Version 3.0 | 01.03.2026

CyberSeal
Liste des points de contrôle

Cap.	Pt.	Contrôle	Prio	Méthode d'audit: A=Autodéclaration E=Entretien T=Terminaux (console)
5.1		**Répartition des tâches client/fournisseur de services informatiques**		
	1	Il existe un accord écrit sur la répartition des tâches avec tous les clients (par ex. un SLA, un contrat de maintenance, une description de service).	1	E
	2	Il existe une personne/un rôle responsable de la cybersécurité.	1	E
	3	Le prestataire de services informatiques établit un rapport de sécurité régulier à l'intention du client.	2	E
5.2		**Gestion de l'accès à l'infrastructure du client**		
	1	Les mutations de personnel chez le prestataire de services informatiques peuvent être facilement mises en œuvre. Un ancien employé ne peut plus accéder à l'infrastructure/aux données du client.	1	E
	2	Le client peut uniquement accéder aux ressources mises à sa disposition par le prestataire informatique, les ressources des autres clients lui étant inaccessibles.	1	E
	3	L'accès à l'infrastructure du client n'est possible qu'avec des appareils gérés. Les jumphosts et les ordinateurs virtuels sont considérés comme gérés.	1	E
	4	Tous les clients sont conscients de l'étendue des autorisations du prestataire de services informatiques.	1	E
	5	Une authentification à plusieurs facteurs est nécessaire pour accéder à l'infrastructure du client.	1	E
5.3		**Crédentiels et autorisations**		
	1	Toute mutation des comptes (y compris des mots de passe) ou des autorisations est traçable.	1	A
	2	Les mots de passe du client sont forts, uniques et conservés en toute sécurité (coffre-fort pour mots de passe ou autre).	1	A
	3	En cas d'urgence, les mots de passe sont accessibles.	1	A
	4	Les comptes privilégiés doivent être particulièrement bien sécurisés.	1	A
	5	Il existe un processus défini et sécurisé pour la mutation des comptes, du mot de passe et des autorisations.	2	A
	6	Un processus défini et sécurisé existe pour l'attribution et la révocation des droits temporaires (ex. limitation dans le temps).	2	A
5.4		**Documentation**		
	1	Pour chaque client, il existe une documentation récapitulative comprenant au moins le nom d'hôte, l'adresse IP et le but des composants gérés (inventaire).	1	E
	2	La documentation peut être remise au client sur demande (format électronique généralement répandu comme le PDF ou le papier).	1	E
	3	La documentation est à jour (pas plus d'un mois après la dernière modification).	2	E
5.5		**Conception du réseau**		
	1	Le réseau est segmenté : par exemple réseau de bureau, composants de base (stockage, plateforme de virtualisation, composants réseau), réseau dans la production, WLAN, WLAN pour les invités.	1	A
	2	Les systèmes/applications non patchables doivent être exploités sur un réseau séparé.	1	A
	3	Les transitions entre les zones ont une connectivité minimale (par exemple au moyen de pare-feux).	2	A
5.6		**Pare-feux**		
	1	Les règles doivent être lisibles (désignations pertinentes et conformes à la documentation). La documentation dans le Ruleset est souhaitée.	1	E
	2	Le Ruleset doit être contrôlé régulièrement et de manière compréhensible. Un principe de double contrôle est recommandé.	1	E
	3	Le jeu de règles est défini le plus étroitement possible. Par exemple, les règles any-any ne sont pas autorisées, le trafic sortant est également limité. Les exceptions doivent être justifiées.	2	E
5.7		**WLAN**		
	1	Des mots de passe distincts et non déductibles doivent être utilisés pour chaque client.	1	E
	2	Un réseau WLAN séparé doit être mis en place pour les appareils privés des collaborateurs et pour les invités.	1	E
	3	Seuls des mécanismes de protection actuels et sûrs sont utilisés.	2	E
5.8		**Gestion des identités (Active Directory, Azure, ...)**		
	1	Le client possède un compte d'administrateur de secours, sauf s'il y renonce explicitement.	1	A
	2	Les comptes dotés d'autorisations étendues ne sont pas utilisés pour les travaux d'application quotidiens.	1	A
	3	Les portails accessibles au public (p. ex. Azure) qui sont synchronisés avec le propre AD sont protégés par une authentification à facteurs multiples.	1	A
	4	Le prestataire de services informatiques dispose de son propre compte d'administrateur sur tous les systèmes du client.	2	A
	5	Les identités et les autorisations doivent être vérifiées régulièrement (au moins une fois par an).	2	A
5.9		**Hardening des composants informatiques**		
	1	Le prestataire de services informatiques dispose d'un processus défini et sécurisé pour le durcissement des systèmes (clients, serveurs, composants réseau).	1	E

Version 3.0 | 01.03.2026

CyberSeal
Liste des points de contrôle

Cap.	Pt.	Contrôle	Prio	Méthode d'audit: A=Autodéclaration E=Entretien T=Terminaux (console)
5.10		**Système de messagerie**		
	1	Le prestataire de services informatiques s'assure que les infrastructures de messagerie sont protégées contre les logiciels malveillants et le spam.	1	T
	2	Le prestataire de services informatiques ne prend en charge que les infrastructures de messagerie qui vérifient l'authenticité de l'expéditeur (SPF. DKIM, etc.).	1	T
5.11		**Gestion des correctifs**		
	1	Le prestataire informatique dispose d'un processus défini et sécurisé pour le déploiement des correctifs, selon une cadence appropriée.	1	T
	2	Face aux vulnérabilités critiques et connues, une réaction immédiate est obligatoire.	1	K
	3	Le prestataire de services informatiques s'assure que tous les systèmes et applications pertinents sont patchés, non seulement les systèmes d'exploitation, mais aussi les applications, les systèmes de production, les pare-feu et les appareils de réseau. Les exceptions justifiées sont consignées par écrit.	2	T
	5	Le système de patchs pour les clients est automatisé et centralisé.	2	T
5.12		**Appareils mobiles (ordinateurs portables, tablettes, smartphones)**		
	1	Les supports de données ou les conteneurs sur les systèmes mobiles sont cryptés.	1	E
	2	L'accès aux données de l'entreprise n'est possible qu'après une authentification suffisante.	1	E
	3	Il existe des exigences pour les appareils mobiles. Ces exigences sont appliquées par des politiques.	2	E
	4	Une gestion des périphériques ou des applications est mise en place.	2	A
5.13		**Travail à distance / Bureau à domicile**		
	2	L'accès à Remote Work n'est possible qu'après une authentification à plusieurs facteurs.	1	E
	3	Une politique de travail à distance est convenue avec les collaborateurs.	2	E
5.14		**Protection contre les logiciels malveillants**		
	1	Tous les systèmes sont dotés d'une protection contre les logiciels malveillants, dans la mesure où ils le permettent techniquement.	1	T
	2	Un concept à deux niveaux (pare-feu et client) est mis en œuvre.	1	T
	3	Les systèmes sans protection contre les logiciels malveillants (par ex. les systèmes de production) doivent être isolés au niveau du réseau.	2	E
	4	Une solution Endpoint Detection and Responce est en place.	2	A
5.15		**Sauvegarde / restauration**		
	1	Le prestataire de services informatiques dispose d'un processus défini et sécurisé pour la sauvegarde/restauration des systèmes et services nécessaires (par ex. : serveurs, composants réseau, services cloud).	1	T
	2	La sauvegarde est régulièrement testée. Des tests de restauration de l'ensemble des systèmes (serveurs), y compris les données, sont nécessaires à intervalles réguliers.	1	T
	3	Une copie de sauvegarde suffisante se compose de plusieurs générations, doit être conservée séparément sur le plan local et ne doit pas être modifiée.	1	T
	4	L'accès à l'infrastructure de sauvegarde ne se fait pas via la gestion régulière des identités.	2	E
5.16		**Gestion du changement / gestion des incidents**		
	1	Toutes les modifications pertinentes des systèmes et services (prestataire et client) suivent des processus définis et sont journalisées de manière traçable.	1	A
	3	Tous les incidents liés à la sécurité sont traités selon un processus défini et peuvent être suivis.	2	A
5.17		**Consignation des données**		
	1	Le prestataire de services informatiques s'assure que tous les journaux du système sont conservés conformément à l'accord (SLA recommandé).	1	A
	2	Au moins chaque accès du prestataire de services informatiques aux systèmes du client et les pannes de matériel doivent être consignés.	1	A
5.18		**Suivi**		
	1	Le prestataire informatique assure la surveillance des systèmes et des services et prend les mesures appropriées si nécessaire.	1	A
	2	Les systèmes de sécurité sont supervisés. Les alertes sont traitées (ex. via un SOC).	3	A
	3	Un processus de gestion des vulnérabilités est en place.	2	A
5.19		**Élimination des supports de données / Effacement des données**		
	1	Le prestataire informatique dispose d'un processus défini et sécurisé pour l'élimination des supports de données.	1	A
	2	Il existe un processus pour la suppression des données.	3	A

Version 3.0 | 01.03.2026

CyberSeal
Liste des points de contrôle

Cap.	Pt.	Contrôle	Prio	Méthode d'audit: A=Autodéclaration E=Entretien T=Terminaux (console)
5.20		**Services de tiers**		
	1	Le prestataire de services informatiques connaît les produits tiers dont il s'occupe et peut offrir un niveau de sécurité comparable à celui des services locaux.	**2**	**A**
	2	Le prestataire informatique s'assure que ses clients sont régulièrement informés des améliorations possibles concernant les services de fournisseurs tiers utilisés, et formule les recommandations correspondantes.	**3**	**A**
	3	Le prestataire informatique accompagne le client dans l'utilisation sécurisée des produits et services de fournisseurs tiers, notamment en matière de protection des données et de prévention des fuites de données.	**3**	**A**
5.21		**Gestion de l'intelligence artificielle**		
	1	La charte des collaborateurs couvre également l'utilisation de l'IA	**1**	**T**
	2	Inventaire des services utilisés	**2**	**A**
	3	Stratégie d'utilisation et de gestion de l'intelligence artificielle	**3**	**A**
5.22		**Formation du personnel**		
	1	Une politique d'utilisation et d'administration (par ex. Acceptable Use Policy) est définie et appliquée.	**1**	**T**
	2	Le prestataire informatique organise régulièrement des formations sur la sécurité de l'information pour ses propres collaborateurs et en vérifie l'efficacité.	**1**	**T**
	3	Le prestataire de services informatiques propose des services de sensibilisation à ses clients ou les met en relation avec un prestataire tiers.	**2**	**A**
5.23		**Concept d'urgence**		
	1	Un concept d'urgence actuel est en place et disponible en cas d'urgence. Il tient compte entre autres du cryptage et de la divulgation des données, ainsi que du chantage.	**1**	**T**
	2	Le concept d'urgence est testé de manière appropriée et régulière.	**2**	**A**
	3	Le concept d'urgence règle également l'implication des services externes (police, BACS, assurances, entreprises de soutien, etc.).	**2**	**A**
	4	Le prestataire de services informatiques propose à ses clients de les aider à mettre en place un plan d'urgence moderne.	**2**	**A**
5.24		**Dates d'expiration**		
	1	Les dates d'expiration des composants informatiques (p. ex. certificats, licences, etc.) sont gérées. Un message est généré à temps avant l'expiration.	**2**	**A**
	2	Le client est rendu attentif à l'obsolescence du matériel et des logiciels, y compris aux risques qui y sont liés.	**2**	**A**
5.25		**Sécurité physique**		
	1	L'accès aux locaux du prestataire de services informatiques est contrôlé et judicieusement limité.	**1**	**E**
	2	L'accès au centre de données du prestataire de services informatiques doit être autorisé et consigné.	**1**	**E**
	3	Les équipements informatiques critiques du prestataire sont protégés contre les influences extérieures (ex. onduleur, climatisation, connexion Internet redondante).	**2**	**E**
5.26		**Gestion des risques informatiques**		
	1	Une gestion des risques / analyse des risques est effectuée chaque année. Le CA signe le rapport de risque à l'attention de la direction et accepte ainsi les risques restants.	**2**	**E**
	2	Un processus a été mis en place pour traiter les risques inacceptables.	**2**	**E**
	3	Si nécessaire, le prestataire de services informatiques assiste le client dans les questions de gestion des risques.	**3**	**A**
	4	La résilience numérique doit être prise en compte dans la gestion des risques informatiques.	**3**	**A**
5.27		**Protection des données et aspects juridiques**		
	1	Les exigences légales et réglementaires pertinentes (ex. DSG, ISG) sont connues et prises en compte.	**1**	**A**
	2	Une analyse d'impact a été réalisée et un processus de notification obligatoire est en place.	**2**	**A**
	3	Le prestataire informatique accompagne les clients si nécessaire dans les exigences du DSG et de l'ISG (analyse d'impact, obligation de notification).	**2**	**A**
5.28		**Développement logiciel**		
	1	Les principes fondamentaux du développement sécurisé de logiciels (par exemple, OWASP Top 10) sont systématiquement appliqués. Le développement de logiciels suit un processus défini.	**1**	**A**
	2	Les aspects liés à la sécurité sont intégrés dans le processus de révision du code.	**2**	**E**
	3	Un processus garantit que les fichiers journaux et les messages d'erreur ne divulguent aucune information sensible et sont traités de manière sécurisée pendant le développement.	**3**	**A**
	4	Lors du développement, des outils et des tests de sécurité (par exemple, analyse statique/dynamique, tests de pénétration) sont systématiquement utilisés pour identifier les vulnérabilités.	**2**	**E**