



MARCHÉ PUBLIC ASSURANCE

Questionnaire Cyber risques

Description des principales activités / compétences :

Activités contrôlées par le système d'information :

☒ Gestion du personnel	☒ Comptabilité	☒ État civil
☒ Urbanisme	☒ Marchés publics	☒ Gestion des listes électorales
☒ Gestion des établissements scolaires	☐ Gestion des prestations sociales	☐ Gestion des crèches
☐ Foyers personnes âgées	☐ Autres :	

Disposez-vous d'équipements matériels/industriels contrôlés par le système d'information (machines, vannes, signalisation urbaine, etc.)

☐ OUI

☒ NON

	< 10	11 - 50	51 - 100	> 100
Nombre d'utilisateurs des SI	☐	☒	☐	☐
Nombre de postes mobiles	☒	☐	☐	☐
Nombre de serveurs administrés en interne	☒	☐	☐	☐
Avez-vous un site web de service en ligne ?	☐ OUI ☒ NON			
Si oui, quelle est la part de CA généré par le site web ?	% ou €			

Les questions de cyber sécurité font-elles l'objet d'un chapitre dans le PCS ?

☐ OUI ☐ NON

Externalisation du système d'information :

Quelles sont les fonctions informatiques externalisées ?	OUI	NON	Nom du fournisseur de service
Gestion des postes de travail	☒	☐	CS prestation
Gestion des serveurs	☒	☐	"
Gestion du réseau	☒	☐	"
Gestion du site web	☒	☐	Intramuros
Gestion d'applications (comptabilité, paye, CRM, ...)	☒	☐	Begeer - Leveult
Autres, à préciser :	☐	☐	

Budgets et personnel :

Budget informatique annuel :

Pourcentage du budget informatique alloué à la cybersécurité : %

Effectif équipes informatiques : 1

Effectif dédié en cybersécurité : 1

Point de contact cybersécurité (RSSI ou rôle équivalent) :

Nom : R. V. TA R. D.

Titre : Responsable

Email : maine@celle4011.fr

Téléphone : 06 75 26 90 16

Appréciation générale du risque

	OUI	NON
Les comptes d'accès au SI sont nominatifs en très grande majorité ou en totalité	☒	☐
Les mots de passe initiaux sur les équipements matériels ou les logiciels sont changés systématiquement, en respectant les bonnes pratiques de complexité ?	☒	☐
Les utilisateurs standards disposent de droits d'administration sur les postes de travail	☐	☒
Les postes de travail sont équipés d'un anti-virus	☒	☐
Les exécutions automatiques (à l'insertion d'un périphérique amovible, ou l'ouverture d'un partage réseau par exemple) sont désactivées	☒	☐
Interdisez-vous la connexion d'équipements personnels sur votre réseau ?	☒	☐
Si vous disposez d'un système d'information industriel ou de matériels contrôlés par le système d'information, sont-ils isolés du système d'information de gestion ?	☒	☐
Avez-vous des accès internet en libre-service (type borne) ?	☐	☒
Si oui, est-il possible depuis cet accès libre-service, d'accéder au reste du SI ?	☐	☐
Avez-vous des réseaux Wifi ?	☒	☐
Si oui : - les équipements personnels ou ceux de visiteurs voire du public, utilisent-ils un réseau Wifi dédié et isolé du reste de votre réseau	☐	☒
- le réseau Wifi professionnel utilise-t-il un chiffrement robuste (WPA2/AES) ?	☒	☐
Vous disposez d'un pare-feu au niveau de l'accès Internet, pour interdire les accès directs à votre SI, en dehors de services en ligne cloisonnés ou d'accès distants bien définis, et pour filtrer les connexions directes sortantes	☒	☐
Votre système d'information est connecté à d'autres SI	☒	☐
Si oui : - Utilisez-vous un canal sécurisé assurant la confidentialité (type VPN) ?	☒	☐
- Filtrez-vous ces accès au strict nécessaire ?	☒	☐
Le stockage des terminaux nomades est chiffré	☐	☒
Les terminaux nomades peuvent se connecter au SI à distance	☒	☐
Si oui : - Ils utilisent un canal d'échange sécurisé (type VPN)	☒	☐
- Ils passent en toute circonstance par votre réseau pour consulter Internet	☐	☒
Vous avez défini une politique de mise à jour des systèmes et logiciels	☒	☐
Que vous ayez une politique ou non, les correctifs les plus critiques sont appliqués rapidement (sous 5j maximum)	☒	☐
Avez-vous des systèmes obsolètes n'étant plus maintenus par leur éditeur ?	☐	☒
Si oui : - Ont-ils été isolés au sein du réseau ?	☐	☐
- Avez-vous planifié leur migration/remplacement ?	☐	☐
Avez-vous mis en œuvre des sauvegardes des systèmes ?	☒	☐
Si oui : - Pour toutes les données (oui) ? Ou seulement les données critiques(non) ?	☒	
Selon quelle fréquence ?		
- Les sauvegardes sont-elles extraites hors-ligne, en lieu sûr ?		☒
- Disposez-vous de plusieurs copies des sauvegardes en des lieux séparés ?	☒	☐
- Les sauvegardes sont-elles dans la même salle que les systèmes sauvegardés ?	☐	☒
- Effectuez-vous des tests réguliers de restauration pour vous assurer que les sauvegardes sont utilisables en cas de besoin ?	☐	☒

Sensibilisation et formation ?

	OUI	NON
Les équipes informatiques suivent des formations sur la sécurité des systèmes d'information (risques et menaces : ransomwares, phishing ou hameçonnage ; authentification et contrôle d'accès, cloisonnement réseau, etc.)	☒	☐
L'utilisateur est informé des règles à respecter et des bons comportements de sécurité dans l'usage de l'informatique et d'Internet (informations sensibles, usage des mots de passe, signalement, verrouillage de session, etc.) Si oui : - dès son arrivée - régulièrement	☐ ☐ ☐	☒ ☒ ☒
Les personnels disposant de terminaux nomades (ordinateur portable, smartphone, tablette) sont sensibilisés aux risques spécifiques du nomadisme (perte, vol, accès distant au SI)	☐	☒
Exigez-vous une formation supplémentaire pour les employés qui échouent aux simulations d'e-mails de phishing ?	☐	☒
Faites-vous appel à des prestations d'infogérance ? Si oui, existe-t-il un document contractuel décrivant l'ensemble des engagements pour garantir le respect des exigences de sécurité (réversibilité, audits, sauvegarde, maintien à niveau de sécurité, etc.) ?	☒ ☒	☐ ☐

A quelle fréquence conduisez-vous la formation suivante pour tous les employés ?

Type de Formation	Jamais/pas régulièrement	Annuellement	2X par an voir plus
Formation interactive sur le phishing	☒	☐	☐
Campagne de phishing	☒	☐	☐

Connaître le système d'information

	OUI	NON
Avez-vous identifié vos données sensibles ? (Identification, données de santé, etc.) Si oui, avez-vous inventorié leur localisation (bases de données, partages de fichiers, postes de travail, etc.)	☒ ☒	☐ ☐
Conservez-vous une cartographie des équipements en lien avec ces localisations, ainsi que des équipements de sécurité qui les protègent ?	☒	☐
Disposez-vous d'un inventaire exhaustif des comptes utilisateurs privilégiés dans votre SI qui indique leur usage ? (Il s'agit des comptes d'utilisateurs de niveau administrateur, les comptes d'utilisateurs permettant d'accéder aux répertoires de travail des responsables ou de tous les utilisateurs, et les comptes d'utilisateurs d'un poste non administré par le service informatique ou sans les mesures de sécurité nécessaires.)	☒	☐
Disposez-vous d'un inventaire des comptes techniques de services et d'administration ?	☐	☒
Lorsqu'un utilisateur change de fonction ou de missions, ses droits sont-ils revus pour supprimer ceux qui ne lui sont plus nécessaires ?	☒	☐
Les droits affectés à une personne sont-ils révoqués lors de son départ ?	☒	☐
Utilisez-vous une configuration de base renforcée sur vos appareils ?	☒	☐

Quel pourcentage de l'entreprise est couvert par des scans de vulnérabilité planifiés ? 0 %

Au cours des deux dernières années, à quelle fréquence avez-vous effectué un scan des vulnérabilités des périphériques de votre réseau ?

☒ Jamais/pas ☐ Régulièrement, annuellement ☐ 2-3 fois par an ☒ Trimestriel ou plus souvent

Au cours des deux dernières années, quelle est la durée moyenne que votre organisation a prise pour corriger les vulnérabilités et expositions communes critiques (CVE critiques) (CVSS version 3.1 score de base 9.0-10.0) sur votre réseau ?

☐ Inconnu ☐ supérieur à 2 semaines ☒ inférieur à 1 semaine ☐ moins de 48 heures

A quelle fréquence effectuez-vous (ou un tiers en votre nom) des tests d'intrusion sur votre réseau ?

☒ Jamais/pas ☐ Régulièrement, annuellement ☐ 2-3 fois par an ☐ Trimestriel ou plus souvent

Authentifier et contrôler les accès

	OUI	NON
Les comptes génériques (donc non nominatifs) sont en nombre restreint et les personnes qui les utilisent sont connues	☒	☐
Les utilisateurs ayant une fonction d'administration du SI disposent d'un compte personnel standard sans privilèges, et d'un compte personnel dédié exclusivement aux opérations d'administration, avec un mot de passe différent	☒	☐
Toutes les actions liées aux comptes sont journalisées (connexion réussies/échouées, compte ajouté, désactivé, etc.)	☒	☐
Avez-vous défini des habilitations pour limiter les accès aux données sensibles ?	☒	☐
Effectuez-vous une revue régulière des droits d'accès sur les emplacements contenant des données sensibles pour détecter des anomalies ?	☐	☒
Le mot de passe de l'utilisateur respecte des règles de complexité (ex : longueur minimale de 8 caractères, typologies variées de caractères, etc.)	☐	☒
Un nombre répété de tentatives infructueuses de connexion verrouille le compte de l'utilisateur	☐	☒
Possédez-vous des dispositifs d'authentification forte pour les accès ou les opérations sensibles ?	☐	☒
Exigez-vous l'authentification multi-facteur (MFA) pour tous <u>les utilisateurs à hauts privilèges</u> de votre réseau ? MFA inclut notamment les éléments suivants ; un appel, un SMS, une notification push, un mot de passe à usage unique, un jeton OATH, un jeton matériel, un certificat lié à l'appareil, des applications d'authentification, la biométrie ou une clé FIDO2.	☐	☒
Exigez-vous l'authentification multi-facteur (MFA) pour <u>tous les utilisateurs</u> de votre réseau pour les accès à distance ? Les utilisateurs comprennent les employés et (le cas échéant) les étudiants, les bénévoles, les stagiaires, les sous-traitants tiers et toute autre personne disposant d'un compte utilisateur sur votre réseau.	☐	☒
Autorisez-vous les utilisateurs à accéder à distance à la messagerie WEB (par exemple : Outlook Web Access OWA) ?	☒	☐
Si « OUI », exigez-vous l'authentification multi-facteur (MFA) pour l'accès aux e-mails Web ?	☐	☒
Autorisez-vous les utilisateurs ordinaires à avoir des droits d'administrateur local sur leurs appareils (par exemple les ordinateurs portables) ?	☐	☒
Utilisez-vous un outil de gestion des accès privilégiés (PAM) ?	☐	☒
Fournissez-vous à vos employés un logiciel des mots de passe ?	☐	☒

Sécuriser les postes

	OUI	NON
La session de l'utilisateur se verrouille automatiquement en cas d'inactivité	☒	☐
L'inventaire des données selon leur niveau de sensibilité est réalisé ?	☐	☒
Les données les plus importantes sur les postes de travail font l'objet de sauvegardes régulières et déconnectées	☐	☐
Les périphériques amovibles sont automatiquement inspectés par l'anti-virus du poste de travail	☒	☐

tout sur le lieu

La gestion des politiques de sécurité des postes de travail est centralisée (Il s'agit de l'application des politiques de mots de passe, les restrictions de certains postes sensibles, les configurations de certaines applications comme les navigateurs web, etc. Il s'agit communément de « GPO » ou équivalent.)	☒	☐
La gestion des politiques de sécurité des serveurs est centralisée	☒	☐
Les postes de travail disposent d'un pare-feu local	☒	☐
Si oui, le pare-feu local autorise l'accès aux protocoles d'administration du poste de travail uniquement aux équipes chargées de l'administration	☒	☐
Avez-vous un service SOC (Centre Opérationnel de Sécurité) ?	☐	☒
Si « OUI », votre SOC est-il interne ou géré par un tiers ?	☐	☐
Si « OUI », votre SOC a-t-il les accès et les autorisations pour répondre aux incidents ? (Par exemple, en isolant et en contenant les terminaux à distance) ?	☐	☐
Utilisez-vous un service de protection DNS (par exemple : QUAD9, OpenDNS ou PDNS du secteur public) ?	☐	☒
Les pare-feux réseau et systèmes sont-ils configurés pour interdire les connexions entrantes par défaut ?	☒	☐
Utilisez-vous un RDP (Remote Desktop Protocol), virtual Network Computing (VNC), AnyDesk, TeamViewer ou d'autres logiciels de bureau à distance ?	☒	☐
Si « OUI », l'accès nécessite-t-il une authentification multi-facteur ?	☐	☒
Refusez-vous toutes les connexions en direct depuis internet de type SMB (Server Message Block) (c'est-à-dire le partage de fichiers Windows) vers les serveurs (sauf en cas de besoin métier identifié) ?	☒	☐

Comptes de service

Combien y a-t-il de comptes de service avec des privilèges d'administrateur de domaine dans votre environnement informatique ? Ces « comptes de service » sont des comptes privilégiés non humains utilisés pour exécuter des applications, accéder aux ressources locales et réseau et exécuter des services automatisés, des instances de machine virtuelle et d'autres processus.

☐10 ☐6-10 ☒1-5 ☐0

	OUI	NON
Configurez-vous des comptes de services en utilisant le principe du moindre privilège ? (C'est-à-dire, avez-vous supprimé les privilèges d'administrateur de domaine des comptes de service qui n'ont pas besoin de tels privilèges pour fonctionner ?)	☒	☐
Avez-vous mis en place des règles de surveillance spécifiques pour alerter votre Centre Opérationnel de Sécurité (SOC) de tout comportement anormal lié aux comptes de service ?	☐	☒
Avez-vous configuré des comptes de service pour refuser les connexions interactives ?	☐	☒
Exigez-vous que les mots de passe supérieur à 25 caractères ou générés de manière aléatoire pour les comptes de service ?	☒	☐
Exigez-vous un changement régulier des mots de passe des comptes de services ?	☒	☐
Gérez-vous les mots de passe pour les comptes de services avec une solution PAM ou un coffre-fort de mots de passe ?	☐	☒

Sécuriser le réseau

	OUI	NON
Le réseau est découpé en différentes zones logiques (adressage) Si oui : - Un pare-feu limite et filtre les échanges entre les différentes zones, et plus spécifiquement entre postes de travail et serveurs - Les postes de travail des équipes d'administration se trouvent sur un réseau logique isolé de celui des postes de travail standards	☐	☒
Les flux Internet sont inspectés (analyse antivirus, filtrage par catégories de site, etc.)	☒	☐
Vous disposez d'un équipement capable d'effectuer une analyse antivirus des messages électroniques reçus avant qu'ils ne soient déposés dans les boîtes aux lettres	☒	☐
Vous disposez d'un anti-spam capable de filtrer les messages malveillants reçus	☒	☐
Les salles serveurs et locaux techniques sont des zones d'accès restreint	☐	☒
Le contrat d'hébergement de votre site intègre-t-il une solution anti-DDoS	☐	☐
Désactivez-vous par défaut les macros dans vos logiciels bureautiques (par exemple, Microsoft Office, Google Workspace) ?	☒	
Si « OUI », les utilisateurs sont-ils autorisés à activer les macros ?	☒	☐
Avez-vous désactivé les protocoles de messagerie qui utilisent l'authentification de base (nom d'utilisateur et mot de passe uniquement), tels que IMAP, POP3 et SMTP ?	☐	☒
Utilisez-vous une solution de sauvegarde hébergée sur votre réseau d'entreprise ?	☒	☐
Utilisez-vous des sauvegardes hébergées sur le cloud ? Si « OUI », votre service de sauvegarde basé sur le cloud est-il un « service de réplication automatique » ? (Exemple : DropBox , OneDrive, SharePoint, Google Drive)		☒
Maintenez-vous des sauvegardes hors ligne ?	☐	☒
Toutes vos sauvegardes sont-elles chiffrées ?	☒	☐
Maintenez-vous une sauvegarde hors ligne de votre (vos) clé(s) de déchiffrement pour vos sauvegardes chiffrées ? (Ignorez cette question si vous n'avez pas de sauvegardes chiffrées.)	☒	☐
Certaines de vos solutions de sauvegarde sont-elles 'immuables' ? (Les sauvegardes immuables ne peuvent pas être modifiées ou supprimées.)	☐	☒
Testez-vous l'intégralité des sauvegardes avant la restauration pour être sûr que vos sauvegardes ne contiennent pas de logiciels malveillants ?	☐	☒

Quelle licence Microsoft 365 (ou licence équivalente) utilisez-vous pour tous, ou presque, tous vos utilisateurs ? ☐E1 ☐E3 ☐E5 ☒Autre ☐Aucune

Si vous utilisez Microsoft 365, utilisez-vous le module complémentaire Microsoft 365 Défender (Advanced Threat Protection) ou un produit cybersecurity équivalent avec des fonctionnalités Advanced Threat Hunting ? ☐OUI ☒NON

Superviser, auditer, réagir

	OUI	NON
Disposez-vous de journaux pertinents pour détecter des tentatives d'accès illicites ?	☐	☒
Effectuez-vous des audits réguliers de votre SI pour analyser ses vulnérabilités ?	☐	☒
Si oui, les recommandations sont-elles mises en œuvre ?	☐	☐
Disposez-vous d'une personne référente de la sécurité du SI ?	☒	☐

Continuité

	OUI	NON
Avez-vous défini et mis en œuvre un plan de reprise d'activité informatique ?	☐	☒
Avez-vous défini et mis en œuvre un plan de continuité d'activité informatique ?	☐	☒
Vos équipements principaux sont-ils redondés ?	☐	☒
Si oui, la redondance est-elle effectuée sur plusieurs salles informatiques ?	☐	☐
Avez-vous sécurisé l'alimentation en électricité de vos systèmes (onduleur, redondance électrique, groupe électrogène, etc.) ?	☐	☒
La ou les salles informatiques sont équipées des dispositifs de protection spécifiques contre l'incendie ?	☐	☒
Avez-vous mené, au cours des deux dernières années, un exercice de simulation de crise ?	☐	☒
Si « OUI », cet exercice incluait-il une attaque par rançongiciel ?	☐	☐

Logiciel en fin de support et/ou en fin de vie

	OUI	NON
Utilisez-vous un outil de découverte qui détecte en permanence les périphériques connectés à votre réseau interne ?	☐	☒
Disposez-vous d'une base de données de vos équipements IT à jour ?	☐	☒
Disposez-vous d'un inventaire de logiciel, matériel et configuration (CMDB) à jour ?	☐	☒
Existe-t-il des systèmes ou des logiciels en fin de vie ou de fin de support (EOL) sur votre réseau ?	☐	☒
Si « OUI », ces logiciels sont-ils isolés du reste du réseau ?	☐	☐

Criticité des Systèmes d'Information

Certification ISO 27001 ☒ oui ☐ non

Existe-t-il un accès distant au système d'information de la Collectivité (VPN ou extranet) ? ☒ oui ☐ non

• La Collectivité autorise-t-elle la connexion au SI d'équipements personnels ? ☐ oui ☒ non

A partir de quelle durée d'interruption de vos Systèmes d'Information vos activités subiront-elles un impact quantifiable ?

Application (ou Activité)	Durée maximale d'une interruption avant impact sur l'activité				
	Immédiat	Max 24 h	Max 72 h	Max 7 j	Au-delà (précisez)
Service	☒	☐	☐	☐	
messagerie	☐	☒	☐	☐	
Berger-Levrault	☐	☒	☐	☐	
	☐	☐	☐	☐	

Autres contrôles de cybersécurité et mesures préventives

Veuillez utiliser l'espace ci-dessous pour clarifier les réponses ci-dessus qui pourraient être incomplètes ou nécessiter des détails complémentaires. Veuillez également décrire toutes les mesures prises par votre organisation pour détecter, prévenir et remédier aux attaques rançongiciels (par exemple : segmentation de votre réseau, contrôles de sécurité logiciels supplémentaires, services de sécurité externes, etc.)

Antispam : mailing-black
firewall : wha tech guard T40
antivirus : bit defender.