NIST - Contrôles de sécurité												
ID	**Sujet**	**Fonction du NIST**	**Type**	**Sous-sujets**	**Point d'évaluation**	**Exigences**	**Le contrôle est-il : négociable, négociable sous conditions de contexte, non-négociable : MSC (must = vital, should=dans la mesure du possible, could=nice to have)**	**Questionnement**	**Niveau d'arbitrage**	**Impact GHG (estimation 0-4)**	**Significatif (Vrai/Faux)**	**Variables**
APP.02-lvl2	APP	PROTECT (PR)	TECH	SDLC tools	How is cybersecurity integrated in your Software Development Life Cycle (projects needs/specifications, development, exploitation, disposal)?	- Some internal tools are created (architecture patterns, list of frameworks, code analyzer...) and used by the application security experts. G19	Should	Négociable en fonction du contexte : Solutions de prortection de la supluy chaine CNAP SCR SBOM répertorier les librairies > niveau de sensibilité des SI > dev secop > pour les nouveaux développements. Analyse de risques. Le niveau de détail de la segmentation dépend. Bibliothèque non maintenue ou avec des failles supprimées plutôt positif. Outillage > optimisé le code > niveau de segmentation > couche et enjeux en fonction du risque. niveau 4 Vérification continue de l'intégrité logiciel. Adapter le niveau du contrôle en fonction du niveau de sécurité attendue de la supply chaine (5 niveaux SLSA) ; nous sommes en amont du run, il s'agit de prévenir le risque.		3	VRAI	
APP.04-lvl4	APP	PROTECT (PR)	TECH	Security requirements deployment tools	How do you manage security protection for applications?	=- Firewall and IPS are deployed to access applications. - Use of reverse proxy. - WAF with advanced configuration (TLS decryption, URL whitelisting, ...) are systematically used for Internet-facing applications.G67	Must			3	VRAI	'For cybersecurity equipements: - € spent in cybersecurity hardware appliances (firewalls, reverse proxies, IPS) - kWh of elecricity used by the appliances mentioned above - Number of servers being used by virtualized cybersecurity components (firewalls, reverse proxies, IPS) - Elecricity used by the servers mentioned above
AS-SET.06-lvl4	ASSET	PROTECT (PR)	TECH	IT assets capacity planning tool	Comment la disponibilité des ressources informatiques est-elle surveillée ?	*Utilisation d'outils de supervervision (ex : Centreon) au niveau des applications.	Should	A mettre en place en relation avec la charge du planning et de l'activité de l'entreprise. D'un point de vue cybersécurité est optionnel, côté écoconception et résilience, cette gestion permet de contrôler, anticiper et d'ajuster l'infrastructure au juste besoin.	A mettre en place en relation avec la charge du planning et de l'activité de l'entreprise. D'un point de vue cybersécurité est optionnel, côté écoconception et résilience, cette gestion permet de contrôler, anticiper et d'ajuster l'infrastructure au juste besoin.	1	FAUX	
AS-SET.09-lvl4	ASSET	PROTECT (PR)	TECH	Obsolescence management tool	How do you manage obsolete assets?	- Obsolete assets are blocked, replaced or protected through specific risk-reduction measures (e.g. network isolation). - Virtual patching is performed to maintain the security level.	Should	négociable en fonction de la criticité et de l'évènement redouté		4	VRAI	'- Average lifespan of a current mobile phone / workstation / server, given the cybersecurity requirements, in years («c» for current) - Average lifespan of a mobile phone / workstation / server, without cybersecurity requirements, in years («p» for potential) - Current number of mobile phones / workstations / servers («n» for number) - Kwh of surplus of electricity used by workstations to process cybersecurity software
AS-SET.10-lvl4	CLOUD	PROTECT (PR)	ORGA	IT assets disposal process	What is your policy for the disposal of devices (server, workstation, smartphone, ...)?	- A process is continuously improved. - Data on devices are securely erased before the device is reassigned or taken out of production. - Regular controls are made to ensure that implementation complies with the policy.	Must			3	VRAI	'- Number of mobile phone / workstation / server being destroyed when deemed obsolete every year for cybersecurity reasons
CLOUD.06-lvl4	CLOUD	PROTECT (PR)	TECH	Cloud services resilience	Quelle est la stratégie mise en place pour assurer la redondance en cas d'interruption du service ?	'*Des capacités de redondance entre les centres de données situés dans différentes régions sont possibles et régulièrement testées.	Could	'Que veut-on protéger ? Quel évènement est redouté ? Quelle échelle de redondance est envisagée : intrarégionale, multirégionale ? Ai-je des locaux dans différentes régions ? Quelles sont les ressources allouées à la mise en place et la maintenance de cette redondance ? La redondance aboutit-elle à se rapprocher des clients ?	'Au niveau «métiers»	4	VRAI	Sites de repli, duplication pour PCA
CLOUD.07-lvl4	CLOUD	PROTECT (PR)	TECH	Cloud data backup	What strategy is in place for data backup?	- Backup capabilities are formalized for Cloud streams and data. - Backups are automated and tested. - Backups are stored beyond their region of creation (in another region, on another account, on-premise, etc...).	Must	Must si la donnée doit nécessairement être backupée, il faut tester le backup		3	VRAI	
CLOUD.08-lvl3	CLOUD	PROTECT (PR)	TECH	Administration access to cloud consoles	Comment l'accès administratif aux consoles cloud est-il géré ?	*L'accès s'effectue via un bastion afin d'assurer la traçabilité.	Should	Pour des SI soumis à moins de contraintes, d'autres mesures déjà en place (plutôt qu'un bastion) peuvent être implémentées. Il existe des mécanismes de sécurité plus facile à appréhender, tant au niveau financier que humain.	'Au niveau «métiers»	3	V RAI	
CLOUD.11-lvl4	DATA	PROTECT (PR)	TECH	Cloud flows security	Comment les flux entrants et sortants sont-ils sécurisés dans le cloud ?	*Une sécurité basée sur l'identité « zero trust » contribue à protéger les environnements cloud.	Could	Selon le niveau d'ouverture du SI, le niveau zero trust n'est pas obligatoire.	'Au niveau «métiers»	2	FAUX	
DA-TA.05-lvl4	DATA	PROTECT (PR)	TECH	Storage	Comment détecter une fuite de données sur Internet ?	'*Une solution DRM (gestion des droits numériques) est utilisée sur tous les dossiers sensibles (par exemple : Varonis, AIP) et DLP. »	Could	la classification des données	Les métiers sont-ils prêts à classifier les données ?	2	FAUX	
DA-TA.06-lvl4	DATA	PROTECT (PR)	TECH	Data in motion	How do you secure sensitive data in transit (data transiting over the networks, applications, or physically)?	- Mechanisms are deployed to detect bypasses on all networks (via DLP solution or SIEM rules). - A secured exchange solution is available for internal & external exchange and mandatory for certain types of exchange.	Must			2	FAUX	'- Number of servers dedicated to DLP, SIEM and external exchange solutions - Electricity used by the servers above
DATA.07-lvl4	DATA	PROTECT (PR)	TECH	Prevention of unstructured data leakage (DLP)	Quels sont les mécanismes mis en place sur les ordinateurs de bureau pour empêcher les fuites de données non structurées ?	*Les solutions DLP pour terminaux (par exemple Varonis, Symantec) sont déployées sur les ordinateurs de bureau. *Cette solution est utilisée pour la détection et la réaction (le transfert est bloqué).	Could	Concernant le DLP poste de travail : le contrôle est-il effectué sur l'endroit le plus simple et le plus efficace (gateway ou postes de travail ?) Quel est le niveau d'ouverture du système d'information et quelle est la capacité utilisée part les postes de travail ?	Les métiers sont-ils prêts à classifier les données ?	2	FAUX	'*kWh d'électricité excédentaire utilisée par les postes de travail pour traiter le logiciel DLP endpoint
DA-TA.08-lvl4	DATA	PROTECT (PR)	TECH	Network DLP	Quelles solutions de sécurité ont été déployées sur les points du réseau afin d'empêcher les fuites de données ?	*Les solutions DLP sont déployées sur les passerelles Web et de messagerie électronique afin de détecter toute exfiltration de données. *Le mode blocage est activé et les communications cryptées sont décryptées à des fins de surveillance.	Could	Concernant le DLP gateway : les services messagerie ontils été externalisés ? Les données sont-elles accessibles à partir de terminaux non maîtrisés (ex : BYOD) ?	Les métiers sont-ils prêts à classifier les données ?	2	FAUX	*Couverture DATA.06-lvl4
DA-TA.09-lvl4	DATA	PROTECT (PR)	TECH	Data desensitization	How is data protected in a non-production environment (lower security level)?	- Desensitization is available for several use cases. - Tools are described in a service catalog widely shared. - The use of desensitization tools is monitored.	Should	Réglementaire ou pas (RGPD) ou politique de confidentialité de l'entreprise		2	FAUX	
EN-DPT.07-lvl4	ENDPT	PROTECT (PR)	TECH	Remote access tool	Comment l'accès à distance est-il accordé aux utilisateurs ?	*Les appareils se connectent systématiquement à un réseau via un VPN crypté standard (par exemple NetScale, Pulse, Cisco), avec authentification par nom d'utilisateur et mot de passe. *Les appareils connectés sont également authentifiés, par exemple à l'aide de certificats. *Une vérification de l'hôte est mise en œuvre (antivirus...). *L'authentification multifactorielle (MFA) est mise en œuvre avec un accès conditionnel (par exemple, emplacement IP, groupes d'individus, appareils utilisés pour la connexion, etc.).	Must	La conformité doit être adpatée au niveau de maîtrise des terminaux (ex : poste personnel, politique de gestion des accès à distance)	Au niveau «DSI / département cybersécurité»	2	FAUX	
EN-DPT.09-lvl3	ENDPT	PROTECT (PR)	TECH	Removable media protection tool	Comment les supports amovibles sont-ils protégés à l'intérieur et à l'extérieur des locaux de l'organisation ?	*Les supports amovibles sont analysés par un logiciel anti-malware lorsqu'ils sont connectés. *Des supports amovibles cryptés sont fournis par l'entreprise pour toutes les utilisations. *Des sandbox USB sont utilisées pour les périmètres les plus critiques.	Should	Il s'agit d'adapter le niveau d'exigences aux enjeux de l'organisation (ex : politique de gestion des périphériques amovibles)	'Au niveau «métiers»	1	FAUX	
EN-DPT.11-lvl4	ENDPT	PROTECT (PR)	TECH	Mobile device security tool	Comment gérez-vous la protection des smartphones ?	*Des outils de gestion des appareils (par exemple MDM, Microsoft Intune, Mobile Iron, AirWatch) sont mis en œuvre pour les appareils mobiles, permettant : > L'application de la configuration de sécurité lors de l'inscription (chiffrement de l'appareil, liste blanche/liste noire des applications) > Contrôler la conformité aux politiques de sécurité (statut root) > Appliquer des correctifs à distance si possible > Mettre en place des plans d'action automatiques pour les appareils non conformes (par exemple, alertes, blocage, etc.).	Must	Il s'agit d'adapter le niveau de gestion des configurations aux enjeux (ex : enjeux de conformité)	Au niveau «DSI»	1	FAUX	
EN-DPT.13-lvl4	ENDPT	PROTECT (PR)	TECH	Email security	How is the email platform secured?	- An anti-virus scan is performed before users receive emails. - A TLS encryption of the exchanges between mail servers is activated to protect the mail. - A relay server, dedicated to sending and receiving messages, is set up in case of internet outage. - An anti-spam and anti-phishing service is used to protect the mailbox. - Mechanisms for verifying the authenticity and correct configuration of public DNS (Domain Name System) records related to the messaging infrastructure (MX, SPF, DKIM, DMARK) are in place. - An advanced threat protection (Windows ATP, Proofpoint, etc.) is used to protect the messaging system.	Must			3	VRAI	
EN-DPT.14-lvl4	ENDPT	PROTECT (PR)	TECH	Security of administrators workstations	Comment les postes de travail des administrateurs sont-ils gérés ?	*Des postes de travail dédiés (Privileged Access Workstation - PAW) sont mis en place.	Could			4	VRAI	'*Postes de travail dédiés à l'administration des numéros *Type de postes de travail dédiés à l'administration
GOV.05-lvl4	GOV	PROTECT (PR)	TECH	Awareness tools	Comment sensibilisez-vous le personnel interne et externe à la cybersécurité ?	*Tests destinés à des populations spécifiques (fraude au président pour les populations financières et comptables, tests d'intrusion physique pour le personnel d'accueil, etc.) *Serious games.	Must	Opportunité pour faire de la sensibilisation commune aux enjeux cyber et aux enjeux numérique responsable		2	FAUX	Y compris module video
IAM.02-lvl4	IAM	PROTECT (PR)	TECH	User identity management tool	Comment les identités des utilisateurs sont-elles gérées ?	*L'outil de gestion du cycle de vie des identités (par exemple SailPoint, Oracle, IBM, One Identity) est alimenté par des sources faisant autorité (RH, achats, etc.). *Il déclenche automatiquement des workflows lors d'événements (par exemple, déménagement, départ, etc.) avec les actions appropriées (telles que la suppression des autorisations). *Le modèle de sécurité Zero Trust est mis en œuvre pour limiter l'accès des utilisateurs aux seules ressources dont ils ont besoin.	Could	En fonction du niveau et des enjeux, il s'agit d'identifier le niveau de management adapté et les outils associés. Si l'organisation requière le Zéro Trust, cela permet une gestion frugale des accès.		2	FAUX	'*Nombre de serveurs dédiés à l'IAM (en pourcentage ? L'IAM étant utile pour l'informatique, indépendamment de la cybersécurité) *Électricité consommée par les serveurs ci-dessus
IAM.10-lvl4	IAM	PROTECT (PR)	TECH	Technical account authentication	What kind of authentication is required for technical identities (scripts, batch, automated processes, robots, etc.) to access resources?	- Alternative mechanisms are used in addition to passwords or in replacement for passwords (e.g. private key hardware protected, network segregation, etc.).	Must	Les protections minimales des comptes de service sont-elles bien présentes afin d'éviter l'achat d'équipement ou des ségrégations réseaux supplémentaires ?		3	VRAI	'*Euros dépensés en jetons physiques *Nombre de serveurs utilisés pour l'authentification *Électricité utilisée à des fins d'authentification
NTW.01-lvl4	NTW	PROTECT (PR)	ORGA	Network segmentation rules	How is the company's network managed?	- A policy is continuously updated to ensure network segmentation principles meet the company network evolution (cloud, internet exposure...). - The information system is segmented into security zones according to exposition (internet-facing, suppliers,...), sensitivity, environment (production/pre-production...) to limit threat propagation. - Regular controls are made to ensure that network design complies with the policy.	Should			3	VRAI	Y compris env de dev/preprod/prod
NTW.09-lvl4	NTW	PROTECT (PR)	TECH	Internet access protection	Comment vous assurez-vous que tous les accès à Internet se font via des plateformes d'accès Internet gérées par l'entreprise ?	*Tous les accès à Internet, y compris au Cloud, se font via un proxy géré par l'entreprise.	Could	Est-il nécessaire de proxifier tous les flux ?		2	FAUX	
NTW.10-lvl4	NTW	PROTECT (PR)	TECH	Browsing protection	Comment vous assurez-vous que tous les accès à Internet se font via des plateformes d'accès Internet gérées par l'entreprise ?	'*Proxy : le trafic de navigation des terminaux est filtré à l'aide d'une liste noire et le trafic de navigation des serveurs est filtré à l'aide d'une liste blanche (par exemple, IronPort Systems Cisco, Apache, Squid). *Les pages Web sont analysées à la recherche de logiciels malveillants. *Utilisation d'un bac à sable pour tester les programmes non vérifiés susceptibles de contenir un virus ou un autre code malveillant. *Utilisation du décryptage TLS.	Must	Le déchiffrement et chiffrement systématique est-il nécessaire ?		2	FAUX	
NTW.11-lvl2	NTW	PROTECT (PR)	TECH	Anti-DDoS protection	Comment sécurisez-vous les services accessibles via Internet ?	*Les points d'accès Internet sont protégés par une solution anti-DDoS basée sur le réseau.	Could	Par opérateur télécom ou équipement réseau que l'on possède		2	FAUX	
NTW.11-lvl4	NTW	PROTECT (PR)	TECH	Anti-DDoS protection	Comment sécurisez-vous les services accessibles via Internet ?	*Tous les services accessibles depuis Internet (sites web, DNS...) sont des points d'accès protégés par une solution anti-DDoS basée sur une application.	Could	Par service, appliquer cette pratique uniquement lorsque l'enjeu le justifie.		2	FAUX	
NTW.14-lvl4	NTW	PROTECT (PR)	TECH	Remote administration accesses tool	How do you prevent unauthorized access when performing remote administration?	- An IS dedicated to administration is implemented, and remote administration is possible only through VPN (e.g. NetScaler) on managed devices and MFA. - A «just-in-time» authentication is implemented, allowing privileged accounts to grant access to the resources when needed.	Must			4	VRAI	
OPS.03-lvl1	OPS	PROTECT (PR)	ORGA	Critical infrastructure hardening	Which specific protection measures do you implement on critical infrastructures (e.g. AD, DNS, SCCM, CyberArk, PKI, ...)	- Hardening on critical infrastructures is done ad hoc.	Must	optimisation de la configutation et réduction de la surface d'attaque (réudction, suppression des composants inutiles, etc.)		4	VRAI	Certains périmetre critiques interdisent d'avoir 2 applis de niveau differents donc duplication d'infra
OPS.08-lvl2	OPS	PROTECT (PR)	TECH	Patch management tool	Comment gérez-vous les correctifs de sécurité sur les systèmes d'exploitation, les intergiciels, les bases de données et l'infrastructure réseau des serveurs ?	*Les correctifs de sécurité sont industrialisés à l'aide d'outils de base (WSUS, SEP).	Should	Le nombre d'équipements justifie-t-il l'utilisation de ce type d'outil ?		2	FAUX	
OPS.08-lvl3	OPS	PROTECT (PR)	TECH	Patch management tool	Comment gérez-vous les correctifs de sécurité sur les systèmes d'exploitation, les intergiciels, les bases de données et l'infrastructure réseau des serveurs ?	*Les correctifs de sécurité sont industrialisés à l'aide d'une solution avancée. *Des correctifs virtuels (par exemple Trend Micro) sont appliqués.	Could	Quelle est la temporalité nécessaire à l'application ou la suppression du patch de façon maîtrisée ?		2	FAUX	
OPS.12-lvl4	OPS	PROTECT (PR)	TECH	Change management process tooling	Comment gérez-vous les changements apportés à vos actifs, notamment en matière d'examen de la sécurité et d'approbation des modifications ?	*Toutes les modifications sont regroupées dans un seul outil ITSM centralisé.	Could	Le nombre de changement justifie-t-il l'utilisation de ce type d'outil ?		2	FAUX	
OPS.14-lvl4	OPS	PROTECT (PR)	TECH	Change detection	Comment détectez-vous les changements dans les configurations de base des actifs ?	*Les différences par rapport aux bases de référence de configuration sont identifiées en temps réel (via les journaux dans SIEM ou à l'aide de logiciels).	Should	Quelle est la temporalité nécessaire à la détection d'une configuration altérée ?		2	FAUX	
OPS.15-lvl4	OPS	PROTECT (PR)	TECH	AD security	At what level is Tier 0 (the sensitive area for AD management) seperate from the rest of the IS?	- The Domain Administrator can only connect to the Domain Controller (the server hosting the AD) with a dedicated workstation. - Possibility to block the connection via GPO (centralized management), Microsoft Silo, etc. - A dedicated infrastructure for the administration of Tier 0 is set up, including hypervisor, network, physical workstation, Domain Controller and transverse infrastructure (update and supervision).	Should	Le questionnement est autour du poste de travail dédié en cherchant des alternatives «virtuelles».		3	VRAI	
OPS.17-lvl4	OPS	PROTECT (PR)	TECH	Certificate Management Tools	Quelles infrastructures sont en place pour gérer le cycle de vie des certificats utilisés ?	*Une seule infrastructure PKI principale au niveau de l'organisation est gérée conformément à la politique de sécurité et peut répondre à tous les besoins de l'organisation. *Des outils d'inventaire et d'analyse garantissent qu'il n'existe aucun certificat au sein de l'organisation autre que ceux émis par cette infrastructure PKI.	Could	A-t-on besoin d'une PKI ? L'achat de certificat auprès d'une authorité de certification reconnue est-il suffisant ?		2	FAUX	
OPS.19-lvl4	OPS	PROTECT (PR)	TECH	Private keys securing	Comment les clés privées des autorités de certification (CA) sont-elles sécurisées ?	*Toutes les clés privées des autorités de certification (racine, intermédiaires ou émettrices) sont sécurisées, sans exception, dans des modules HSM ou dans un coffre-fort physique (pour les autorités de certification déconnectées) en appliquant les processus appropriés de sauvegarde et de contrôle d'accès. *De plus, si le cadre réglementaire auquel l'organisation est soumise et les cas d'utilisation l'exigent (par exemple PCI-DSS, LPM, FIPS, etc.), les HSM utilisés disposent des qualifications de sécurité nécessaires (ANSSI, certification FIPS, etc.).	Could	Si une PKI est nécessaire, le dispositif est-il une AC Racine off-line et une AC opérationnelle fille ? La partie HSM est à déterminer en fonction de la régulation.		2	FAUX	
OPS.20-lvl4	OPS	PROTECT (PR)	TECH	Security of remote deployment means on the IS	Comment les moyens de déploiement à distance des mises à jour sur le SI sont-ils sécurisés ? (GPO, LANDESK, etc...)	*L'authentification multifactorielle (MFA) est utilisée pour sécuriser la connexion aux outils de déploiement à distance. *Des tests sont systématiquement effectués dans un environnement hors production. *Une double vérification est effectuée par deux administrateurs avant de valider un déploiement.	Must			2	FAUX	
RISK.11-lvl4	RISK	PROTECT (PR)	ORGA	Audit plan	Comment mettez-vous en œuvre les audits de sécurité sur votre SI ?	*Des audits techniques et organisationnels sont réalisés sur les domaines critiques. *Un plan d'action est élaboré et mis en œuvre après chaque audit. *Des programmes de bug bounty sont mis en place afin d'améliorer les capacités de détection des vulnérabilités.	Should	Quel niveau d'audit interne est-il nécessaire par rapport aux enjeux ? Quels sont les volumes / les fréquence ?		2	FAUX	'*Nombre de serveurs utilisés pour les audits techniques et organisationnels *Électricité consommée par les serveurs ci-dessus *Montant en euros dépensé pour les audits techniques et organisationnels externes