	RAS
58	Une analyse des risques est-elle effectuée pour les projets les plus sensibles ? A quelle fréquence est-elle mise à jour ?	0	RAS
59	Quels périmètres font l'objet d'une démarche d'homologation ? Qui est autorité d'homologation ?	0	RAS
60	Des principes de développement sécurisé sont-ils mis en œuvre pour tous les projets applicatifs ? Un guide de développement sécurisé est-il formalisé ?	0	RAS
61	Comment l'intégrité du code source d'une application est garantie à toutes les étapes d'un projet (développement, exploitation, communication externe et interne) ? Des outils sont-ils utilisés dans ce cadre pour gérer les accès et tracer les actions réalisées sur celui-ci ? (plateforme centralisée d'intégration…)	0	RAS

ID	Question	Score	Commentaire
62	Des contrôles basés sur une liste de sécurité (e.g. top 10 OWASP) sont-ils réalisés ? Tous les projets applicatifs sont-ils couverts ?	0	RAS
63	Des contrôles basés sur scans de vulnérabilité sont-ils réalisés sur les applications en développement ? Quel périmètre des projets applicatifs est couvert ?	0	RAS
64	Des contrôles basés sur des tests d'intrusion sont-ils réalisés sur les applications en développement les plus sensibles ? Quel ratio des projets applicatifs est couvert ?	0	RAS
65	Des contrôles basés sur une revue du code, éventuellement de façon automatisée, sont-ils réalisés sur les applications en développement ? Est-il mis en œuvre pour tous les projets applicatifs ?	0	RAS
66	Un processus de déploiement des correctifs de sécurité sur les applications est-il mis en œuvre ? Avec quel outillage ? Est-il automatisé ? Est-il formalisé ? Une veille sécurité est-elle réalisée concernant la gestion des vulnérabilités (e.g. abonnement newsletter CSIRT…) sur les applications ?	0	RAS
67	Quel est le délai défini pour la mise en œuvre des correctifs standards et des correctifs critiques ?	0	RAS
68	Quel est le taux d'application des correctifs sur les applications ? Sont-ils appliqués sur l'ensemble des environnements (e.g. production, développement, recette…) ?	0	RAS
69	Des mesures de sécurisation complémentaire de la messagerie sont-elles mises en place (e.g. antispam, sandboxing, réécriture et analyse des liens dans un mail, captcha en cas de premier mail, contrôle de réputation de l'émetteur…) ?	0	RAS
70	Les applications obsolètes (e.g : Exchange obsolète) /contenant des composants obsolètes (e.g. : serveur SQL, système de gestion de base de données) , ou en passe de l'être, sont-elles identifiées et répertoriées dans un inventaire centralisé ? Les éléments obsolètes font-ils l'objet de mesures correctives (e.g. montée de version, remplacement…) ou, si ce n'est pas possible, sont-elles protégées par des mesures spécifiques de réduction des risques (e.g. isolement du réseau) ?	0	RAS
71	Une démarche est-elle mise en œuvre pour identifier le shadow IT mis en œuvre au sein de votre organisation ? Des mesures sont-elles mises en œuvre pour identifier les enjeux SSI associés aux périmètres concernés ? Des mesures sont-elles mises en œuvre pour réintégrer ces périmètres dans le SI légitime ou pour en maîtriser les impacts ?	0	RAS
72	Des contrôles basés sur scans de vulnérabilité sont-ils réalisés sur les applications en production ? Est-il mis en œuvre pour toutes les applications ?	0	RAS
73	Des contrôles basés sur des tests d'intrusion sont-ils réalisés sur les applications en production les plus sensibles ? Quel ratio des applications sensibles est couvert ?	0	RAS
74	Des contrôles basés sur une revue du code, éventuellement de façon automatisée, sont-ils réalisés sur les applications en production ? Est-il mis en œuvre pour toutes les applications ?	0	RAS
75	Comment le décommissionnement des applications est-il appliqué ?	0	RAS
76	Les fournisseurs de services informatiques (e.g. développeurs, éditeurs, infogérants, hébergeurs, fournisseurs de matériel…) sont-ils inventoriés ? Dans quels documents et/ou outils sont-ils formalisés ? Le risque inhérent de ces fournisseurs pour la sécurité de votre organisation est-il identifié ? Est-il évalué en fonction des prestations qu'ils réalisent ?	0	RAS
77	Des clauses de sécurité (e.g. cloisonnement des données, communication des incidents de sécurité, confidentialité des données,…) sont-elles intégrées dans les contrats ? Ces clauses sont-elles sélectionnées selon les différents types des prestations ? Tous les contrats où ces clauses seraient pertinentes sont-ils couverts ?	0	RAS
78	Le niveau de maturité cyber d'un prestataire est-il évalué finement (e.g. à l'aide d'un Plan d'Assurance Sécurité) dans le cadre des prestations d'un certain niveau de criticité ? Des plans d'actions sont-ils mis en œuvre en cas d'identification de risques non négligeables ?	0	RAS
79	Les clauses contractuelles comprennent-elles un droit à l'audit lorsque c'est estimé nécessaire ? Des critères sont-ils fixés pour déterminer si ce droit d'audit doit être intégré aux clauses ?	0	RAS

ID	Question	Score	Commentaire
80	Des audits de sécurité des prestataires les plus critiques sont-ils effectués ? Combien d'audits ont-ils été réalisés ces 2 dernières années ?	0	RAS
81	Les partenaires (e.g. autres organismes publics, entreprises, associations...) ayant des interactions métier avec votre organisation et/ou dont le SI est interconnecté au votre sont-ils inventoriés ? Dans quels documents et/ou outils sont-ils formalisés ? Le risque inhérent de ces partenaires pour la sécurité de votre organisation et de ses données est-il évalué ?	0	RAS
82	Des clauses de sécurité (e.g. cloisonnement des données, communication des incidents de sécurité, confidentialité des données,…) sont-elles intégrées dans des conventions avec les partenaires ? Ces clauses sont-elles sélectionnées selon la nature des relations avec les partenaires et des ressources SI/données auxquelles ils ont accès ? Tous les partenariats où ces clauses seraient pertinentes sont-ils couverts ?	0	RAS
83	Le niveau de maturité cyber d'un partenaire est-il évalué finement (e.g. à l'aide d'un bilan de maturité) dans le cadre des partenariats d'un certain niveau de criticité ? Des plans d'actions sont-ils mis en œuvre en cas d'identification de risques non négligeables ?	0	RAS
84	Avez-vous identifié les rôles et responsabilités liés à votre cybersécurité et tenus par des prestataires et partenaires ? Avez-vous identifiés les risques liés à ces transferts ou partages de compétences/responsabilités ? Font-ils l'objet d'actions de mise sous contrôle ?	0	RAS
85	Les ressources informatiques de l'organisation sont-elles répertoriées au sein d'un inventaire centralisé (e.g. CMDB) qui comprend tous les éléments nécessaires à leur connaissance (e.g. propriétaire du bien, services /applications associées..) ? Quel outil ou document est utilisé pour ce faire ?	0	RAS
86	Un inventaire des infrastructures sensibles (e.g. AD, DNS, hyperviseur, KPI, etc.) est-il réalisé ? Quel outil ou document est utilisé pour ce faire ?	0	RAS
87	Comment se fait la connexion des administrateurs aux ressources ? (e.g. directement, via un serveur de rebond, via un bastion) En cas d'accès par un serveur de rebond ou un bastion, les flux d'accès directs des administrateurs aux serveurs sont coupés ? Est-ce qu'une authentification forte est mise en œuvre ? Les actions des administrateurs sont-elles tracées ?	0	RAS
88	Les flux d'administrations sont-ils chiffrés ? Sur quels périmètres reste-t-il des flux d'administration non chiffrés (de type Telnet) ?	0	RAS
89	Les infrastructures obsolètes, ou en passe de l'être, sont-elles identifiées et répertoriées dans un inventaire centralisé ?	0	RAS
90	Les infrastructures obsolètes, ou en passe de l'être, identifiées font-elles l'objet de mesures correctives (mise à jour, remplacement…) ou, si ce n'est pas possible, sont-elles protégées par des mesures spécifiques de réduction des risques (e.g. isolement du réseau) ?	0	RAS
91	Des règles de durcissement sont-elles définies pour les infrastructures (OS, middlewares, bases de données, infrastructure réseau) ? Incluent-elles le principe de la fonctionnalité minimale (seules les fonctionnalités nécessaires ne sont pas bloquées) ?	0	RAS
92	Le durcissement des actifs (OS, middlewares, bases de données, et infrastructure réseau...) est-il effectué pour les nouveaux projets ? (i.e. lors de l'installation de l'actif) Est-il effectué sur le SI existant ?	0	RAS
93	La configuration des infrastructures critiques est-elle à l'état de l'art (e.g. AD, DNS, SCCM, PKI, …) ?	0	RAS
94	Avez-vous déployé sur les serveurs une protection anti-malwares/anti-virus basée sur les signatures ? Quelle solution est mise en place ? L'ensemble du parc est-il couvert ? Quelle est la fréquence et quelles sont les modalités de mise à jour ?	0	RAS
95	Avez-vous mis en œuvre un EDR sur tous les serveurs pour une surveillance et une analyse continue afin d'identifier, de détecter et de prévenir plus facilement les menaces avancées et les signaux faibles ? L'ensemble du parc est-il couvert ?	0	RAS
96	Quels dispositifs d'effacement sécurisé/destruction sont mis en œuvre dans le cadre du cycle de vie des disques et bandes de données (maintenance externalisée, fin de vie,…) ? En cas d'externalisation du processus, quelles preuves sont générées (e.g. certificat de destruction, audit...) ?	0	RAS

ID	Question	Score	Commentaire
97	Un processus de déploiement des correctifs de sécurité sur les serveurs est-il mis en œuvre ? Avec quel outillage ? Est-il automatisé ? Est-il formalisé ? Une veille sécurité est-elle réalisée concernant la gestion des vulnérabilités (e.g. abonnement newsletter CSIRT…) sur les serveurs ?	0	RAS
98	Quel est le délai défini pour la mise en œuvre des correctifs standards et des correctifs critiques ?	0	RAS
99	Quel est le taux d'application des correctifs sur les serveurs ? Sont-ils appliqués sur l'ensemble des environnements (e.g. production, développement, recette…) ?	0	RAS
100	Des scans de vulnérabilité sont-ils réalisés afin de détecter des vulnérabilités (liées à l'absence de durcissement ou à un défaut de mise à jour) sur les OS, middlewares, bases de données et infrastructure réseau ? A quelle fréquence ces scans sont-ils réalisés et avec quels outils?	0	RAS
101	Les flux de données sont-ils cartographiés et mis à jour à chaque évolution (ouverture/fermeture de flux) pour chaque projet ? Pour toute l'organisation ? Dans quels documents et/ou outils sont-ils formalisés (e.g. : Dossier d'Architecture Technique (DAT) des projets, CMDB, outil de cartographie automatique - développement interne ou outil du marché,…) ?	0	RAS
102	Un inventaire des interconnexions de tous les SI externes (e.g. SaaS, fournisseurs Cloud, partenaires infogérants…) au SI interne est-il réalisé ? Dans quels documents et/ou outils sont-ils formalisés ?	0	RAS
103	Un référentiel des points d'accès à Internet (entrants et sortants) est-il formalisé et mis à jour à chaque évolution ? En particulier, les points d'accès (e.g. box ADSL) mis en place de façon indépendante par les directions métiers sont-ils référencés ?	0	RAS
104	Des équipements de filtrage standards (Firewall) sont-ils déployés et configurés pour filtrer les flux entre des zones de sécurité définies en fonction de l'exposition (internet, fournisseurs, partenaires,...), de la sensibilité, de l'environnement (production, pré-production,...) pour limiter la propagation des menaces ?	0	RAS
105	Une micro segmentation est-elle mise en œuvre pour les SI les plus sensibles ?	0	RAS
106	Un filtrage périmétrique est-il mis en place ? Une DMZ contenant les ressources exposées est-elle mise en place ?	0	RAS
107	Le réseau d'administration système est-il cloisonné ?	0	RAS
108	Des revues régulières des règles de filtrage du réseau sont-elles réalisées (sur les routeurs et/ou les firewalls) ?	0	RAS
109	Les accès Internet (pour la navigation, par les applications) sont-ils filtrés et journalisés (e.g. avec un proxy géré par l'organisation ou FW type UTM) ? Les outils mettant en œuvre ce filtrage et cette traçabilités sont-ils centralisés ?	0	RAS
110	Tout le trafic de navigation est-il filtré à l'aide de listes de blocage (e.g. liée à la réputation, liste noire…) ?	0	RAS
111	L'architecture réseau liée au Wi-Fi est-elle sécurisée (e.g. Wi-Fi public déconnecté du réseau professionnel de l'organisation, Wi-Fi professionnel situé sur un VLAN dédié filtré avec le reste du réseau,...) Les flux de navigation Internet des utilisateurs du Wi-Fi transitent-ils par un proxy ?	0	RAS
112	Une authentification est-elle en place pour la connexion au Wi-Fi professionnel ? Comment se fait-elle ? (e.g. via une clé publique partagée, par 802.1x avec certificat ou mot de passe) Est-ce que ces accès sont journalisés ? Pendant quelle durée ?	0	RAS
113	Est-ce que l'accès à ce Wi-Fi public est identifié (e.g. avec une adresse mail) ou authentifié (e.g. avec un code à usage unique) ? Est-ce que ces accès sont journalisés ? Pendant quelle durée ?	0	RAS
114	Quels outils sont utilisés par les administrateurs (internes ou infogérants) pour accéder aux ressources en cas de maintenance à distance (e.g. accès direct, accès via serveur de rebond ou bureau virtuel, accès via bastion, accès VPN, etc.) ?	0	RAS
115	Les accès dans le cadre de la maintenance à distance de ressources (système ou applicatives) sont-ils approuvés et enregistrés ?	0	RAS
116	Les accès de maintenance à distance par des intervenants externes sont-ils ouverts uniquement avec une durée de validité limitée de manière à empêcher tout accès non autorisé ?	0	RAS

ID	Question	Score	Commentaire
117	Les points d'accès Internet entrants sont-ils protégés par une solution anti-DDoS réseau ?	0	RAS
118	Les applications exposées à Internet (e.g. sites web, DNS...) sont-elles protégées par une solution applicative anti-DDoS ?	0	RAS
119	Des reverse proxies sont-ils utilisés pour sécuriser les applications exposées ?	0	RAS
120	Des pare-feux applicatifs (WAF) sont-ils déployés pour sécuriser les applications exposées sur Internet ? Ces WAF incluent-ils des vérifications avancées (e.g. déchiffrement TLS, whitelisting Url, etc.) ?	0	RAS
121	Une méthodologie de classification des données structurées (e.g. dans les bases de données et applications) et non structurées (e.g. mails, fichiers…) est-elle définie ? Permet-elle d'évaluer la criticité SSI des données ?	0	RAS
122	Toutes les données sensibles (e.g. bases de données) structurées sont-elles classifiées ? Dans quels documents et/ou outils cette classification est formalisée ?	0	RAS
123	Toutes les données sensibles non structurées (e.g. documents) ou binaires (e.g. fichiers non textuels) sont-elles classifiées ? Dans quels documents et/ou outils cette classification est formalisée ?	0	RAS
124	Les bases de données applicatives sensibles sont-elles protégées (e.g. accès aux bases de données, chiffrement,…) ? Sur quel périmètre est-ce mis en œuvre ? En cas de chiffrement, est-il réalisé au niveau des serveurs applicatifs ? Comment les clés de chiffrement sont-elles protégées ?	0	RAS
125	Comment les données applicatives sensibles sont-elles protégées sur un environnement hors production (formation, développement, intégration, recette…) ?	0	RAS
126	Comment sont gérées les bases de mots de passe (e.g. en clair, chiffrées, hachées,…) ? En cas de hachage, quel est l'algorithme utilisé ? Les mots de passe sont-ils salés avant d'être hachés ? Comment les clés de chiffrement/hachage sont-elles protégées ?	0	RAS
127	Les sauvegardes des données sensibles sont-elles protégées (e.g. accès aux fichiers de sauvegarde, chiffrement,…) ? En cas de chiffrement, est-il réalisé au niveau des serveurs de sauvegarde ? Comment les clés de chiffrement sont-elles protégées ?	0	RAS
128	L'utilisation de supports amovibles est-elle autorisée sur les postes de travail ? Sur les serveurs ? Un blocage technique est-il mis en place pour l'empêcher ?	0	RAS
129	Une solution de GDN (Gestion des Droits Numériques / DRM en anglais) est-elle utilisée sur les dossiers sensibles ?	0	RAS
130	Une solution d'échange sécurisée est-elle mise à disposition des utilisateurs pour les échanges externes de données non structurées (fichiers…) ? Est-elle utilisée ?	0	RAS
131	Des consignes de chiffrement des données sensibles partagées par mail sont-elles partagées ? Ces consignes sont-elles respectées ? Des outils de chiffrement des pièces jointes sont-ils mis à disposition des utilisateurs ?	0	RAS
132	Les flux applicatifs web sont-ils chiffrés (e.g. protocoles https, FTPS...) ?	0	RAS
133	Des solutions de prévention de fuite des données (DLP) sont-elles déployées sur les passerelles Web et Email pour détecter l'exfiltration des données ? Sont-elles déployées en mode détection ou blocage ? Les communications chiffrées sont-elles déchiffrées pour permettre la surveillance ?	0	RAS
134	Un processus de gestion des arrivées et départs des utilisateurs du SI est-il mis en œuvre ? Ce processus est-il lié aux processus d'arrivée et départ RH ? Couvre-t-il également les mobilités entre les services ? Ce processus est-il formalisé ?	0	RAS
135	Quels outils sont utilisés pour gérer les arrivées et départs des utilisateurs du SI ? (e.g. processus manuel par mail, outil de ticketing, outils IAM dédié, etc.)	0	RAS
136	Des revues des identités sont-elles mises en place pour s'assurer de la cohérence des référentiels RH avec les identités existantes sur le SI ?	0	RAS
137	Un processus de gestion des demandes d'habilitation sur le SI est-il défini (pour les accès utilisateurs et les accès administrateurs) ? Est-il mis en cohérence avec les arrivées/départs/mobilités ?	0	RAS

ID	Question	Score	Commentaire
138	Les habilitations sont-elles attribuées sur la base de profils définis selon le principe du moindre besoin/privilège ? (pour les accès utilisateurs/administrateurs fonctionnels et les accès administrateurs techniques)	0	RAS
139	Quelles mesures sont mises en place pour assurer la ségrégation des tâches afin d'éviter les combinaisons de droits toxiques (e.g. même personne en action et en validation) ? (e.g. contrôles manuels a posteriori, blocage automatique lors du workflow de demande d'habilitation, etc.) (pour les accès utilisateurs/administrateurs fonctionnels et les accès administrateurs techniques)	0	RAS
140	Quel outil est utilisé pour gérer les habilitations sur le SI ? (e.g. processus manuel par mail, outil de ticketing, outils IAM dédié, etc.) (pour les accès utilisateurs/administrateurs fonctionnels et les accès administrateurs techniques)	0	RAS
141	Les événements du cycle de vie (e.g. arrivée, mobilité, demande d'ajout ponctuel de droit, départ, etc.) déclenchent-ils automatiquement des workflows concernant les habilitations ? Ces workflows incluent-ils une étape de validation par un responsable hiérarchique ou un responsable de ressource ? (pour les accès utilisateurs/administrateurs fonctionnels et les accès administrateurs techniques)	0	RAS
142	Un processus de revue des habilitations aux ressources du SI est-il défini (recertification) ? Quels périmètres d'habilitations sont couverts (e.g. administration fonctionnelle, utilisation d'application, accès aux répertoires partagés...) ? A quelle fréquence sont réalisées les revues ? (pour les accès utilisateurs/administrateurs fonctionnels)	0	RAS
143	Quels outils sont utilisés pour mener les revues des habilitations ? (e.g. outil maison, outils IAG) Le déclenchement de la campagne de revue est-il automatisé ? (pour les accès utilisateurs/administrateurs fonctionnels)	0	RAS
144	Est-il nécessaire de s'authentifier pour accéder aux applications ? Comment l'authentification est-elle réalisée ? (e.g. pas d'authentification, utilisation d'identifiants stockés dans chaque base de données applicative, SSO avec authentification transparente, Fédération d'identité avec un protocole standard type SAML, etc.) (pour les accès utilisateurs/administrateurs fonctionnels)	0	RAS
145	Avez-vous mis en place un annuaire centralisé pour la gestion des comptes utilisateurs (e.g. AD) ? Quels périmètres couvre-t-il ? (pour les accès utilisateurs/administrateurs fonctionnels et les accès administrateurs techniques)	0	RAS
146	Des comptes génériques sont-ils utilisés par les utilisateurs pour se connecter aux ressources du SI ? (poste de travail ou applications) (pour les accès utilisateurs/administrateurs fonctionnels)	0	RAS
147	Quelle politique de mot de passe (exigences en terme de complexité, de fréquence de mise à jour et d'historique) est mise en œuvre pour les utilisateurs ? (pour les accès utilisateurs/administrateurs fonctionnels)	0	RAS
148	Une authentification multifacteur est-elle mise en œuvre en fonction du niveau de sensibilité des ressources accédées et du contexte de connexion (depuis Internet, sur site,…) ? (pour les accès utilisateurs/administrateurs fonctionnels et les accès administrateurs techniques)	0	RAS
149	Les comptes à privilèges de la DSI (e.g. administrateurs système, développeurs, helpdesk…) sont-ils inventoriés de façon exhaustive ? Quels outils/documents sont utilisés pour ce faire ?	0	RAS
150	Les utilisateurs à privilèges de la DSI utilisent-ils uniquement des comptes nominatifs pour se connecter aux ressources du SI dans le cadre de leurs activités ou utilisent-ils dans certains cas des comptes génériques ?	0	RAS
151	Lorsque les utilisateurs à privilèges de la DSI utilisent des comptes nominatifs pour réaliser des activités, utilisent-ils des comptes à privilèges dédiés et distincts de leurs comptes utilisateur du quotidien ?	0	RAS
152	Quelle politique de mot de passe (exigences en terme de complexité, de fréquence de mise à jour et d'historique) est mise en œuvre pour les utilisateurs à privilèges de la DSI ?	0	RAS
153	Comment sont stockés les mots de passe des comptes à privilèges de la DSI ? (e.g. fichier Excel, coffre fort de mots de passe, bastion d'administration...)	0	RAS
154	Des revues des accès des comptes à privilèges de la DSI sont-elles réalisées ? A quelle fréquence ?	0	RAS
155	Les comptes techniques (machine-to-machine) au sein de l'organisation sont-ils inventoriés ? Dans quels outils ou documents ?	0	RAS

ID	Question	Score	Commentaire
156	Quelle est la logique de définition des comptes techniques ? (e.g. un compte unique partagé par tout le SI, un compte partagé par type d'actif - applications, hyperviseurs, bases de données…-, un compte spécifique par ressource, etc.) Ces comptes sont-ils inventoriés ? Avec l'aide de quel outil ?	0	RAS
157	Comment sont protégés les identifiants/mots de passe des comptes techniques ? (e.g. identifiant/mot de passe en clair dans les fichiers de configuration, stockage dans un format hashé, stockage dans un coffre-fort de mot de passe, etc.)	0	RAS
158	Est-il interdit de créer une session interactive (utilisable par des agents) avec ces comptes techniques ? D'autres mécanismes sont-ils utilisés en complément des mots de passe ou en remplacement des mots de passe pour sécuriser l'accès aux comptes techniques ? (e.g. certificat, clé SSH, passage par un coffre-fort sécurisé etc.)	0	RAS
159	Existe-il une politique encadrant l'usage des certificats électroniques au sein de l'organisation (algorithme de chiffrement, taille de clé…) ? Quelle est l'organisation mise en place pour supporter ces usages ?	0	RAS
160	Quelles sont les infrastructures mises en place pour gérer le cycle de vie des certificats utilisés ? Quel est le niveau d'industrialisation des processus de délivrance et renouvellement des certificats ? Des moyens de contrôle des certificats sont-ils mis en œuvre ?	0	RAS
161	Comment sont sécurisées les clés privées des autorités de certification (AC) ?	0	RAS
162	Des dérogations et exceptions de sécurité sont-elles réalisées au niveau de la gestion des droits d'accès ? Si Retenu, font-elles l'objet d'un processus formalisé et tracé ? Qui réalise ces dérogations ? Ces dérogations sont-elles à durée limitée ?	0	RAS
163	L'accès aux salles/centres informatiques est-il protégé (e.g. serrure, badge…) ?	0	RAS
164	Les salles/zones sensibles sont-elles surveillées par des systèmes de vidéosurveillance 24 heures sur 24, 7 jours sur 7 ?	0	RAS
165	L'accès physique aux baies sensibles est-il protégé (e.g. badges, clés,…) ?	0	RAS
166	Les journaux des dispositifs de sécurité réseau (e.g. pare-feu, passerelles d'accès à distance, etc.) sont-ils collectés ? Quelles sont les traces générées et les périmètres concernés ? Les journaux sont-ils stockés localement ou centralisés (au sein d'un puit de logs ou d'un SIEM) et disponibles pour preuve ? Quelle est la durée de rétention des journaux ?	0	RAS
167	Les journaux des solutions de sécurité (e.g. anti-virus, HIPS...) sont-ils collectés ? Quelles sont les traces générées et les périmètres concernés ? Les journaux sont-ils stockés localement ou centralisés (au sein d'un puit de logs ou d'un SIEM) et disponibles pour preuve ? Quelle est la durée de rétention des journaux ?	0	RAS
168	Les journaux d'infrastructure (e.g. serveurs / base de données / middleware) sont-ils collectés ? Quelles sont les traces générées et les périmètres concernés ? Les journaux sont-ils stockés localement ou centralisés (au sein d'un puit de logs ou d'un SIEM) et disponibles pour preuve ? Quelle est la durée de rétention des journaux ?	0	RAS
169	Les journaux des applications métiers concernant les évènements de sécurité sont-ils collectés ? Quelles sont les traces générées et les périmètres concernés ? Les journaux sont-ils stockés localement ou centralisés (au sein d'un puit de logs ou d'un SIEM) et disponibles pour preuve ? Quelle est la durée de rétention des journaux ?	0	RAS
170	Les accès aux traces centralisées sont-ils restreints ?	0	RAS
171	Quels dispositifs sont mis en place pour prouver l'intégrité des traces (e.g. hasher une archive des traces puis la stocker via un flux TCP sur un répertoire sécurisé pour comparaison si nécessaire) ?	0	RAS
172	Comment sont exploités les journaux des dispositifs de sécurité réseau (e.g. pare-feu, passerelles d'accès à distance, etc.) (e.g. analyse ponctuelle suite à évènement, dans un SIEM…) ?	0	RAS
173	Comment sont exploités les journaux des solutions de sécurité (e.g. anti-virus, HIPS...) (e.g. analyse ponctuelle suite à évènement, dans un SIEM…) ?	0	RAS
174	Comment sont exploités les journaux d'infrastructure (e.g. serveurs / base de données / middleware) (e.g. analyse ponctuelle suite à évènement, dans un SIEM…) ?	0	RAS

ID	Question	Score	Commentaire
175	Comment sont exploités les journaux des applications métiers concernant les évènements de sécurité (e.g. analyse ponctuelle suite à évènement, dans un SIEM…) ?	0	RAS
176	Avez-vous déployé des IDS sur votre réseau afin de détecter les flux suspects (e.g. option sur un parefeu, sonde on premise, solution d'analyse externalisée/SaaS,...) ? De quelle façon sont-ils supervisés (e.g. alerte par mail, interconnexion avec un SIEM…) ?	0	RAS
177	Avez-vous déployé des systèmes de prévention d'intrusion (IPS) sur votre réseau afin de détecter et bloquer les flux suspects (e.g. option sur un parefeu, sonde on premise, solution d'analyse externalisée/SaaS,...) ? De quelle façon sont-ils supervisés (e.g. alerte par mail, interconnexion avec un SIEM…) ?	0	RAS
178	Avez-vous un SIEM ? Quels périmètres sont couverts par les alertes automatiques (e.g. infrastructures réseau, infrastructures serveurs, applications métiers, solutions de sécurité) ? Avec quelle exhaustivité ?	0	RAS
179	Des alertes automatiques (basées sur de la corrélation et/ou des modèles et/ou du machine Learning) sont-elles implémentées pour détecter une activité anormale pour des cas d'usage "classiques" (e.g. modifications de configuration sur des SI sensibles, modification du DNS, création d'un compte d'administrateur du domaine, détection d'un hit antivirus sur un serveur, tentative de brute force sur un compte AD, connexion VPN depuis des nœuds d'anonymisation ou depuis des zones géographiques à risque ou hors heures ouvrées etc.) En cas d'arrêt d'émission de logs vers un SIEM, une alerte est-elle générée ?	0	RAS
180	Comment sont construits les cas d'usage "avancés" de détection utilisés par le SIEM ? (e.g. sur la base des risques identifiés pour l'organisation, d'éléments de threat intelligence et des leçons apprises (e.g. Faux négatifs))	0	RAS
181	Les SI gérés par les fournisseurs sont-ils intégrés au périmètre de détection ? (e.g. applications SaaS, SI infogéré, etc.)	0	RAS
182	Enrichissez-vous vos alertes à l'aide d'informations de Threat Intelligence recueillies auprès de diverses sources (Open Source, fournisseurs externes, pairs de l'industrie, autorités, dark web, réseaux sociaux....) ? Ces informations sont-elles personnalisées et diversifiées (menaces sectorielles, journaux internes...) ?	0	RAS
183	Disposez-vous d'un SOC ? Les rôles et les responsabilités liées au SOC sont-ils définis ?	0	RAS
184	Des points de contact uniques (e.g. RSSI, Représentant Métier, Administrateurs…) sont-ils identifiés pour que le SOC puisse leur communiquer des alertes pour traitement N2/N3 ?	0	RAS
185	Un processus de gestion des incidents de sécurité (avec matrice de classification, modalités de traitement, rôles et responsabilités) est-il défini et appliqué ? Contient-il une procédure d'escalade ? A qui est-il communiqué ?	0	RAS
186	Des plans de cyber-réponse (e.g. fiches réflexes) sont-ils documentés pour répondre aux incidents et aux scénarios classiques d'attaques ?	0	RAS
187	Des procédures d'arrêt d'urgence du SI (applicables en cas de panne de climatisation, d'attaque cyber avérée…) sont-elles définies et formalisées ? Permettent-elles de n'arrêter de façon maîtrisée qu'une partie spécifique du SI ? Sont-elles communiquées à toutes les équipes ? Sont-elles testées ?	0	RAS
188	Une politique de sauvegarde (précisant notamment les périmètres à couvrir, les fréquences associés et les outils utilisés) est-elle définie ? Est-elle mise en œuvre ? Est-elle formalisée ?	0	RAS
189	Les sauvegardes sont-elles isolées physiquement des environnements de production ? Sont-elles isolées logiquement (afin d'éviter qu'elles ne soient perdues en cas de cryptolocker généralisé) ?	0	RAS
190	Des tests de restauration sont-ils effectués ? A quelle fréquence ? S'agit-il de restaurations suite à des demandes en production (e.g. restauration d'une base de données) ou dans le cadre de tests formels ? Quel est le périmètre couvert par ces tests ?	0	RAS
191	Les processus critiques en terme de disponibilité et les ressources informatiques qui les supportent sont-ils identifiés au sein d'un inventaire centralisé (BIA) ? Sont-ils mis à jour en fonction des nouveaux risques et de la veille ? A quelle fréquence ?	0	RAS
192	Les ressources techniques en support des infrastructures et applications sensibles sont-elles redondées ? Dans quelles proportions la bascule vers les ressources de secours est-il automatique en cas de défaillance d'équipement (e.g. actif-actif) ? Les équipements en redondance sont-ils sur des sites physiques différents ?	0	RAS

ID	Question	Score	Commentaire
193	Les risques ou scénario (hors scénarios d'attaque cyber) qui doivent être couverts par un plan de reprise d'activité sont-ils identifiés ? Une stratégie de reprise d'activité a-t-elle été définie pour répondre à ces risques ou scénarios critiques ?	0	RAS
194	Existe-t-il une stratégie de reprise d'activité en réponse au scénario d'attaque cyber ?	0	RAS
195	Des procédures et dispositifs techniques et opérationnels de reprise d'activité (permettant par exemple le déploiement de serveurs de reprise) sont-ils définis, documentés et déployés en déclinaison des stratégies ?	0	RAS
196	En particulier, des procédures et dispositifs techniques et opérationnels de reprise d'activité sont-ils définis, formalisés et déployés en réponse au scénario d'attaque cyber ?	0	RAS
197	Quels tests sont réalisés pour les plans de reprise d'activité ? (périmètres techniques couverts, scénarios couverts, fréquence…)	0	RAS
198	En particulier, des tests du plan de reprise d'activité en cas d'attaque cyber sont-ils réalisés ?	0	RAS
199	Avez-vous créé une sauvegarde spécifique de serveurs permettant de reconstruire ex nihilo un cœur d'infrastructures critiques (AD-DNS-DHCP-Console AV-Console SCCM- …) ? Est-elle protégée d'une attaque de type ransomware généralisé (e.g. via sauvegarde sur bande, solution de sauvegarde immuable...)?	0	RAS
200	Un plan de reconstruction/reprise rapide des serveurs d'infrastructure critiques et des terminaux a-t-il été défini ? Est-il testé ?	0	RAS
201	Un processus de gestion de crise est-il défini ? A-t-il été partagé à toutes les personnes susceptibles d'intervenir en gestion de crise ? Inclut-il un volet cyber ?	0	RAS
202	La mise en œuvre du processus de gestion de crise est-elle testée ? Le volet cyber est-il testé ? A quelle fréquence ?	0	RAS
203	Des outils sont-ils mis en place afin de communiquer avec toutes les personnes impliquées dans une gestion de crise ? (e.g. main courante traçant les évènements tenue à jour, conférence téléphonique sécurisée, messagerie sécurisée et résiliente, annuaire de secours - par exemple avec téléphone personnel-...)	0	RAS
204	Des équipes sont-elles identifiées comme très rapidement mobilisables en cas d'attaque ou d'incident majeur (e.g. en interne - management, administrateurs techniques, experts -, via un abonnement CERT ou CSIRT...) ? Quand sont-elles mobilisables (en HO, en HNO) ? Le dispositif d'intervention type et ses modalités d'interventions ont-elles été formalisées ?	0	RAS
205	Des critères d'éligibilité sont-ils définis pour maitriser les risques d'hébergement d'une application dans le Cloud (e.g. données sensibles, faisabilité technique, coût, contraintes légales...) ? Des niveaux attendus de sécurisation des services cloud sont-ils associés à ces critères d'éligibilité ? Le respect de ces critères et la mise en place de mesures de sécurisation en cas de besoin est-elle contrôlée ? (services IaaS, PaaS, SaaS)	0	RAS
206	Une politique/stratégie de sécurisation/durcissement est-elle définie pour chaque fournisseur de service cloud utilisé ? Est-elle appliquée (e.g. en configurant les services visés, en définissant des exigences contractuelles, en utilisant un service disposant déjà d'une certification - comme le SOC2 - délivrée par une autorité externe) ? Est-elle formalisée ? (services IaaS, PaaS, SaaS)	0	RAS
207	La mise en œuvre de la stratégie de durcissement est-elle contrôlée ? De quelle façon (e.g. avec des contrôles manuels réguliers, avec des contrôles automatiques) ?	0	RAS
208	Comment sont corrigés les écarts à la politique/stratégie ? (e.g. manuellement sous une semaine, remédiation automatique,…)	0	RAS
209	Un responsable de la sécurité du Cloud est-il nommé ? Son rôle et ses responsabilités sont-ils clairement définis dans une fiche de poste ? (services IaaS, PaaS, SaaS)	0	RAS
210	La conformité des fournisseurs de services Cloud à leurs obligations contractuelles est-elle contrôlée (e.g. par un audit, par la vérification de l'existence d'une certification reconnue à jour) ? (services IaaS, PaaS, SaaS)	0	RAS
211	La restitution et l'effacement des données hébergées par le Cloud sont-ils contractuellement définis (notamment dans le cadre de la réversibilité)? Ces dispositifs sont-ils régulièrement testés ? (services IaaS, PaaS, SaaS)	0	RAS

ID	Question	Score	Commentaire
212	Une stratégie de sauvegarde est-elle définie pour les données/workload dans le Cloud ? Est-elle formalisée ? Comment sont effectuées les sauvegardes (e.g. déclenchement manuel, déclenchement automatisé) ? (services IaaS, PaaS, SaaS)	0	RAS
213	Les sauvegardes sont-elles stockées dans une zone de disponibilité autre que celle où elles sont créées (e.g. dans une autre zone de disponibilité, chez un autre fournisseur, on-premise, etc.) ? (services IaaS, PaaS, SaaS)	0	RAS
214	Les sauvegardes sont-elles testées ? (services IaaS, PaaS, SaaS)	0	RAS
215	Des capacités de redondance sont-elles mises en place sur des services Cloud pour éviter les cas d'interruption de service ? Quels sont les périmètres couverts par des capacités de redondance ? Quelle stratégie est mise en place (e.g. redondance au sein d'un site, entre zones de disponibilité,…) ? (services IaaS, PaaS, SaaS)	0	RAS
216	Des tests réguliers des capacités de redondance mises en place sont-ils effectués ? (services IaaS, PaaS, SaaS)	0	RAS
217	Comment sont gérés les accès d'administration au Management plane (portails d'administration des fournisseurs Cloud) ? (e.g. par login/mdp, par MFA, via un bastion…) Les droits d'accès sont-ils régulièrement revus ? (services IaaS, PaaS, SaaS)	0	RAS
218	Comment sont sécurisés les accès d'administration au Data plane pour les environnements IaaS (e.g. par un serveur de rebond, via un bastion…) ? Les droits d'accès sont-ils régulièrement revus ? (services IaaS)	0	RAS
219	Les journaux des accès administrateurs aux environnements Cloud IaaS sont-ils activés ? Sont-ils centralisés ? (services Iaas, PaaS, SaaS)	0	RAS
220	Des pare-feux applicatifs (WAF) sont-ils déployés (e.g. Iaas, par le client ; SaaS/PaaS, par le fournisseur) afin de protéger les services Cloud exposés sur Internet ? (services Iaas, PaaS, SaaS)	0	RAS
221	Des équipements anti-DdoS sont-ils déployés (e.g. IaaS, par le client ou le fournisseur ; SaaS/PaaS, par le fournisseur) afin de protéger les services Cloud exposés sur Internet ? (services IaaS, PaaS, SaaS)	0	RAS
222	L'exposition (ou la non exposition) des services Cloud sur Internet est-elle maîtrisée (e.g. IaaS, à l'aide des équipements de type proxy ou FW ; PaaS, par la configuration du service (ouvert sur Internet/ Non ouvert sur Internet) ? (services IaaS, PaaS)	0	RAS
223	Des dispositifs sont-ils mis en œuvre pour sécuriser les flux entrants depuis Internet et sortants des services Cloud ? (e.g. FW, politiques de filtrage, infrastructures d'inspection des flux…) (services IaaS, PaaS)	0	RAS
224	Un responsable de la sécurité informatique industrielle (dédié ou non) est-il nommé ? Son rôle et ses responsabilités sont-ils clairement définis dans une fiche de poste ?	0	RAS
225	Les ressources informatiques industrielles (actifs physiques, actifs réseau, SI, applications) de l'organisation sont-elles répertoriées au sein d'un inventaire centralisé (e.g. CMDB) qui comprend tous les éléments nécessaires à leur connaissance (e.g. propriétaire du bien,..) ? Quel outil ou document est utilisé pour ce faire ?	0	RAS
226	Par quels moyens la sécurité est-elle intégrée dans les projets SI industriels ?	0	RAS
227	Quels dispositifs sont mis en œuvre pour contrôler la sécurité des SI industriels ?	0	RAS
228	Quelles mesures de protection sont mises en place pour filtrer et sécuriser les flux entre le réseau industriel et le réseau de l'organisation ?	0	RAS
229	Des équipements de filtrage standards (firewall, diode) sont-ils déployés au sein des réseaux industriels et configurés pour filtrer les flux entre des zones de sécurité définies en fonction de l'exposition (fournisseurs,...), de la sensibilité, de l'environnement (production, sécurité,...) pour limiter la propagation des menaces ?	0	RAS
230	Comment sont gérés les comptes utilisateurs en environnement industriel ? Les comptes génériques sont-ils interdits ? Un outil de gestion centralisée d'identification et d'authentification (p. ex. AD) est-il utilisé ? Est-il dédié aux SI industriels ?	0	RAS

ID	Question	Score	Commentaire
231	Comment sont gérés les accès d'administration sur les SI industriels par les équipes internes ? Un bastion est-il mis en œuvre en cas d'accès depuis un réseau distant (e.g. Internet, réseau bureautique) ? Est-ce que ce bastion est dédié au SI industriel ?	0	RAS
232	Quels outils sont utilisés par les administrateurs externes (tiers infogérants) pour accéder aux SI industriels en cas de maintenance à distance (e.g. accès direct, accès via serveur de rebond ou bureau virtuel, accès via bastion, accès VPN, etc.) ?	0	RAS
233	Les postes de travail associés aux SI industriels sont-ils sécurisés ? Des mesures de durcissement sont-elles mises en œuvre (e.g. gel de configuration, postes en mode kioske...) Quels types de postes de travail sont concernés (e.g. postes raccordés aux machines, postes de maintenance) ?	0	RAS
234	Des règles de durcissement (e.g. changement des identifiants, désactivation des fonctions non nécessaires…) sont-elles définies pour les automates ? Sur quels périmètres sont-elles appliquées ? (nouveaux automates installés, automates critiques,…)	0	RAS
235	Avez-vous déployé sur les SI industriels (automates et postes de travail) une protection anti-malwares/anti-virus basée sur les signatures ? Quelle solution est mise en place ? L'ensemble du périmètre est-il couvert ? Quelle est la fréquence et quelles sont les modalités de mise à jour ?	0	RAS
236	Un processus de déploiement des correctifs de sécurité sur les SI industriels (automates et postes de travail) est-il mis en œuvre ? Avec quel outillage ? Est-il automatisé ? Est-il formalisé ? Une veille sécurité est-elle réalisée concernant la gestion des vulnérabilités (e.g. abonnement newsletter CSIRT…) sur les SI industriels ?	0	RAS
237	Comment les services d'infrastructure et de sécurité (e.g. antivirus, SCCM, NTP…) sont-ils fournis aux réseaux industriels ?	0	RAS
238	Les actifs industriels obsolètes, ou en passe de l'être, sont-ils identifiés ? Si Retenu, font-ils l'objet de mesures correctives (mise à jour, remplacement…) ou, si ce n'est pas possible, sont-ils protégés par des mesures spécifiques de réduction des risques (e.g. isolement du réseau) ?	0	RAS
239	Des dérogations et exceptions de sécurité sont-elles réalisées au niveau du SI Industriel ? Si Retenu, font-elles l'objet d'un processus formalisé et tracé ? Qui réalise ces dérogations ? Ces dérogations sont-elles à durée limitée ?	0	RAS
240	Les journaux des SI industriels concernant les évènements de sécurité sont-ils collectés ? Quelles sont les traces générées et les périmètres concernés ? Les journaux sont-ils stockés localement ou centralisés (au sein d'un puit de logs ou d'un SIEM) et disponibles pour preuve ? Quelle est la durée de rétention des journaux ? Comment sont exploités les journaux des SI industriels concernant les évènements de sécurité (e.g. analyse ponctuelle suite à évènement, dans un SIEM…) ?	0	RAS
241	Est-ce que le périmètre industriel est inclus dans le périmètre de gestion des incidents et de gestion de crise ? Est-ce que les spécificités du monde industriel sont prises en compte ?	0	RAS
242	Une politique de sauvegarde (précisant notamment les périmètres à couvrir, les fréquences associés et les outils utilisés) est-elle définie pour les SI industriels ? Est-elle communiquée aux parties prenantes ? Est-elle mise en œuvre ? Les sauvegardes sont-elles testées ?	0	RAS
243	Un plan de reconstruction des automates et des terminaux en cas d'attaque a-t-il été défini ? Est-il testé ?	0	RAS
244	Des audits (techniques et organisationnels, hors audit prestataires) sont-ils réalisés ? Sur quels périmètres (hors applications et SI industriels) ? A quelle fréquence ? Une stratégie d'audit est-elle définie annuellement ?	0	RAS
245	Avez-vous réalisé un audit red-team ?	0	RAS
246	Un plan d'action est-il établi et mis en œuvre après chaque audit ? Sa mise en œuvre est-elle contrôlée ?	0	RAS
247	A quels référentiels de sécurité est soumise l'organisation (e.g. NIS, RGPD, LPM, NIST, ISO 27000, PSSI-E…) ? La conformité à ces référentiels est-vérifiée ?	0	RAS

2.Plans d'actions

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
1	XX	XX	XX	XX	XX	XX	XX	XX
2	XX	XX	XX	XX	XX	XX	XX	XX
3	XX	XX	XX	XX	XX	XX	XX	XX
4	XX	XX	XX	XX	XX	XX	XX	XX
5	XX	XX	XX	XX	XX	XX	XX	XX
6	XX	XX	XX	XX	XX	XX	XX	XX
7	XX	XX	XX	XX	XX	XX	XX	XX
8	XX	XX	XX	XX	XX	XX	XX	XX
9	XX	XX	XX	XX	XX	XX	XX	XX
10	XX	XX	XX	XX	XX	XX	XX	XX
11	XX	XX	XX	XX	XX	XX	XX	XX
12	XX	XX	XX	XX	XX	XX	XX	XX
13	XX	XX	XX	XX	XX	XX	XX	XX
14	XX	XX	XX	XX	XX	XX	XX	XX
15	XX	XX	XX	XX	XX	XX	XX	XX
16	XX	XX	XX	XX	XX	XX	XX	XX
17	XX	XX	XX	XX	XX	XX	XX	XX
18	XX	XX	XX	XX	XX	XX	XX	XX
19	XX	XX	XX	XX	XX	XX	XX	XX
20	XX	XX	XX	XX	XX	XX	XX	XX
21	XX	XX	XX	XX	XX	XX	XX	XX
22	XX	XX	XX	XX	XX	XX	XX	XX
23	XX	XX	XX	XX	XX	XX	XX	XX
24	XX	XX	XX	XX	XX	XX	XX	XX
25	XX	XX	XX	XX	XX	XX	XX	XX
26	XX	XX	XX	XX	XX	XX	XX	XX
27	XX	XX	XX	XX	XX	XX	XX	XX
28	XX	XX	XX	XX	XX	XX	XX	XX
29	XX	XX	XX	XX	XX	XX	XX	XX
30	XX	XX	XX	XX	XX	XX	XX	XX
31	XX	XX	XX	XX	XX	XX	XX	XX
32	XX	XX	XX	XX	XX	XX	XX	XX
33	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
34	XX	XX	XX	XX	XX	XX	XX	XX
35	XX	XX	XX	XX	XX	XX	XX	XX
36	XX	XX	XX	XX	XX	XX	XX	XX
37	XX	XX	XX	XX	XX	XX	XX	XX
38	XX	XX	XX	XX	XX	XX	XX	XX
39	XX	XX	XX	XX	XX	XX	XX	XX
40	XX	XX	XX	XX	XX	XX	XX	XX
41	XX	XX	XX	XX	XX	XX	XX	XX
42	XX	XX	XX	XX	XX	XX	XX	XX
43	XX	XX	XX	XX	XX	XX	XX	XX
44	XX	XX	XX	XX	XX	XX	XX	XX
45	XX	XX	XX	XX	XX	XX	XX	XX
46	XX	XX	XX	XX	XX	XX	XX	XX
47	XX	XX	XX	XX	XX	XX	XX	XX
48	XX	XX	XX	XX	XX	XX	XX	XX
49	XX	XX	XX	XX	XX	XX	XX	XX
50	XX	XX	XX	XX	XX	XX	XX	XX
51	XX	XX	XX	XX	XX	XX	XX	XX
52	XX	XX	XX	XX	XX	XX	XX	XX
53	XX	XX	XX	XX	XX	XX	XX	XX
54	XX	XX	XX	XX	XX	XX	XX	XX
55	XX	XX	XX	XX	XX	XX	XX	XX
56	XX	XX	XX	XX	XX	XX	XX	XX
57	XX	XX	XX	XX	XX	XX	XX	XX
58	XX	XX	XX	XX	XX	XX	XX	XX
59	XX	XX	XX	XX	XX	XX	XX	XX
60	XX	XX	XX	XX	XX	XX	XX	XX
61	XX	XX	XX	XX	XX	XX	XX	XX
62	XX	XX	XX	XX	XX	XX	XX	XX
63	XX	XX	XX	XX	XX	XX	XX	XX
64	XX	XX	XX	XX	XX	XX	XX	XX
65	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
66	XX	XX	XX	XX	XX	XX	XX	XX
67	XX	XX	XX	XX	XX	XX	XX	XX
68	XX	XX	XX	XX	XX	XX	XX	XX
69	XX	XX	XX	XX	XX	XX	XX	XX
70	XX	XX	XX	XX	XX	XX	XX	XX
71	XX	XX	XX	XX	XX	XX	XX	XX
72	XX	XX	XX	XX	XX	XX	XX	XX
73	XX	XX	XX	XX	XX	XX	XX	XX
74	XX	XX	XX	XX	XX	XX	XX	XX
75	XX	XX	XX	XX	XX	XX	XX	XX
76	XX	XX	XX	XX	XX	XX	XX	XX
77	XX	XX	XX	XX	XX	XX	XX	XX
78	XX	XX	XX	XX	XX	XX	XX	XX
79	XX	XX	XX	XX	XX	XX	XX	XX
80	XX	XX	XX	XX	XX	XX	XX	XX
81	XX	XX	XX	XX	XX	XX	XX	XX
82	XX	XX	XX	XX	XX	XX	XX	XX
83	XX	XX	XX	XX	XX	XX	XX	XX
84	XX	XX	XX	XX	XX	XX	XX	XX
85	XX	XX	XX	XX	XX	XX	XX	XX
86	XX	XX	XX	XX	XX	XX	XX	XX
87	XX	XX	XX	XX	XX	XX	XX	XX
88	XX	XX	XX	XX	XX	XX	XX	XX
89	XX	XX	XX	XX	XX	XX	XX	XX
90	XX	XX	XX	XX	XX	XX	XX	XX
91	XX	XX	XX	XX	XX	XX	XX	XX
92	XX	XX	XX	XX	XX	XX	XX	XX
93	XX	XX	XX	XX	XX	XX	XX	XX
94	XX	XX	XX	XX	XX	XX	XX	XX
95	XX	XX	XX	XX	XX	XX	XX	XX
96	XX	XX	XX	XX	XX	XX	XX	XX
97	XX	XX	XX	XX	XX	XX	XX	XX
98	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
99	XX	XX	XX	XX	XX	XX	XX	XX
100	XX	XX	XX	XX	XX	XX	XX	XX
101	XX	XX	XX	XX	XX	XX	XX	XX
102	XX	XX	XX	XX	XX	XX	XX	XX
103	XX	XX	XX	XX	XX	XX	XX	XX
104	XX	XX	XX	XX	XX	XX	XX	XX
105	XX	XX	XX	XX	XX	XX	XX	XX
106	XX	XX	XX	XX	XX	XX	XX	XX
107	XX	XX	XX	XX	XX	XX	XX	XX
108	XX	XX	XX	XX	XX	XX	XX	XX
109	XX	XX	XX	XX	XX	XX	XX	XX
110	XX	XX	XX	XX	XX	XX	XX	XX
111	XX	XX	XX	XX	XX	XX	XX	XX
112	XX	XX	XX	XX	XX	XX	XX	XX
113	XX	XX	XX	XX	XX	XX	XX	XX
114	XX	XX	XX	XX	XX	XX	XX	XX
115	XX	XX	XX	XX	XX	XX	XX	XX
116	XX	XX	XX	XX	XX	XX	XX	XX
117	XX	XX	XX	XX	XX	XX	XX	XX
118	XX	XX	XX	XX	XX	XX	XX	XX
119	XX	XX	XX	XX	XX	XX	XX	XX
120	XX	XX	XX	XX	XX	XX	XX	XX
121	XX	XX	XX	XX	XX	XX	XX	XX
122	XX	XX	XX	XX	XX	XX	XX	XX
123	XX	XX	XX	XX	XX	XX	XX	XX
124	XX	XX	XX	XX	XX	XX	XX	XX
125	XX	XX	XX	XX	XX	XX	XX	XX
126	XX	XX	XX	XX	XX	XX	XX	XX
127	XX	XX	XX	XX	XX	XX	XX	XX
128	XX	XX	XX	XX	XX	XX	XX	XX
129	XX	XX	XX	XX	XX	XX	XX	XX
130	XX	XX	XX	XX	XX	XX	XX	XX
131	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
132	XX	XX	XX	XX	XX	XX	XX	XX
133	XX	XX	XX	XX	XX	XX	XX	XX
134	XX	XX	XX	XX	XX	XX	XX	XX
135	XX	XX	XX	XX	XX	XX	XX	XX
136	XX	XX	XX	XX	XX	XX	XX	XX
137	XX	XX	XX	XX	XX	XX	XX	XX
138	XX	XX	XX	XX	XX	XX	XX	XX
139	XX	XX	XX	XX	XX	XX	XX	XX
140	XX	XX	XX	XX	XX	XX	XX	XX
141	XX	XX	XX	XX	XX	XX	XX	XX
142	XX	XX	XX	XX	XX	XX	XX	XX
143	XX	XX	XX	XX	XX	XX	XX	XX
144	XX	XX	XX	XX	XX	XX	XX	XX
145	XX	XX	XX	XX	XX	XX	XX	XX
146	XX	XX	XX	XX	XX	XX	XX	XX
147	XX	XX	XX	XX	XX	XX	XX	XX
148	XX	XX	XX	XX	XX	XX	XX	XX
149	XX	XX	XX	XX	XX	XX	XX	XX
150	XX	XX	XX	XX	XX	XX	XX	XX
151	XX	XX	XX	XX	XX	XX	XX	XX
152	XX	XX	XX	XX	XX	XX	XX	XX
153	XX	XX	XX	XX	XX	XX	XX	XX
154	XX	XX	XX	XX	XX	XX	XX	XX
155	XX	XX	XX	XX	XX	XX	XX	XX
156	XX	XX	XX	XX	XX	XX	XX	XX
157	XX	XX	XX	XX	XX	XX	XX	XX
158	XX	XX	XX	XX	XX	XX	XX	XX
159	XX	XX	XX	XX	XX	XX	XX	XX
160	XX	XX	XX	XX	XX	XX	XX	XX
161	XX	XX	XX	XX	XX	XX	XX	XX
162	XX	XX	XX	XX	XX	XX	XX	XX
163	XX	XX	XX	XX	XX	XX	XX	XX
164	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
165	XX	XX	XX	XX	XX	XX	XX	XX
166	XX	XX	XX	XX	XX	XX	XX	XX
167	XX	XX	XX	XX	XX	XX	XX	XX
168	XX	XX	XX	XX	XX	XX	XX	XX
169	XX	XX	XX	XX	XX	XX	XX	XX
170	XX	XX	XX	XX	XX	XX	XX	XX
171	XX	XX	XX	XX	XX	XX	XX	XX
172	XX	XX	XX	XX	XX	XX	XX	XX
173	XX	XX	XX	XX	XX	XX	XX	XX
174	XX	XX	XX	XX	XX	XX	XX	XX
175	XX	XX	XX	XX	XX	XX	XX	XX
176	XX	XX	XX	XX	XX	XX	XX	XX
177	XX	XX	XX	XX	XX	XX	XX	XX
178	XX	XX	XX	XX	XX	XX	XX	XX
179	XX	XX	XX	XX	XX	XX	XX	XX
180	XX	XX	XX	XX	XX	XX	XX	XX
181	XX	XX	XX	XX	XX	XX	XX	XX
182	XX	XX	XX	XX	XX	XX	XX	XX
183	XX	XX	XX	XX	XX	XX	XX	XX
184	XX	XX	XX	XX	XX	XX	XX	XX
185	XX	XX	XX	XX	XX	XX	XX	XX
186	XX	XX	XX	XX	XX	XX	XX	XX
187	XX	XX	XX	XX	XX	XX	XX	XX
188	XX	XX	XX	XX	XX	XX	XX	XX
189	XX	XX	XX	XX	XX	XX	XX	XX
190	XX	XX	XX	XX	XX	XX	XX	XX
191	XX	XX	XX	XX	XX	XX	XX	XX
192	XX	XX	XX	XX	XX	XX	XX	XX
193	XX	XX	XX	XX	XX	XX	XX	XX
194	XX	XX	XX	XX	XX	XX	XX	XX
195	XX	XX	XX	XX	XX	XX	XX	XX
196	XX	XX	XX	XX	XX	XX	XX	XX
197	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
198	XX	XX	XX	XX	XX	XX	XX	XX
199	XX	XX	XX	XX	XX	XX	XX	XX
200	XX	XX	XX	XX	XX	XX	XX	XX
201	XX	XX	XX	XX	XX	XX	XX	XX
202	XX	XX	XX	XX	XX	XX	XX	XX
203	XX	XX	XX	XX	XX	XX	XX	XX
204	XX	XX	XX	XX	XX	XX	XX	XX
205	XX	XX	XX	XX	XX	XX	XX	XX
206	XX	XX	XX	XX	XX	XX	XX	XX
207	XX	XX	XX	XX	XX	XX	XX	XX
208	XX	XX	XX	XX	XX	XX	XX	XX
209	XX	XX	XX	XX	XX	XX	XX	XX
210	XX	XX	XX	XX	XX	XX	XX	XX
211	XX	XX	XX	XX	XX	XX	XX	XX
212	XX	XX	XX	XX	XX	XX	XX	XX
213	XX	XX	XX	XX	XX	XX	XX	XX
214	XX	XX	XX	XX	XX	XX	XX	XX
215	XX	XX	XX	XX	XX	XX	XX	XX
216	XX	XX	XX	XX	XX	XX	XX	XX
217	XX	XX	XX	XX	XX	XX	XX	XX
218	XX	XX	XX	XX	XX	XX	XX	XX
219	XX	XX	XX	XX	XX	XX	XX	XX
220	XX	XX	XX	XX	XX	XX	XX	XX
221	XX	XX	XX	XX	XX	XX	XX	XX
222	XX	XX	XX	XX	XX	XX	XX	XX
223	XX	XX	XX	XX	XX	XX	XX	XX
224	XX	XX	XX	XX	XX	XX	XX	XX
225	XX	XX	XX	XX	XX	XX	XX	XX
226	XX	XX	XX	XX	XX	XX	XX	XX
227	XX	XX	XX	XX	XX	XX	XX	XX
228	XX	XX	XX	XX	XX	XX	XX	XX
229	XX	XX	XX	XX	XX	XX	XX	XX
230	XX	XX	XX	XX	XX	XX	XX	XX

ID	Score actuel	Actions	Priorité	Score après plan d'actions P0/P1	Score après plan d'actions P2	Score après plan d'actions P3	Coûts projet	Coûts récurrents
231	XX	XX	XX	XX	XX	XX	XX	XX
232	XX	XX	XX	XX	XX	XX	XX	XX
233	XX	XX	XX	XX	XX	XX	XX	XX
234	XX	XX	XX	XX	XX	XX	XX	XX
235	XX	XX	XX	XX	XX	XX	XX	XX
236	XX	XX	XX	XX	XX	XX	XX	XX
237	XX	XX	XX	XX	XX	XX	XX	XX
238	XX	XX	XX	XX	XX	XX	XX	XX
239	XX	XX	XX	XX	XX	XX	XX	XX
240	XX	XX	XX	XX	XX	XX	XX	XX
241	XX	XX	XX	XX	XX	XX	XX	XX
242	XX	XX	XX	XX	XX	XX	XX	XX
243	XX	XX	XX	XX	XX	XX	XX	XX
244	XX	XX	XX	XX	XX	XX	XX	XX
245	XX	XX	XX	XX	XX	XX	XX	XX
246	XX	XX	XX	XX	XX	XX	XX	XX
247	XX	XX	XX	XX	XX	XX	XX	XX