LE PREMIER MINISTRE

REPUBLIQUE TOGOLAISE
Travail - Liberté - Patrie

ARRETE N° 2022-040 /PMRT
portant adoption des règles de cybersécurité en République togolaise

---

LE PREMIER MINISTRE,

Vu la Constitution du 14 octobre 1992 ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, modifiée la loi n° 2022-009 du 24 juin 2022 ;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité (ANCy) ;

Vu le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du Gouvernement, complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

Vu le décret n° 2021-045/PR du 29 avril 2021 portant nomination du directeur général de l'Agence nationale de la cybersécurité ;

ARRETE :

Article 1er : Objet

Le présent arrêté porte adoption des règles de cybersécurité applicables aux opérateurs de services essentiels désignés par l'Agence nationale de la cybersécurité, et à toute l'administration publique togolaise.

Les règles de cybersécurité annexées au présent arrêté en font partie intégrante.

Article 2 : Application

Les ministres et les premiers responsables des institutions de la République veillent, chacun en ce qui le concerne, à l'application des dispositions du présent arrêté par les administrations et les opérateurs de services essentiels relevant de leur ressort.

Article 3 : Exécution

Le directeur général de l'Agence nationale de la cybersécurité (ANCy) est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel de la République togolaise.

Fait à Lomé, le 29 juin 2022

SIGNE

Victoire S. TOMEGAH-DOGBE

Pour ampliation,

Le Ministre,
Secrétaire Général du Gouvernement

Kanka Malik NATCHABA

ANNEXE

REGLES DE CYBERSECURITE EN REPUBLIQUE TOGOLAISE

MINISTÈRE DE L'ÉCONOMIE
NUMÉRIQUE ET DE
LA TRANSFORMATION DIGITALE

RÉPUBLIQUE TOGOLAISE

MINISTÈRE DE LA SÉCURITÉ
ET DE LA PROTECTION CIVILE

ANCy
Agence Nationale
de la Cybersécurité

Règles de Cybersécurité

Version 1.0

Juin 2022

Table des matières

1. Cadre légal et réglementaire 3
2. Définitions 4
3. Introduction 5
4. Contrôle de conformité de la sécurité des infrastructures essentielles (IE) et accréditation 7
5. Domaines et sous-domaines des règles de cybersécurité 7
G1 – Gouvernance, gestion et leadership 8
G2 – Politique de sécurité et plan de sécurité d'opérateur (PSO) 10
G3 – Conformité, audit et performance 12
G4 – Gestion des risques de cybersécurité 14
G5 – Ressources Humaines 16
G6 – Relation fournisseur 18
P1 – Contrôle d'accès 21
P2 – Gestion des actifs 24
P3 – Sécurité des communications 26
P4 – Systèmes d'information, acquisition et maintenance 31
P5 – Sécurité des opérations 34
P6 – Sécurité environnementale et physique 38
D1 – Gestion des incidents de sécurité 41
R1 – Gestion de la continuité des activités 45
6. Références 48
7. Facteurs clés de succès 48

1. Cadre légal et réglementaire

Les présentes Règles de Cybersécurité sont établies dans le cadre de la législation togolaise, en particulier des textes législatifs et règlementaires suivants :

- La loi n°2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo ;
- La loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (« **Loi sur les Données Personnelles** ») ;
- La loi n°2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité (« **Loi sur la Cybersécurité** ») ;
- La loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise (« **Loi sur les Transactions Electroniques »**) ;
- La loi d'orientation n°2017-006 du 22 juin 2017 sur la société de l'information au Togo (« **Loi sur la Société de l'Information** ») ;
- La loi n°2014-014 du 22 octobre 2014 portant modernisation de l'action publique de l'Etat en faveur de l'économie (« **Loi sur la Modernisation de l'Action Publique** ») ;
- La loi no 2012-018 du 17 décembre 2012 sur les communications électroniques, modifiée par la loi n°2013-003 du 19 février 2013 (« **Loi sur les Communications Electroniques** ») ;
- Le décret n°2021-102/PR du 29 septembre 2021 portant création, attributions, organisation et fonctionnement de l'Agence Togo Digital (ATD) ;
- Le décret n°2021-031/PR du 24 mars 2021 portant numérisation des paiements de l'Administration publique ;
- Le décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo (« **Décret sur les Transactions Electroniques** ») ;
- Le décret n°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA) (« **Décret CDA** »).
- Le décret n°2019-095/PR du 8 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes (« **Décret OSE** ») ;
- Le décret n°2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité (ANCy) (« **Décret ANCy** ») ;
- L'arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des prestataires de services de confiance établis hors du territoire national (« **Arrêté PSCE** »).

2. Définitions

En plus des termes définis dans la loi sur la Cybersécurité, dans le préambule, l'introduction et/ou dans les autres paragraphes de ce document, les acronymes et termes suivants sont définis comme suit :

Délégataire de l'ANCy : La société d'économie mixte Cyber Defense Africa S.A.S. (CDA), ayant son siège social à Lomé et ayant signé avec l'ANCy un contrat de délégation de service public portant sur la création et l'exploitation de structures permettant de sécuriser le cyberespace togolais et chargeant CDA de fournir des solutions nécessaires (infrastructure informatique, logiciels et services) afin de prévenir, analyser et répondre aux attaques informatiques et cyberattaques visant ou impliquant des systèmes informatiques ou systèmes d'information appartenant à des opérateurs de services essentiels et/ou autres organisations installées sur le territoire de la République togolaise.

La liste à jour des délégataires de l'ANCy peut être trouvée sur le site Internet de l'Agence.

CERT National : Equipe nationale de gestion des incidents de cybersécurité fournissant des services de CERT (*Computer Emergency Response Team*) National sur le territoire de la République togolaise.

Personnel Essentiel : Personnel de l'OSE (interne ou externe, qu'il soit lié par un contrat de travail, de service ou toute autre relation contractuelle) nécessaire à la fourniture continue et ininterrompue du ou des Service(s) Essentiel(s) de l'OSE.

Prestataire de services de confiance en cybersécurité qualifié par l'ANCy : prestataires fournissant des services qui contribuent à la sécurité (i) des systèmes d'information des administrations ou des opérateurs de services essentiels et (ii) de tout matériel, logiciel ou système d'information destiné à traiter des informations couvertes par le secret de la défense nationale.

SOC : désigne un Security Operation Center ou Centre opérationnel de sécurité ;

3. Introduction

Conformément au Décret ANCy, l'Agence Nationale de la Cybersécurité (ANCy) est l'autorité nationale en matière de sécurité des systèmes d'information au Togo. Elle concourt à la définition et à la mise en œuvre de la politique et des orientations stratégiques du pays en matière de cybersécurité.

Le Décret OSE définit les modalités et critères de désignation des opérateurs de services essentiels (ci-après les « **Opérateurs de Services Essentiels** » ou « **OSE** »), de déclaration des infrastructures essentielles situées sur le territoire togolais (les « **Infrastructures Essentielles** » ou « **IE** ») et fixe les obligations et règles relatives à la cybersécurité desdites Infrastructures Essentielles. Les services essentiels des OSE (ci-après les « **Services Essentiels** ») sont listés en annexe du Décret OSE.

Les présentes Règles de Cybersécurité sont fixées par l'ANCy conformément à l'article 11 du Décret OSE et s'articulent autour des quatre domaines suivants :

1. **La gouvernance de la sécurité des réseaux et systèmes d'information**
2. **La protection des réseaux et systèmes d'information**
3. **La défense des réseaux et systèmes d'information**
4. **La résilience des activités**

Pour chaque domaine, ces règles définissent les contrôles appropriés dans chacun des sous-domaines suivants :

1. **La gouvernance de la sécurité des réseaux et systèmes d'information (G)**

   G1. Gouvernance, Gestion et Leadership

   G2. Politique de sécurité et plan de sécurité d'opérateur (PSO)

   G3. Conformité, audit et performance

   G4. Gestion des risques de cybersécurité

   G5. Ressources humaines

   G6. Relations avec les fournisseurs

2. **La protection des réseaux et systèmes d'information (P)**

   P1. Contrôle d'accès

   P2. Gestion des actifs

   P3. Sécurité des réseaux et des communications

   P4. Systèmes d'information, acquisition et maintenance

   P5. Sécurité des opérations

   P6. Sécurité environnementale et physique

3. **La défense des réseaux et systèmes d'information (D)**

   D1. Gestion des incidents de sécurité

4. **La résilience des activités (R)**

   R1. Gestion de la continuité des activités

Le tableau ci-dessous décrit chacun des sous-domaines mentionnés ci-dessus

Réf.	Domaine de contrôle	Description
G1	Gouvernance, gestion et leadership	Préparer le terrain pour la mise en place efficace de la fonction de cybersécurité au sein de l'OSE, en identifiant les principaux intervenants, leurs rôles et responsabilités connexes.
G2	Politique de sécurité et plan de sécurité d'opérateur (PSO)	Fournit un ensemble de directives de politique de cybersécurité que les OSE peuvent adopter et mettre en œuvre.
G3	Conformité, Audit et performance	Fournit des contrôles pour garantir la conformité aux règles, aux performances et à la surveillance requises.
G4	Gestion des risques de cybersécurité	Traite des contrôles et des pratiques d'identification et de gestion des risques.
G5	Ressources humaines	Répertorie les contrôles, les exigences et vérifications à effectuer pour fournir une assurance et une minimisation des risques liés aux comportements et aux personnes.
G6	Relations avec les fournisseurs	Fournit des pratiques sécurisées à inclure dans l'engagement de fournisseurs et de tiers, y compris le traitement des données, le flux d'informations, etc..
P1	Contrôle d'accès	Détaille les contrôles à mettre en œuvre pour un accès sécurisé à l'infrastructure numérique des OSE, y compris, mais sans s'y limiter, aux locaux, aux systèmes d'exploitation, etc.
P2	Gestion des actifs	Détaille les contrôles à appliquer pour la gestion des actifs informationnels critiques.
P3	Sécurité des réseaux et des communications	Fournit des exigences et des contrôles pour la mise en œuvre, l'utilisation et l'exploitation sécurisées des systèmes, des télécommunications, de la messagerie et des réseaux des OSE pour le transfert, le traitement et le stockage de données sensibles.
P4	Systèmes d'information, acquisition et maintenance	Répond aux exigences en matière des acquisitions, de développement et de gestion des systèmes d'information sécurisés.
P5	Sécurité des opérations	Fournit des contrôles pour effectuer des opérations sécurisées des OSE.
P6	Sécurité environnementale et physique	Identifie l'ensemble des contrôles nécessaires à mettre en place ou à améliorer en matière de sécurité physique lors de l'accès aux installations des OSE.
D1	Gestion des incidents de sécurité	Fournit des conseils et des contrôles en vue de l'identification précoce des menaces potentielles à la sécurité et de la prise de mesures d'atténuation immédiates.
R1	Gestion de la continuité des activités	Assure la résilience et la continuité des opérations face aux événements désastreux imprévus pour les OSE.

Conformément au Décret OSE, les Opérateurs de Services Essentiels doivent respecter les présentes Règles de Cybersécurité, sous peine de sanctions.

Les présentes Règles de Cybersécurité peuvent être modifiées en cas de besoin et ce au moins tous les deux (2) ans.

4. Contrôle de conformité de la sécurité des infrastructures essentielles (IE) et accréditation

La société CDA est chargée du contrôle annuel des OSE par un contrat de délégation de service signé avec l'ANCy. Ce contrôle vise à vérifier l'application et l'efficacité des mesures de sécurité du PSO pour chaque IE dans le respect des présentes Règles de Cybersécurité.

A l'issue de l'audit de conformité, la société CDA élabore un rapport d'audit qui expose les constatations sur les mesures appliquées et sur le respect du PSO et des présentes Règles de Cybersécurité. Le rapport précise si le niveau de sécurité atteint est conforme aux objectifs de sécurité du PSO, compte tenu des menaces et des vulnérabilités connues. Il formule des recommandations pour remédier aux éventuelles non-conformités et vulnérabilités découvertes. Le rapport est couvert par le secret professionnel, comme toute l'activité du délégataire de l'ANCy.

Lors de cette procédure d'accréditation, prenant en compte les évènements intervenus durant l'année écoulée, le PSO de l'OSE est mis à jour avec notamment une éventuelle redéfinition des objectifs, de la stratégie et des mesures mises en place.

5. Domaines et sous-domaines des règles de cybersécurité

Dans cette section, des domaines et sous-domaines ont été identifiés comme mesures de contrôles qui fournissent des exigences de sécurité pour un niveau minimum de protection contre la cybercriminalité croissante pour les actifs informationnels et les systèmes sous-jacents de tous les OSE.

L'adoption accrue de la numérisation, des communications électroniques et du cyberespace, composé d'un réseau mondial d'infrastructures de réseau interdépendantes, de réseaux de télécommunications et de systèmes de traitement informatique, a entraîné des progrès dans les services numériques ainsi que des cybermenaces.

Au fur et à mesure que les cybermenaces telles que l'hacktivisme et la cybercriminalité évoluent, les efforts visant à les combattre de manière coordonnée et systématique doivent également évoluer. Pour aligner et diriger les efforts nationaux de cybersécurité, L'ANCy a développé un ensemble de règles de cybersécurité à respecter par tous les OSE.

Ces règles sont classées en quatorze sous-domaines avec les principaux contrôles et sous-contrôles qui doivent être mis en œuvre par les OSE.

La conformité à ces règles fournira une base de protection minimale pour les OSE et accordera des capacités pour dissuader les cyberattaques de manière cohérente dans tout le pays ainsi que pour promouvoir un environnement numérique de confiance pour les particuliers et les entreprises.

Plus précisément, ces règles fournissent comment la cyber assurance numérique est réalisée dans toute la République togolaise, en définissant les rôles et les responsabilités des principales parties prenantes pour la stratégie, la planification, le développement, la mise en œuvre et le suivi continu des performances de ces règles d'assurance.

Les règles fournissent également comme point de référence des contrôles de cybersécurité communs pour se défendre contre les menaces courantes qui exploitent les vulnérabilités connues en matière de cybersécurité et minimisent le risque d'exploitation pour les vulnérabilités non encore découvertes ou autrement connues sous le nom de vulnérabilités Zero day.

Ces règles de cybersécurité font partie des éléments essentiels de la stratégie nationale de cybersécurité de la République togolaise portée par l'ANCy.

G1 – Gouvernance, gestion et leadership

Ce domaine décrit les exigences de gouvernance requises pour les OSE en matière de règles de cybersécurité. Il s'agit d'améliorer davantage la responsabilisation en matière de cybersécurité et de promouvoir la visibilité globale requise de l'OSE.

Il s'agit également de faciliter l'atteinte des objectifs de cybersécurité et de fournir un niveau optimal de gestion des risques de cybersécurité.

Le domaine garantit en outre que la stratégie de sécurité doit être alignée sur la stratégie commerciale globale et assurer l'alignement et la conformité aux exigences de l'industrie, ainsi qu'aux lois et réglementations applicables.

Les contrôles et sous-contrôles suivants doivent être implémentés par tous les OSE.

G1.1	Leadership et engagement de la direction	
Objectif	Définir les rôles et les responsabilités de toutes les parties prenantes en vue de défendre et de renforcer la posture de cybersécurité de l'OSE.	
Contrôle	Faire preuve de leadership et d'engagement en matière de cybersécurité	
Sous-contrôles	G1.1.1	Conseil d'administration
		Le conseil d'administration est globalement responsable de l'état de la cybersécurité de l'OSE et doit recevoir des mises à jour régulières sur l'état de la sécurité de l'information au moins une fois par an.
	G1.1.2	PDG/Directeur Général
		Le PDG / Directeur Général a la responsabilité d'accepter et d'approuver les exigences de cybersécurité ; d'appliquer les contrôles de cybersécurité pour l'ensemble du Système d'informations de l'OSE, de veiller à ce que les politiques, les processus et les normes de cybersécurité soient mis en œuvre à l'échelle de l'OSE.
	G1.1.3	Comité de direction de la cybersécurité
		Le comité de direction de la cybersécurité doit être établi sous la présidence du Directeur Général ou de son délégué. Le comité comprend les chefs de chaque division de l'OSE qui assument les rôles suivants :

		a) superviser la mise en œuvre du programme de cybersécurité de l'OSE b) promouvoir la culture de la cybersécurité et de la sécurité chez l'OSE c) suivre et surveiller les performances du programme de cybersécurité de l'OSE d) s'assurer que le programme de cybersécurité est conforme aux exigences légales applicables e) s'assurer que des ressources et des compétences adéquates sont disponibles pour exécuter le programme de cybersécurité.
	G1.1.4	Position en cybersécurité
		La position de la fonction de cybersécurité dans l'OSE est importante pour lui donner l'indépendance dans l'exécution de ses responsabilités et pour prévenir tout conflit d'intérêts. L'OSE évitera tout conflit d'intérêts en vue de la mise en place de la fonction cybersécurité. Idéalement, la fonction de cybersécurité devrait relever de la Direction Générale ou de l'entité de gestion des risques et non au sein des directions informatiques.
	G1.1.5	Rôle du Responsable de la Sécurité du Système d'Information (RSSI)
		Le RSSI doit être nommé pour chaque OSE et avoir la responsabilité de coordonner et d'exécuter la conformité à cette règle. L'OSE élabore et met en œuvre un plan de formation et de montée en compétences du RSSI qui comprend au minimum une formation "ISO/IEC/27001 Management de la sécurité de l'information" ou équivalente.
	G.1.1.6	Communication des coordonnées du RSSI
		L'OSE communique les coordonnées de son Responsable de la sécurité des systèmes d'information (RSSI) ou de son point de contact en cybersécurité à son autorité de tutelle sectorielle, à l'ANCy et à son délégataire dans un délai de six (6) mois à compter de la notification de sa désignation comme OSE, ainsi qu'après chaque mise à jour de ces données.
	G1.1.7	Salariés
		Tous les employés ont la responsabilité de respecter les politiques publiées et de respecter les exigences et les directives en matière de cybersécurité.

G1.2	Organisation de la cybersécurité	
Objectif	Identifier les fonctions et relations clés pour la bonne performance en matière de cybersécurité	
Contrôle	S'assurer que la visibilité de la cybersécurité et les relations pertinentes sont établies ou renforcées.	
Sous-contrôles	G1.2.1	Contact avec les autorités
		L'OSE maintien des contacts appropriés et applicables avec les autorités, y compris, sans s'y limiter, l'élaboration de politiques et de procédures à cette fin.
	G1.2.2	Dossier d'accréditation
		L'OSE maintient et tient à jour un dossier d'accréditation, soumis à un contrôle annuel après sa désignation comme OSE. Le dossier contient : a. l'analyse de risques et les objectifs de sécurité pour les IE ; b. les procédures et les mesures de sécurité appliquées aux IE ; c. les risques résiduels, les mesures de réduction de ces risques et les raisons justifiant leur acceptation.
	G1.2.3	Contact avec les groupes d'intérêts spéciaux
		Des contacts appropriés avec des groupes d'intérêts spéciaux ou d'autres forums spécialisés dans la sécurité et des associations professionnelles doivent être établies ou renforcées.
	G1.2.4	La cybersécurité dans la gestion de projet
		Un responsable cybersécurité doit être présent dans toutes les fonctions de gestion de projet et faire partie des contributeurs, des examinateurs et des approbateurs avant l'achèvement du projet.
	G1.2.5	Séparation des tâches
		Les tâches et les domaines de responsabilité conflictuels doivent être examinés et séparés afin de réduire les possibilités de modification ou d'utilisation abusives ou non autorisées des actifs de l'OSE et de l'infrastructure essentielle.
	G1.2.6	Rôles et responsabilités en matière de cybersécurité
		Tous les rôles et responsabilités en matière de cybersécurité doivent être définis et attribués aux personnes appropriées.

G2 – Politique de sécurité et plan de sécurité d'opérateur (PSO)

Les politiques de sécurité de l'information sont une partie importante des activités visant à établir des règles et des lignes directrices pour des fonctionnalités numériques efficaces afin de protéger les actifs de l'OSE et de ses infrastructures essentielles.

Les politiques fourniront un cadre, une orientation de gestion et un soutien en matière de cybersécurité pour l'OSE conformément aux exigences opérationnelles et aux lois et règlements applicables.

G2.1	Direction de gestion de la cybersécurité	
Objectif	Avoir des directives sur les pratiques de sécurité de l'information régissant les activités et les opérations des OSE.	
Contrôle	Avoir une politique de cybersécurité	
Sous-contrôles	G2.1.1	Politique de cybersécurité
		La politique doit : a. être établie et documentée pour l'OSE b. être pertinente et appropriée pour l'OSE c. inclure des objectifs de cybersécurité d. inclure l'engagement de répondre à toutes les exigences en matière de cybersécurité e. être approuvée par le conseil d'administration ou le directeur général/chef de la direction selon les cas
	G2.1.2	Politiques de soutien en matière de cybersécurité
		L'OSE établira et communiquera à l'ANCy un ensemble de politiques de cybersécurité à l'appui qui traitent de tous les aspects de la cybersécurité inclus dans ce règlement, tels que : a. Contrôle d'accès b. Gestion d'actifs c. Continuité d'activités d. Conformité en matière de sécurité e. Gestion des communications et des opérations f. Politique des ressources humaines g. Développement de systèmes d'information h. Gestion des incidents de sécurité i. Informatique mobile j. Cadre environnemental et physique k. Échange d'informations l. Cybersécurité m. Utilisation acceptable d'Internet n. Organisation de la cybersécurité
	G2.1.3	Examen des politiques de cybersécurité
		Les politiques doivent être maintenues, révisées, mises à jour à intervalles annuels et lorsque des changements importants se produisent.
	G2.1.4	Communiquer les politiques de cybersécurité
		a. Les politiques doivent être communiquées à tout le personnel et une confirmation de reconnaissance doit être obtenue pour s'assurer que tout le personnel comprend les attentes en la matière. b. Les politiques doivent être écrites et peuvent être communiquées à des tiers ou des fournisseurs pour la conformité. c. La communication des politiques aux utilisateurs doit se faire sous une forme pertinente, accessible et compréhensible. d. Une formation et une connaissance suffisantes des politiques doivent être fournies au public visé pour faciliter la connaissance de leur contenu.

		e. Les politiques doivent également être partagées aux nouveaux employés au cours du processus d'intégration et obtenir leur acceptation desdites politiques.

G3 – Conformité, audit et performance

Ce domaine fournit des contrôles pour s'assurer que l'OSE reste conforme à ses directives de cybersécurité tout au long des périodes tout en exigeant des examens annuels fournissant des assurances de conformité.

G3.1	**Conformité**	
Objectif	Éviter les violations des obligations légales, statutaires, réglementaires ou contractuelles liées à la sécurité de l'information et de toute exigence de sécurité.	
Contrôle	Se conformer aux exigences légales, contractuelles et de cybersécurité	
Sous-contrôles	G3.1.1	Identification de la législation applicable et des exigences contractuelles
		Toutes les exigences législatives, réglementaires et contractuelles pertinentes et l'approche de l'organisation pour répondre à ces exigences doivent être explicitement identifiées, documentées et tenues à jour pour chaque système d'information de l'OSE.
	G3.1.2	Droits de propriété intellectuelle
		Des procédures appropriées doivent être mises en œuvre pour assurer le respect des exigences législatives, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de produits logiciels propriétaires.
	G3.1.3	Protection des documents
		Les dossiers doivent être protégés contre la perte, la destruction, la falsification, l'accès non autorisé et la divulgation non autorisée, conformément aux exigences législatives, réglementaires, contractuelles et commerciales.
	G3.1.4	Confidentialité et protection des données à caractère personnel
		La confidentialité et la protection des données à caractère personnel doivent être assurées conformément à la législation et à la réglementation pertinentes, le cas échéant.
	G3.1.5	Réglementation du contrôle cryptographique
		Les contrôles cryptographiques doivent être utilisés conformément à tous les accords, lois et règlements pertinents.
	G3.1.6	Politique de conformité
		Mettre en place une politique de conformité qui encadre les exigences de sécurité juridiques, techniques et de gestion auxquelles l'OSE doit se conformer. La politique devrait également fournir l'approche pour établir les exigences de conformité et les étapes possibles que l'OSE suivra pour répondre aux exigences identifiées.
	G3.1.7	Conformité aux politiques et normes de sécurité
		Le premier responsable de l'OSE doit soutenir et s'assurer que celui-ci respecte les politiques et les normes de cybersécurité.

		Les gestionnaires doivent examiner régulièrement la conformité aux exigences en matière de cybersécurité au sein de leurs services responsables et prendre des mesures correctives en cas de lacunes.

G3.2	**Audits de cybersécurité**	
Objectif	S'assurer que la sécurité de l'information est mise en œuvre et exploitée conformément aux politiques et procédures organisationnelles	
Contrôle	Effectuer des examens pour l'assurance de la cybersécurité	
Sous-contrôles	G3.2.1	Audit indépendant de cybersécurité
		L'approche de l'OSE à l'égard de la gestion de la sécurité de l'information et de sa mise en œuvre (c.-à-d. les objectifs de contrôle, les contrôles, les politiques, les processus et les procédures de sécurité de l'information) doit être examinée de façon indépendante à des intervalles planifiés ou lorsque des changements importants se produisent.
	G3.2.2	Conformité aux politiques et normes de sécurité
		Les responsables examinent régulièrement la conformité du traitement et des procédures de l'information dans leur domaine de responsabilité avec les politiques, normes et autres exigences de sécurité appropriées.
	G3.2.3	Audit de la conformité technique
		Les systèmes d'information doivent faire l'objet d'un examen régulier pour s'assurer qu'ils sont conformes aux politiques et aux normes de sécurité de l'information de l'OSE.

G3.3	**Audit**	
Objectif	S'assurer que le programme de cybersécurité de l'OSE et ses opérations font l'objet d'un audit indépendant afin de fournir une assurance de l'efficacité du programme de protection de l'institution.	
Contrôle	Effectuer un audit régulier des fonctions de cybersécurité à l'OSE	
Sous-contrôles	G3.3.1	Vérification interne
		L'OSE procède à des audits internes à intervalles réguliers afin de fournir des assurances sures : a. l'harmonisation du programme et des opérations de sécurité de cyber avec les pratiques exemplaires b. l'alignement et conformité aux exigences togolaises en matière de cybersécurité c. l'identification des risques découlant de l'évaluation et ceux ayant été traités et corrigés.
	G3.3.2	Audit externe/Assurance
		L'OSE procède régulièrement à une évaluation de la cybersécurité au moins une fois tous les deux ans par un fournisseur externe indépendant et réputé. L'évaluation devrait inclure des tests d'intrusion techniques de l'infrastructure OSE.

G3.4	Performances en matière de cybersécurité	
Objectif	Mettre en place des indicateurs de performance afin de déterminer l'efficacité du programme de cybersécurité au sein de l'OSE	
Contrôle	Élaborer des indicateurs de performance pour mesurer l'efficacité des programmes et des opérations de cybersécurité	
Sous-contrôles	G3.4.1	Indicateurs de performance
		L'OSE élabore et met en œuvre des indicateurs de performance clés pour mesurer la performance des mesures de cybersécurité, notamment : a. Nombre d'incidents de sécurité détectés et évités b. Nombre de risques identifiés et corrigés c. Progression des vulnérabilités identifiées et corrigées d. Respect des présentes règles de cybersécurité e. Performances par rapport au PSO etc.
	G3.4.2	Tableau de bord de cybersécurité
		L'OSE élabore un tableau de bord de cybersécurité mettant en évidence les indicateurs de performance clés dans les domaines de la cybersécurité. Le tableau de bord doit être examiné et approuvé par la haute direction ou le comité directeur de la cybersécurité.

G4 – Gestion des risques de cybersécurité

S'assurer que les risques liés à la sécurité de l'information dans l'OSE sont identifiés, évalués et que ces risques sont traités conformément aux exigences et aux objectifs de sécurité de l'information de l'OSE.

L'analyse des risques consiste à identifier les principaux scénarios pertinents de menaces potentielles ou d'actes intentionnels possibles visant à interrompre le fonctionnement de l'Infrastructure Essentielle ou à la détruire.

G4.1	Méthodologie d'évaluation des risques	
Objectif	Mettre en place un processus d'identification des risques et d'évaluation régulière des risques	
Contrôle	Élaborer et documenter une méthodologie d'identification et d'évaluation des risques	
Sous-contrôles	G4.1.1	Identification des risques
		L'OSE dispose d'un processus documenté d'identification des risques conformément aux politiques, normes et procédures de cybersécurité publiées.
	G4.1.2	Méthodologie d'évaluation des risques
		L'OSE élabore une méthodologie d'évaluation des risques qui s'aligne sur les exigences des programmes de cybersécurité ainsi que sur les meilleures pratiques mondiales.
	G4.1.3	Fréquence de l'évaluation des risques

		L'OSE détermine une fréquence d'évaluation des risques conforme à la stratégie et aux opérations organisationnelles, idéalement une évaluation des risques par an.
	G4.1.4	Déterminer les critères de risque acceptables
		Identifier les critères de risques acceptables pour l'OSE dans le cadre de la méthode d'évaluation des risques
	G4.1.6	Déterminer la portée de l'évaluation des risques
		La portée de l'évaluation des risques est définie en collaboration avec les parties prenantes concernées dont l'environnement doit être évalué dans le cadre de cet exercice.
	G4.1.7	Menaces et vulnérabilités
		L'OSE dans le cadre de la méthodologie d'évaluation des risques détermine les menaces et les vulnérabilités connexes.
	G4.1.8	Sensibilisation à l'évaluation des risques
		L'OSE sensibilise tous les intervenants et le personnel à l'évaluation des risques sur la méthodologie d'évaluation des risques.

G4.2	**Évaluation du risque**	
Objectif	Effectuer une évaluation régulière des risques conformément à la méthodologie approuvée	
Contrôle	Effectuer une évaluation régulière des risques	
Sous-contrôles	G4.2.1	Évaluation régulière des risques
		L'OSE effectue une évaluation régulière et détaillée des risques conformément à la méthodologie d'évaluation des risques approuvée.
	G4.2.2	Analyse et hiérarchisation des risques
		L'OSE analyse et hiérarchise les risques en fonction de leur criticité afin d'établir des plans et des contrôles de prévention.
	G4.2.3	Résultats de l'évaluation des risques
		Les résultats d'évaluation des risques doivent être documentés et communiqués à toutes les parties prenantes pour avis et observations.

G4.3	**Traitement et atténuation des risques**	
	Objectif : Mettre en place un processus de prévention et de traitement des risques.	
Contrôle	Traiter et à atténuer les risques	
Sous-contrôles	G4.3.1	Plan de traitement des risques
		Un contrôle et un plan appropriés de traitement des risques doivent être identifiés pour faire face aux risques découlant de l'exercice d'évaluation des risques.
	G4.3.2	Approuver le plan de traitement des risques
		Le plan de traitement des risques identifié doit être documenté et approuvé par la haute direction appropriée.
	G4.3.3	Examen du traitement des risques

		Le plan de traitement des risques doit contenir des indicateurs de performance et faire l'objet d'un examen sur une fréquence régulière d'au moins deux fois par an.

G4.4	**Acceptation des risques**	
	Objectif : Avoir un processus formel en place pour l'acceptation des risques	
Contrôle	Gérer les risques acceptés	
Sous-contrôles	G4.4.1	Gestion des risques non traités
		L'OSE doit mettre en place un processus pour documenter le risque non traité ainsi que les risques résiduels et détermine comment ces risques doivent être gérés à l'avenir. Les risques non traités doivent être documentés et approuvés par le comité de direction.
	G4.4.2	Renonciation aux risques
		L'OSE dispose d'un processus de renonciation aux risques dans le cadre duquel le risque non traité est réduit au minimum par des contrôles compensatoires et les risques résiduels sont documentés et examinés sur une base trimestrielle jusqu'à ce que le risque soit traité.

G5 – Ressources Humaines

La sécurité des ressources humaines est une partie importante de la portée globale de la cybersécurité, car l'erreur humaine est la source principale dans plus de 90 % des incidents de sécurité (clic sur un lien de malveillant, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées). Il est donc important de mener et de mettre en œuvre des processus et des procédures de sécurité des ressources humaines pour tous les OSE.

G5.1	**Vérifications avant l'emploi**	
Objectif	S'assurer que les employés et les sous-traitants comprennent leurs responsabilités et sont adaptés aux rôles pour lesquels ils sont considérés.	
Contrôle	Réaliser des vérifications des antécédents avant l'embauche du personnel	
Sous-contrôles	G5.1.1	Vérification des antécédents
		Les vérifications des antécédents de tous les candidats à l'emploi doivent être effectuées conformément aux lois, règlements et éthiques pertinents et sont proportionnelles aux exigences de l'OSE, à la classification des informations à consulter et aux risques présentés, le cas échéant.
	G5.1.2	Communication relative au personnel essentiel
		L'OSE communique à l'ANCy toute embauche de son personnel essentiel
	G5.1.3	Conditions d'emploi
		Les ententes contractuelles avec les employés et les sous-traitants doivent énoncer leurs responsabilités et celles de l'OSE en matière de sécurité de l'information.

G5.2	Vérifications pendant l'emploi	
	Objectif : S'assurer que les employés et les sous-traitants sont conscients et s'acquittent de leurs responsabilités en matière de sécurité de l'information.	
Contrôle	Faire adhérer les employés aux politiques et pratiques de cybersécurité	
Sous-contrôles	G5.2.1	Responsabilités de gestion
		La direction exige que tous les employés et sous-traitants appliquent la sécurité de l'information conformément aux politiques et procédures établies de l'OSE.
	G5.2.2	Sensibilisation, éducation et formation à la sécurité de l'information
		Tous les employés de l'OSE et, le cas échéant, les sous-traitants doivent recevoir une éducation et une formation ou une sensibilisation appropriée et des mises à jour régulières des politiques et procédures organisationnelles, selon ce qui est pertinent pour leur fonction. Plus précisément pour respecter les exigences ci-dessous : a. Sensibilisation et formation du personnel b. Le PSO présente un plan de sensibilisation et de formation du personnel incluant la direction de l'OSE, les services en charge des Ressources Humaines, de la communication interne et externe, du système d'information, les directions métiers. c. Ce plan de formation est adapté aux différents interlocuteurs, en fonction de leurs responsabilités et de leurs fonctions dans l'OSE et dans le cadre du PSO. d. Chaque utilisateur de l'OSE a, au minimum, une session de formation ou de sensibilisation annuelle. e. Les administrateurs du système d'information et le Personnel Essentiel sont régulièrement formés sur la maintenance des équipements, des logiciels et des services dont ils ont la responsabilité.
	G5.2.3	Processus disciplinaire
		Un processus disciplinaire officiel et communiqué doit être mis en place pour prendre des mesures contre les employés qui commettent une atteinte à la sécurité de l'information.
	G5.2.4	Disponibilité du Personnel Essentiel
		Le Personnel Essentiel de l'OSE doit être suffisamment disponible pour une fourniture continue et ininterrompue du ou des Service(s) Essentiel(s) de l'OSE. L'OSE communique à l'ANCy et/ou à son délégataire la liste de son Personnel Essentiel dans un délai de trois (3) mois à compter de la notification de sa désignation comme OSE, ainsi qu'après chaque mise à jour de ces coordonnées.

G5.3	Cessation d'emploi et changement d'emploi	
Objectif	Protéger les intérêts de l'OSE dans le cadre du processus de changement ou de cessation d'emploi	
Contrôle	Sécuriser la cessation ou le changement d'emploi	
Sous-contrôles	G5.3.1	Cessation d'emploi ou changement de responsabilités
		Les responsabilités et les obligations en matière de sécurité de l'information qui restent valables après la cessation d'emploi ou le changement d'emploi doivent être définies, communiquées à l'employé ou à l'entrepreneur et appliquées.
	G5.3.2	Communication relative au personnel essentiel
		L'OSE communique à l'ANCy toute cessation d'emploi de son personnel essentiel

G6 – Relation fournisseur

L'objectif de ce contrôle est de s'assurer que toutes les relations avec les fournisseurs sont exploitées et gérées de manière sécurisée afin de ne pas introduire de risques de sécurité pour l'OSE dans la conduite des affaires.

G6.1	Sécurisation des relations avec les fournisseurs	
Objectif	S'assurer que toutes les relations avec les fournisseurs sont sécurisées	
Contrôle	Avoir des accords et des processus avec les fournisseurs pour leur adhésion aux politiques de cybersécurité de l'OSE	
Sous-contrôles	G6.1.1	Politique relative aux relations avec les fournisseurs
		Les exigences en matière de sécurité des informations doivent être définies, documentées et convenues avec le fournisseur afin de minimiser les risques associés aux relations contractuelles avec ce dernier.
	G6.1.2	Accords avec les fournisseurs
		Toutes les exigences de sécurité doivent être documentées dans tous les accords.

G6.2	Gestion de la prestation de services	
Objectif	Avoir un niveau convenu de cybersécurité et de prestation de services	
Contrôle	S'assurer que les services convenus sont maintenus tout le temps	
Sous-contrôles	G6.2.1	Surveiller et examiner les services des fournisseurs
		Surveiller et examiner régulièrement les services des fournisseurs au moins une fois par an.
	G6.2.2	Changements aux services des fournisseurs
		Toute modification apportée aux services des fournisseurs doit être notifiée et gérée de manière à identifier les risques liés à la sécurité de l'information.

G6.3	Processus d'approvisionnement	
Objectif	S'assurer que toutes les relations avec les fournisseurs sont sécurisées et conformes aux réglementations et aux politiques de l'OSE	
Contrôle	Inclure la sécurité dans les accords avec les fournisseurs	
Sous-contrôles	G6.3.1	Obtention d'accords
		Les accords avec les fournisseurs doivent traiter des aspects liés : a. Au respect de l'environnement légal togolais dans tout contrat avec un fournisseur b. A la protection des données à caractère personnel c. A la protection des informations confidentielles concernant les IE d. A la situation financière du fournisseur au moment de la signature du contrat et à son actionnariat e. A la signature d'un accord de confidentialité avec des sanctions réelles en cas de violation, avant tout autre contrat f. Aux possibilités de transfert de droits d'auteur dans le cadre du développement de logiciels pour un droit de modifications du logiciel ou de développements ultérieurs de manière indépendante, ou au moins à un mécanisme de séquestre (notarié par exemple) concernant les codes sources et l'environnement de développement d'une application donnée g. A toutes solutions, organisationnelles, matérielles et techniques concernant la continuité de services du fournisseur en cas d'une défaillance de ce dernier h. Aux règles de suppression des erreurs signalées, sous forme « d'accord de niveau de service » (SLA – Service-Level Agreement), avec procédures de coopération pour une suppression en temps voulu des erreurs signalées, et sanction pour retards ou non-suppression i. Au partenariat en cas de détection de nouvelles vulnérabilités des logiciels fournis par un éditeur avec un "accord de niveau de service" (SLA – Service-Level Agreement) j. A l'accès au code source, pendant toute la durée du contrat et après sa résiliation, par l'OSE ou à l'auditeur choisi par les parties, concernant les logiciels critiques pour les IE de l'OSE k. Aux dispositions sur la procédure de gestion des modifications d'un logiciel et le mode de rémunération du prestataire de services l. Aux dispositions relatives aux mécanismes de sanctions au bénéfice de l'OSE à l'encontre d'un fournisseur en cas de violation de ses obligations. L'objectif est que les sanctions soient à la hauteur des responsabilités du fournisseur et des risques pour l'OSE m. A l'obligation du fournisseur de souscrire à une police d'assurance contre les dommages causés par une mauvaise exécution du contrat. n. A une procédure permettant de prendre des mesures immédiates en cas de menaces pour la fourniture d'un service essentiel résultant d'attaques contre l'Infrastructure Essentielle

		o. A une procédure de voie d'escalade formalisée pour résoudre des problèmes découlant de l'exécution du contrat

G6.4	Logiciel acheté	
Objectif	Protéger les logiciels achetés	
	Prendre des dispositions renforçant la sécurité contre les menaces des logiciels fournis, y compris notamment, de systèmes d'automatisation ou de contrôle industriel	
Contrôle	S'assurer de la mise en place d'un mécanisme adéquat pour couvrir les risques liés aux logiciels achetés	
Sous-Contrôle	G6.4.1	S'assurer qu'il n'y a pas de faille de sécurité dans les logiciels fournis
		L'obligation du fournisseur de vérifier que le logiciel fourni ne présente pas de lacunes de sécurité connues et d'informer l'OSE de toute lacune existante.
	G6.4.2	Correction des vulnérabilités logicielles
		La déclaration que l'architecture du logiciel fourni permet de supprimer les éventuelles failles de sécurité qui seront détectées pendant le cycle de vie du logiciel.
	G6.4.3	Composants logiciels
		La liste de tous les composants du logiciel fourni est jointe au contrat.
	G6.4.4	Déclaration du fournisseur sur le logiciel fourni
		L'éditeur de logiciels met à la disposition une déclaration sur les règles qu'il applique pour combler les lacunes de sécurité détectées, les règles d'information des utilisateurs sur les lacunes de sécurité détectées et les règles de distribution des correctifs.

P1 – Contrôle d'accès

Pour garantir des contrôles d'accès sécurisés, des politiques et des procédures sont mises en place et appliquées aux utilisateurs, aux réseaux, aux systèmes, aux applications et aux systèmes d'exploitation afin de prévenir ou de minimiser les tentatives et les accès non autorisés.

P1.1	**Exigences métiers pour le contrôle d'accès**	
Objectif	Contrôler l'accès aux systèmes d'information et de traitement de l'information au niveau de l'utilisateur, de l'application, du réseau et du système d'exploitation, y compris l'informatique mobile ainsi que les procédures d'autorisation des actifs informationnels.	
Contrôle	Contrôler l'accès aux ressources de l'OSE	
Sous-contrôles	P1.1.1	Politique de contrôle d'accès
		La politique de contrôle d'accès doit être mise en place et documentée en fonction des exigences métiers et de cybersécurité.
	P1.1.2	Accès aux systèmes, aux réseaux et aux applications
		Accès aux réseaux, aux systèmes et aux infrastructures essentielles uniquement après autorisation.

P1.2	**Gestion de l'accès des utilisateurs**	
Objectif	Assurer l'accès autorisé des utilisateurs et empêcher l'accès non autorisé aux systèmes et services	
Contrôle	Gérer les exigences d'accès des utilisateurs	
Sous-contrôles	P1.2.1	Enregistrement et radiation de l'utilisateur
		Un processus formel d'enregistrement et de radiation des utilisateurs est mis en œuvre pour permettre l'attribution des droits d'accès.
	P1.2.2	Provisionnement de l'accès utilisateur
		Un processus documenté de provisionnement de l'accès des utilisateurs doit être mis en œuvre pour attribuer ou révoquer les droits d'accès pour tous les types d'utilisateurs à tous les systèmes et services.
	P1.2.3	Gestion des droits d'accès privilégiés
		L'attribution et l'utilisation des droits d'accès privilégiés sont restreintes et contrôlées sur la base du principe du « need to know et du need to have ». Les droits d'accès privilégiés ne sont accordés qu'aux personnes qui en fonction de leurs positions et de leurs rôles en un moment donné en ont réellement besoin.
	P1.2.4	Gestion des informations d'authentification restreintes des utilisateurs
		L'attribution d'informations d'authentification restreintes doit être contrôlée au moyen d'un processus documenté.
	P1.2.5	Examen régulier des droits d'accès des utilisateurs
		Les propriétaires d'actifs doivent examiner les droits d'accès des utilisateurs à intervalles réguliers.
	P1.2.6	Suppression ou ajustement des droits d'accès

		Les droits d'accès de tous les employés et utilisateurs externes aux installations de traitement de l'information doivent être supprimés à la cessation de leur emploi ou de leur contrat ou ajustés en cas de modification.

P1.3	**Responsabilités de l'utilisateur**	
Objectif	Assurer la responsabilisation à l'égard de la protection des renseignements d'authentification des utilisateurs	
Contrôle	Protéger les informations d'authentification des utilisateurs	
Sous-contrôles	P1.3.1	Utilisation des informations d'authentification restreinte
		Les utilisateurs doivent respecter les exigences et les pratiques de cybersécurité de l'OSE en ce qui concerne l'utilisation des informations secrètes d'authentification.

P1.4	**Contrôle d'accès aux systèmes et aux applications**	
Objectif	Empêcher l'accès non autorisé aux systèmes et applications	
Contrôle	Restreindre l'accès aux systèmes et aux applications	
Sous-contrôles	P1.4.1	Restrictions d'accès aux informations
		L'accès aux fonctions de l'information et du système d'application est limité conformément à la politique de contrôle d'accès.
	P1.4.2	Procédures de connexion sécurisées
		Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications est contrôlé par une procédure de connexion sécurisée.
	P1.4.3	Système de gestion des mots de passe
		Les systèmes de gestion des mots de passe sont interactifs et garantissent la qualité des mots de passe.
	P1.4.4	Utilisation de programmes utilitaires privilégiés
		L'utilisation de programmes utilitaires susceptibles de contourner les contrôles du système et des applications doit être restreinte et étroitement contrôlée.
	P1.4.5	Contrôle d'accès au code source
		L'accès au code source des logiciels développés en internes doivent être restreint et diffusé seulement sur la base du principe du « need to know et du need to have ».
	P1.4.6	Authentification
		Tous les systèmes de l'OSE sont accessibles via des mécanismes d'authentification où des noms d'utilisateur et des mots de passe sont utilisés pour accéder aux systèmes. Une authentification multi facteur supplémentaire sera déployée pour tous les accès aux systèmes critiques ainsi que l'accès aux informations sensibles.
	P1.4.7	Comptes par défaut du fournisseur

		Tous les comptes et mots de passe par défaut du fournisseur doivent être remplacés par les comptes uniques de l'OSE conformément à la stratégie de mot de passe (sous-contrôle 4.4.9).
	P1.4.8	Les éléments secrets d'authentification
		Les éléments secrets d'authentification sont modifiés par l'OSE chaque fois que cela est nécessaire, entre autres : a. Suite à l'installation par le fabricant ou le fournisseur d'une ressource, avant sa mise en service. b. à chaque retrait d'un utilisateur d'un compte commun de plusieurs utilisateurs. c. en cas de suspicion de compromission. d. trimestriellement (au maximum). Quand un élément secret ne peut pas être modifié, l'OSE met en place un contrôle d'accès approprié à la ressource concernée ainsi que des mesures de traçabilité des accès et de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe. Les utilisateurs qui n'en ont pas la responsabilité ne peuvent pas modifier les éléments secrets d'authentification. Ils ne peuvent pas non plus accéder à ces éléments en clair.
	P1.4.9	Mot de passe en tant que données d'authentification
		Lorsque les éléments secrets d'authentification sont des mots de passe : a. L'OSE a une politique de construction de mots de passe "forts" et définit la complexité (types de caractères) et la longueur minimale de ces mots de passe, tout en prenant en compte les limites permises par la ressource concernée. L'OSE met en place, autant que possible, des mécanismes de contrôles des règles définies, et les documente. b. L'OSE s'assure que les mots de passe temporaires attribués à un utilisateur sont uniques et qu'ils sont modifiés lorsqu'ils sont utilisés pour la première fois. c. Lors du transfert d'un mot de passe, il convient d'utiliser un canal de communication différent de celui utilisé pour le transfert d'un identifiant, par exemple l'identifiant par courrier électronique et le mot de passe par SMS, MMS, Messagerie instantanée, ou autre canal de communication approprié. d. L'OSE vérifie que les utilisateurs ne puissent pas réutiliser le même mot de passe entre plusieurs comptes, avec une particulière attention sur les comptes privilégiés. e. Dans le cadre de la sauvegarde des mots de passe, seules les "hash" sont conservés et dans les cas où il est nécessaire de récupérer un mot de passe, il doit être conservé dans une enveloppe sécurisée dans un coffre.
	P1.4.10	Accès à distance
		Lorsque l'accès à l'IE est effectué depuis un site extérieur à celui de l'OSE : a. il doit être protégé par des mécanismes de chiffrement et d'authentification, des solutions de chiffrement de la

		transmission des données, telles que VPN, SSH ou autres, afin d'éviter les écoutes et l'interception des informations ; b. le mécanisme d'authentification est renforcé en mettant en œuvre une authentification à double facteur (authentification impliquant à la fois un élément secret et un autre élément propre à l'utilisateur), sauf si des raisons techniques ou opérationnelles ne le permettent pas, ce qui doit être documenté le cas échéant ; c. toutes les sessions d'accès à distance doivent être automatiquement enregistrées. Cela s'applique aux employés et aux prestataires de services (tel que le personnel technique externe) ; d. les mémoires de masse de ces équipements doivent être en permanence protégées par des mécanismes de chiffrement et d'authentification.

P2 – Gestion des actifs

Il s'agit d'une part de s'assurer que tous les actifs sont référencés et inclus dans les programmes de sécurité et d'autre part d'assurer la protection des actifs informationnels et leur classification.

Ce domaine fournit des assurances contre les actifs non autorisés à placer dans l'environnement de l'OSE, fournit un processus visant à maintenir la responsabilité lors de la gestion, et du traitement des informations organisationnelles et des actifs d'infrastructure.

P2.1	**Responsabilité des actifs**	
Objectif	Identifier les actifs de l'OSE et définir la protection et les responsabilités appropriées	
Contrôle	Gérer les actifs	
Sous-contrôles	P2.1.1	Cartographie des actifs
		L'OSE réalise l'inventaire des actifs pour son IE à la fois logiciel et matériel.
	P2.1.2	Propriété des actifs
		Tous les actifs doivent être attribués à un propriétaire spécifié avec des responsabilités de gestion pour chaque actif identifié.
	P2.1.3	Utilisation acceptable des biens
		L'OSE doit identifier les règles régissant l'utilisation des actifs informationnels. Ces règles doivent être identifiées, documentées et mises en œuvre.
	P2.1.4	Rendement des actifs
		L'OSE met en place un processus pour tous les utilisateurs, le personnel et les sous-traitants qui détiennent des actifs de l'OSE à retourner à la fin de leurs engagements. La restitution des ressources doit également être effectuée en cas de changement d'emploi ou lorsque l'employé cesse d'utiliser la ressource dans l'exercice de ses fonctions.

P2.2	Classification des actifs	
Objectif	S'assurer que les actifs informationnels bénéficient d'un niveau de protection approprié	
Contrôle	Classifier les actifs	
Sous-Contrôle	P2.2.1	Classification des actifs informationnels
		Les OSE classent leurs informations en fonction de la sensibilité de l'accès ou de la divulgation non autorisés.
	P2.2.2	Étiquetage des informations
		Des procédures d'étiquetage conformes à la classification des actifs sont élaborées.
	P2.2.3	Gestion des actifs
		Ces procédures sont utilisées pour la manipulation des actifs conformément au système de classification des actifs.

P2.3	Gestion des médias	
Objectif	Empêcher la modification, la suppression, la divulgation ou la destruction non autorisées d'informations stockées dans un média	
Contrôle	Avoir des processus et des procédures pour la gestion des médias	
Sous-contrôles	P2.3.1	Gestion des supports de suppression
		L'OSE devra mettre en place des procédures documentées pour la suppression des supports médias conformément au système de classification.
	P2.3.2	Cession des supports
		Les supports doivent être éliminés en toute sécurité lorsqu'ils ne sont plus nécessaires.
	P2.3.3	Transfert de support physique
		Les OSE doivent mettre en place des procédures et des équipements pour protéger les supports contenant des informations contre l'accès non autorisé, l'utilisation abusive ou la corruption pendant le transport.

P2.4	Politique de gestion des actifs	
Objectif	Disposer d'une politique pour diriger et guider les OSE ayant un processus et une pratique de gestion des actifs	
Contrôle	Avoir une politique de gestion des actifs documentée	
Sous-contrôles	P2.4.1	Contenu de la politique
		La politique de gestion des actifs doit : a) Refléter et être approprié aux actifs des OSE b) Fournir un cadre et une structure sur la gestion des actifs c) Responsabiliser des personnes dans la gestion des actifs

		d) S'aligner sur d'autres politiques de cybersécurité et directives de cybersécurité en matière de la gestion des actifs

P2.5	Gestion des équipements personnels (BYOD – Bring Your Own Device)	
Objectif	Faciliter l'intégration des équipements et des terminaux personnels (Bring Your Own Device) de manière sécurisée tout en accédant aux ressources d'information des OSE.	
Contrôle	Elaborer des règles régissant l'utilisation sécurisées des équipements personnels	
Sous-contrôles	P2.5.1	Utilisation acceptable du BYOD
		Les règles acceptables sur l'utilisation du BYOD doivent être documentées et communiquées. Utilisation de contrôles techniques à adopter pour faire respecter les règles d'utilisation du BYOD.
	P2.5.2	Séparation des informations personnelles avec celles des OSE
		L'accès à l'information doit être séparé entre les données personnelles et les données de l'OSE.
	P2.5.3	Accès BYOD basé sur les rôles (fonctions)
		Définir l'accès BYOD en fonction des différents rôles et pour des besoins de traçabilité.

P3 – Sécurité des communications

Sécuriser les canaux de communication, y compris l'infrastructure sous-jacente entre diverses organisations, ainsi que les communications internes au sein de l'OSE.

Ce domaine répond également aux exigences relatives à la sécurisation de l'information en transit ainsi qu'au partage de l'information entre divers OSE et individus. Cela assure en outre la présence de contrôles pour protéger l'échange d'informations.

P3.1	Contrôles de sécurité réseau	
	Objectif : Assurer la protection de l'information dans les réseaux et ses moyens de traitement	
Contrôle	Gérer et contrôler les réseaux pour protéger les informations contenues dans les systèmes et les applications.	
Sous-contrôles	P3.1.1	Contrôles réseau
		Les réseaux sont gérés et contrôlés pour protéger les informations stockées, traitées et transmises dans les systèmes et les applications.
	P3.1.2	Sécurité des services réseau
		Les mécanismes de sécurité, les niveaux de service et les exigences de gestion de tous les services de réseau doivent être identifiés et inclus dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.
	P3.1.3	Ségrégation dans les réseaux

		Les groupes de services d'information, d'utilisateurs et de systèmes d'information sont séparés sur les réseaux.

P3.2	**Transfert d'informations**	
	Objectif : Maintenir la sécurité des informations transférées au sein d'un OSE et avec toute entité externe	
Contrôle	Contrôler et sécuriser les flux d'informations	
Sous-contrôles	P3.2.1	Politiques et procédures de transfert de l'information
		Des politiques, des procédures et des contrôles formels en matière de transfert doivent être mises en place pour protéger le transfert d'information par l'utilisation de tous les types d'installations de communication.
	P3.2.2	Accords sur le transfert d'informations
		Les ententes portent sur le transfert sécurisé d'informations sensibles entre l'OSE et les parties externes.
	P3.2.3	Messagerie électronique
		Les informations contenues dans la messagerie électronique doivent être protégées de manière appropriée.
	P3.2.4	Accords de confidentialité ou de non-divulgation
		Les exigences en matière d'ententes de confidentialité ou de non-divulgation reflétant les besoins de l'OSE en matière de protection de l'information doivent être identifiées, régulièrement examinées et documentées.

P3.3	**Filtrage réseau**	
Objectif	Filtrer le trafic réseau non autorisé et autoriser uniquement le trafic requis à traverser le réseau OSE	
Contrôle	Filtrer le trafic réseau non autorisé	
Sous-contrôles	P3.3.1	Filtrage du flux de données
		L'opérateur de services essentiels met en place des mécanismes de filtrage des flux de données circulant dans ses Infrastructures Essentielles et avec les infrastructures tierces afin de bloquer la circulation de flux non strictement nécessaires au fonctionnement de ses infrastructures et pour l'ensemble des systèmes.
	P3.3.2	Documentation des règles de filtrage
		Une documentation à jour doit faire part des règles de filtrage mises en place pour chaque IE ainsi que des risques acceptés par l'OSE et des mesures supplémentaires de réduction du risque que l'OSE met en place.
	P3.3.3	Paramètres de filtrage
		L'OSE définit les règles de filtrage des flux de données (filtrage sur les adresses réseau, sur les protocoles, sur les numéros de port, etc.) afin

		de limiter la circulation des flux de données nécessaires au fonctionnement et à la sécurité de ses IE.
	P3.3.4	Solution de filtrage à mettre en place
		L'OSE précise les solutions de filtrage telles que pare-feu ou division en VLAN utilisées pour l'optimisation du filtrage et de la séparation du trafic entrant et sortant des IE, ainsi que sur les flux entre les sous-systèmes des IE.
	P3.3.5	Empêcher l'accès direct à Internet
		Les IE de l'OSE n'ont pas d'accès direct à internet. Les ressources matérielles et logicielles des IE de l'OSE ne sont pas directement connectées à Internet. Elles passent par un pare-feu-passerelle (gateway firewall) de dernière génération pour empêcher des connexions réseau sortantes et sont séparées des serveurs DNS, des serveurs de courrier électronique et des serveurs proxy.
	P3.3.6	Avoir mis en place des procédures d'enregistrement, de surveillance et de blocage
		L'OSE met en œuvre les procédures d'enregistrement, de surveillance et de blocage des accès aux adresses IP nuisibles, aux publicités et aux réseaux anonymes. La catégorisation (liste blanche) des types de contenu de réseau et des sites ayant une bonne réputation est mise en place et documentée.
	P3.3.7	Par défaut, bloquer le trafic non requis
		Par défaut, l'OSE bloque tout trafic réseau (entrant ou sortant) inutile et non autorisé – y compris celui généré par des applications non fiables – par l'utilisation de solutions adéquates telles que des IPS/IDS ou des pare-feu applicatifs (Web Application Firewall ou WAF).
	P3.3.8	Filtrage et contrôle DNS
		L'OSE ne permet la connexion qu'aux seuls serveurs DNS de confiance et un filtrage détaillé des requêtes DNS doit être effectué.

P3.4	**Protection des e-mails**	
Objectif	Protéger les messages électroniques et les communications avec l'extérieur	
Contrôle	Protéger le trafic de messagerie et le système	
Sous-contrôles	P3.4.1	Avoir une stratégie et un plan de protection des e-mails documentés
		L'OSE élabore, met en œuvre et documente son plan de protection des messages électroniques–pour se protéger contre les courriels d'hameçonnage, d'harponnage (phishing, spear phishing) ainsi que les possibilités d'usurpation d'identités, principaux vecteurs d'attaques informatiques.
	P3.4.2	Compte de messagerie individuel pour tout le personnel
		Chaque utilisateur de l'OSE a une adresse de courrier électronique, propriété de l'OSE, contrôlée par l'OSE.
	P3.4.3	Limitation de l'utilisation des e-mails personnels
		L'utilisation d'autres adresses de courrier électronique par l'utilisateur (notamment adresses emails personnelles) n'est pas accessible sur les infrastructures informatiques de l'OSE. Tout cas

		contraire est justifié, documenté, et des mécanismes de traçabilité sont mis en place pour réduire le niveau de risque lié à cette utilisation.
	P3.4.4	Sensibilisation à l'utilisation et à la protection des e-mails
		L'OSE met en œuvre son plan d'éducation des utilisateurs à l'utilisation de la messagerie électronique d'entreprise, moyen de base pour protéger ses IE. Cette éducation comprend entre autres : a) Les moyens d'identifier et d'éviter les courriels d'hameçonnage (par exemple avec des liens pour se connecter à de fausses pages) ; b) L'explication et l'incitation à l'utilisation des adresses de courrier électronique fournies par l'OSE à l'utilisateur dans le cadre de ses fonctions.
	P3.4.5	Protection des e-mails contre les menaces connues et inconnues
		L'OSE définit, met en œuvre et documente les procédures appropriées afin : a. D'isoler du contenu du réseau (sandboxing) par un blocage en cas de comportement suspect, par exemple basé sur le trafic réseau, les fichiers nouveaux ou modifiés et autres changements inhabituels du système ; b. D'utiliser une catégorisation des types de pièces jointes autorisées (liste blanche), interdites (liste noire), y compris les archives et les archives imbriquées, et protégées par un mot de passe ; c. D'analyser/nettoyer les liens, les fichiers PDF et de passer les macros Microsoft Office ou leur configuration par une période de quarantaine ; d. D'utiliser le "Sender Policy Framework" ou le "Sender ID" pour vérifier les courriers électroniques entrants ; e. D'utiliser les méthodes "SPF TXT hard fail", les enregistrements "DNS DMARC" et les enregistrements "DNS DKIM" (DomainKeys Identified Mail) pour bloquer les courriers électroniques se faisant passer pour des courriers électroniques de votre propre organisation ; f. De bloquer les services de cloud computing non fiables/non approuvés ; g. D'enregistrer les destinataires, la taille, le nombre et la fréquence des e-mails envoyés ; h. De bloquer les messages contenant des pièces jointes sous forme de fichiers exécutables.
	P3.4.6	Chiffrement des e-mails
		L'OSE élabore, met en œuvre et documente des mécanismes de chiffrement puissants utilisés entre les serveurs de courrier électronique ou pour protéger le courrier électronique lui-même.
	P3.4.7	Protection des transactions
		Les informations sur les détails des transactions ne doivent pas être disponibles sur les réseaux publics.

P3.5	Comptes d'administration – Limitation et supervision des droits d'accès privilégiés	
Objectif	Prévenir les abus ou l'accès non autorisé aux comptes privilège	
Contrôle	Disposer d'un processus de protection des comptes à privilège	
Sous-contrôles	P3.5.1	Gestion de compte privilège
		L'OSE définit, conformément à son PSO, les règles de gestion et d'attribution des comptes privilégiés liés à ses Infrastructures Essentielles.
	P3.5.2	Procédures pour les modifications de compte à privilège
		La procédure de modification (ajout, suppression, suspension ou modification des droits associés) sur les comptes privilégiés, inclut une vérification stricte des droits, pour s'assurer que seuls les droits strictement nécessaires sont accordés en cohérence avec les besoins d'utilisation de chaque compte.
	P3.5.3	Allocation documentée des comptes à privilège avec les droits respectifs
		Une documentation des comptes privilégiés et des droits associés est établie et maintenue, indiquant l'ensemble des comptes et droits privilégiés existants liés aux IE, ainsi que toutes les fonctions privilégiées concernant les IE, toutes les procédures et fonctions de protection mises en place et décrivant les risques existants, acceptés et gérés. La liste des comptes privilégiés des IE est systématiquement maintenue.
	P3.5.4	Affectations de privilège minimales
		Suivant la définition de ses fonctions, chaque utilisateur ayant des droits privilégiés, principalement pour l'administration des systèmes doit avoir, autant que possible, des droits strictement restreints au périmètre fonctionnel et technique dont il est responsable.
	P3.5.5	Comptes administratifs privilégiés
		Les droits d'accès privilégiés, principalement pour l'administration, sont identifiés par système ou par processus, et par utilisateur auquel ils sont accordés.
	P3.5.6	Allocation de compte de privilège de l'administrateur minimum
		Les privilèges d'administrateur pour les systèmes d'exploitation, les bases de données et les applications sont limités au minimum nécessaire, en fonction des tâches à effectuer.
	P3.5.7	Droits du personnel privilégié
		Les droits accordés aux employés privilégiés, dont les administrateurs, doivent être divisés en trois comptes : a. Compte d'utilisateur – Compte personnel ; b. Compte d'administrateur local – Compte d'assistance aux utilisateurs ; c. Compte d'administrateur sur les serveurs - Compte d'administration des serveurs.

	P3.5.8	Utilisation des comptes à privilège
		Les comptes privilégiés sont exclusivement utilisés pour des activités professionnelles impliquant des droits d'accès privilégiés. De même, les accès privilégiés sont exclusivement réalisés par des comptes privilégiés.
	P3.5.9	Authentification de compte à privilège
		L'authentification multi-facteur est utilisée pour tous les utilisateurs aux droits d'accès privilégiés par accès à distance (à partir de réseaux externes).
	P3.5.10	Pistes d'audit de compte privé et utilisation de la solution PAM
		Des mesures de traçabilité, des fonctions privilégiées dont celles d'administration, ainsi que des comptes privilégiés sont mises en place. La restriction de l'accès des utilisateurs aux seuls systèmes et ressources dont ils ont besoin et la mise en œuvre des exigences relatives à la gestion des accès privilégiés sont facilitées par les solutions PAM (Privileged Access Management).
	P3.5.11	Audit annuel du compte de privilège
		La tenue des comptes privilégiés est auditée dans le cadre de la procédure d'accréditation annuelle.

P4 – Systèmes d'information, acquisition et maintenance

Ce domaine énumère les contrôles nécessaires pour sécuriser le processus d'acquisition, de développement et de maintenance des systèmes afin d'éviter l'utilisation abusive des informations ou la modification non autorisée et d'élever les niveaux de sécurité dans les applications, pendant le développement, ainsi que pour traiter les vulnérabilités techniques.

Le domaine intègre davantage les exigences de cybersécurité au développement du cycle de vie des systèmes et des applications.

P4.1	**Exigences de sécurité des systèmes d'information**	
Objectif	S'assurer que la sécurité de l'information fait partie intégrante des systèmes d'information tout au long du cycle de vie. Cela inclut également les exigences applicables aux systèmes d'information qui fournissent des services sur les réseaux publics.	
Contrôle	Sécuriser les systèmes de traitement des informations	
Sous-contrôles	P4.1.1	Analyse et spécifications des exigences en matière de sécurité de l'information
		Les exigences relatives à la sécurité de l'information sont incluses dans les exigences relatives à l'acquisition de nouveaux systèmes d'information ou aux améliorations apportées aux systèmes d'information existants.
	P4.1.2	Sécurisation des services applicatifs sur les réseaux publics
		Les informations impliquées dans les services applicatifs passant sur les réseaux publics doivent être protégées contre les activités

		frauduleuses, les litiges contractuels, la divulgation et la modification non autorisées.
	P4.1.3	Protection des transactions des services applicatifs
		Les informations impliquées dans les transactions de service d'application doivent être protégées afin d'éviter une transmission incomplète, un mauvais routage, une altération non autorisée des messages, une divulgation non autorisée, une duplication ou une relecture non autorisée des messages.

P4.2	**Sécurité dans les processus de développement et de support**	
Objectif	S'assurer que la sécurité de l'information est conçue et mise en œuvre dans le cycle de vie de développement des systèmes d'information	
Contrôle	S'assurer que la cybersécurité est intégrée dans les systèmes et le développement d'applications	
Sous-contrôles	P4.2.1	Politique de développement sécurisée
		Les règles pour le développement de logiciels et de systèmes doivent être établies et appliquées aux développements au sein de l'OSE.
	P4.2.2	Procédures de contrôle des modifications du système
		Les modifications apportées aux systèmes au cours du cycle de vie du développement doivent être contrôlées par l'utilisation de procédures formelles de contrôle des modifications.
	P4.2.3	Examen technique des applications après des modifications de la plate-forme d'exploitation
		Lorsque les plates-formes d'exploitation sont modifiées, les applications critiques de l'OSE doivent être examinées et testées pour s'assurer qu'il n'y a pas d'impact négatif sur les opérations ou la sécurité de celui-ci.
	P4.2.4	Restrictions sur les modifications apportées aux progiciels
		Les modifications apportées aux progiciels seront déconseillées, limitées aux modifications nécessaires et toutes les modifications seront strictement contrôlées.
	P4.2.5	Principes d'ingénierie des systèmes sécurisés
		Les principes d'ingénierie des systèmes sécurisés doivent être établis, documentés, maintenus et appliqués à tout effort de mise en œuvre de systèmes d'information.
	P4.2.6	Environnement de développement sécurisé
		Les OSE doivent établir et protéger de manière appropriée des environnements de développement sécurisés lors des développements et d'intégration de systèmes qui couvrent l'ensemble du cycle de vie desdits systèmes.
	P4.2.7	Développement externalisé
		L'OSE doit superviser et surveiller l'activité de développement de systèmes externalisés.
	P4.2.8	Tests de sécurité du système
		Des essais de la fonctionnalité de sécurité doivent être effectués pendant le développement.
	P4.2.9	Tests d'acceptation du système

		Des programmes d'essais d'acceptation et des critères connexes doivent être établis pour les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions.

P4.3	Données à tester	
Objectif	Contrôle des données à des fins de test	
Contrôle	S'assurer que les données utilisées pour les tests sont sécurisées et n'exposent pas les OSE	
Sous-contrôles	P4.3.1	Protection des données d'essai
		Les données d'essai doivent être sélectionnées avec soin, protégées et contrôlées.

P4.4	Séparation des environnements de développement, de tests et de production	
Objectif	Dans le cadre de la mise en œuvre de nouvelles applications logicielles ou dans le cadre de modifications de logiciels existants, l'OSE sépare les environnements de développements, de tests, de production et les sécurise.	
Contrôle	Assurer la séparation de l'environnement de test, du développement et de la production	
Sous-contrôles	P4.4.1	Disposer des contrôles documentés du mouvement des données
		Définir les règles de transferts des logiciels du niveau de développement à celui de production.
	P4.4.2	Test des systèmes avant l'environnement de production
		Tests obligatoires des modifications des systèmes logiciels en production dans un environnement de tests séparé, avant leur mise en œuvre, avec documentation des mesures de sécurité complémentaires. Toute impossibilité technique ou organisationnelle à cet égard doit être documentée.
	P4.4.3	Accès du personnel pour tester l'environnement
		L'accès du personnel de développement et de tests à l'environnement de production est documenté, limité au minimum nécessaire et contrôlé.
	P4.4.4	Utilisation minimale des données en direct
		Dans les environnements de tests et de développement, les données réelles provenant de l'environnement de production (par exemple, les copies) doivent être limitées au minimum nécessaire.
	P4.4.5	Protection des données sensibles dans l'environnement de test
		Si des informations relatives à la sécurité de l'infrastructure essentielle sont disponibles dans les environnements de tests et de développement (par exemple données d'accès, détails de la

		configuration de sécurité), elles doivent être sécurisées de la même manière que dans l'environnement de production.
	P4.4.6	Suppression des données de test
		Si les environnements de tests et de développement ne sont pas (ou plus) utilisés, les données qui y sont recueillies doivent être supprimées en toute sécurité. Ce processus doit être documenté.
	P4.4.7	Protection des nouveaux logiciels
		Les procédures de mise en œuvre de nouvelles applications logicielles, de modifications des applications logicielles existantes au sein des IE doivent être décrites dans le PSO.
	P4.4.8	Cloisonnement
		Le réseau OSE sera logiquement et si possible physiquement séparé entre différentes fonctions telles que DNS et courrier, systèmes externes et internes ainsi que des tiers. Le trafic réseau sera contrôlé par des systèmes tels que des pares-feux et ne sera autorisé que lorsque les exigences de l'entreprise le justifient avec les autorisations appropriées. Le trafic autorisé doit être surveillé, sécurisé et documenté, une documentation précise à ce sujet doit être maintenue et tenue à jour.

P5 – Sécurité des opérations

Il est important de maintenir des opérations sécurisées dans l'ensemble des OSE afin de s'assurer que les activités opérationnelles n'exposent pas l'OSE aux menaces liées à la cybersécurité. Le domaine fournit des exigences pour la mise en œuvre des contrôles de sécurité, y compris les procédures connexes pour la conformité des OSE.

P5.1	**Procédures opérationnelles et responsabilités**	
Objectif	S'assurer que des procédures correctes sont en place et mises en œuvre	
Contrôle	Avoir des procédures opérationnelles documentées et mises en œuvre	
Sous-contrôles	P5.1.1	Procédures d'exploitation documentées
		Toutes les procédures opérationnelles doivent être documentées et mises en œuvre.
	P5.1.2	Gestion du changement
		Tous les changements doivent être documentés et contrôlés.
	P5	Gestion de la capacité
		Surveiller l'utilisation des ressources pour assurer une capacité adéquate pour l'avenir.

P5.2	Protection contre les logiciels malveillants	
Objectif	S'assurer que les informations et les installations de traitement de l'information sont protégées contre les logiciels malveillants	
Contrôle	Se protéger contre les logiciels malveillants	
Sous-contrôles	P5.2.1	Détecter et prévenir les logiciels malveillants
		Des contrôles de détection, de prévention et de récupération pour se protéger contre les logiciels malveillants doivent être mis en œuvre, combinés à une sensibilisation appropriée des utilisateurs.
	P5.2.2	Installation antivirus
		A propos des anti-virus : a. L'installation et l'assurance du bon fonctionnement et de la mise à jour systématique des anti-virus doit être assurée b. Les anti-virus vérifient, entre autres, avant le lancement d'un fichier, sa prévalence et sa signature numérique (par l'utilisation, par exemple, de logiciels antivirus basés sur l'heuristique et l'évaluation de la réputation).
	P5.2.3	Liste blanche des applications
		L'utilisation de logiciels de confiance, pour empêcher l'exécution de codes malveillants en bloquant les fichiers.exe, les DLL, les scripts (par exemple Windows Script Host, PowerShell et HTA) et les installateurs. A cette fin, il est nécessaire, autant que possible, d'utiliser les listes blanches d'applications autorisées.
	P5.2.4	Protection des systèmes industriels
		Les systèmes pour lesquels il n'est pas possible de mettre en œuvre les améliorations de sécurité recommandées (par exemple les systèmes d'OT[1]), d'autres mesures de sauvegarde assurant un niveau de sécurité adéquat sont prévues et mises en œuvre. [1]*OT ou Operational Technology (Technologie Opérationnelle en francais) désigne un système informatique dédié à l'environnement des systèmes de contrôle industriels (surveillance et/ou contrôle direct d'équipements, de biens, de processus et d'évènements industriels). L'OT présente des différences technologiques et fonctionnelles avec les systèmes informatiques traditionnels.*
	P5.2.5	Sécurisation des macros
		La configuration du support des macros Microsoft Office, afin de bloquer les macros des documents téléchargés sur Internet et pour n'autoriser que les macros testés et approuvés, entre autres des macros signées numériquement à partir d'une source fiable. Pour les autres macros, ne permettre leur exécution que dans un "environnement sécurisé" avec des droits d'écriture limités.
	P5.2.6	Utilisation d'un certificat électronique de confiance
		Les applications qui nécessitent Java sont exécutées après avoir été ajoutées à la liste des applications sûres ou utilisant des certificats électroniques fiables.

P5.3	Contrôle des logiciels opérationnels	
Objectif	Assurer l'intégrité des systèmes opérationnels.	
Contrôle	Avoir des procédures documentées d'installation de logiciels sur le système opérationnel	
Sous-contrôles	P5.3.1	Installation de logiciels sur les systèmes opérationnels
		Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciels sur les systèmes opérationnels.
	P5.3.2	Installation de la dernière version
		L'OSE installe les dernières versions du logiciel et du matériel, sauf si des exceptions sont obtenues et autorisées à installer une version inférieure à la version la plus récente. L'OSE applique les conditions suivantes : a. Préalablement à l'installation de toute nouvelle version, l'OSE : - S'assure de l'origine de cette version et de son intégrité ; - Analyse son impact technique et opérationnel sur l'IE. b. Dès qu'il a connaissance d'une nouvelle version ou d'une mesure correctrice de sécurité concernant une de ses ressources, et sauf en cas de difficultés techniques ou opérationnelles justifiées, l'OSE en planifie l'installation après avoir effectué les vérifications mentionnées précédemment, et procède à cette installation dans les délais prévus par la procédure de surveillance et de mise à jour des conditions de sécurité des IE. c. Les systèmes d'exploitation ainsi que les équipements réseaux de l'OSE sont utilisés dans leur version légale actuelle et sont tenus à jour. d. Les versions de ressources matérielles ou logicielles non supportées ne sont pas utilisées, sauf par décision de l'OSE, lorsque des raisons techniques ou opérationnelles justifient, pour certaines ressources de ses IE, de ne pas installer la dernière version et/ou une version supportée par le fournisseur, l'éditeur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'OSE met en œuvre des mesures techniques ou organisationnelles prévues par la procédure de surveillance et de mise à jour des conditions de sécurité des IE pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues.

P5.4	Configuration	
Objectif	Garantir des configurations sécurisées de tous les systèmes OSE	
Contrôle	Avoir des pratiques de configuration sécurisées	
Sous-contrôles	P5.4.1	Installations restreintes
		L'OSE installe sur ses IE les seuls services et fonctionnalités qui sont indispensables à leur fonctionnement ou à leur sécurité. Il désactive les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, et les désinstalle si cela est possible. Lorsque la désinstallation n'est pas possible, l'OSE le mentionne dans le PSO en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre.
	P5.4.2	Contrôle des logiciels utilitaires
		Entre autres, l'OSE limite et supervise l'utilisation de logiciels utilitaires de contournement de la sécurité des systèmes et des applications. Les logiciels utilitaires peuvent être des programmes pour, par exemple, l'optimisation des systèmes, la virtualisation, ainsi que des interprètes de commandes tels que Windows PowerShell. Les logiciels utilitaires utilisés sont enregistrés ou soumis à des procédures d'identification, d'authentification et d'autorisation, et il est mis en œuvre une séparation de ces utilitaires des applications. L'OSE crée, maintient et surveille une liste de logiciels utilitaires approuvés, et supprime ou bloque l'utilisation de tous les programmes utilitaires inutiles.
	P5.4.3	Utilisation des supports amovibles
		L'OSE ne connecte à ses IE que des équipements, matériels périphériques et supports amovibles dont il assure la gestion et qui sont indispensables au fonctionnement ou à la sécurité de ses IE. Tout autre utilisation de support amovible est interdite.
	P5.4.4	Rechercher les logiciels malveillants avant d'utiliser le support amovible
		L'OSE procède, avant chaque utilisation de supports amovibles, à l'analyse de leur contenu, notamment à la recherche de codes malveillants. L'OSE met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques d'exécution de codes malveillants provenant de ces supports.
	P5.4.5	Protection des appareils informatiques fonctionnant hors site
		L'OSE dispose de procédures et de mécanismes pour protéger ses propres appareils ou équipements mobiles hors sites. Les procédures doivent comprendre au moins : a) Des exigences relatives à la protection physique des équipements ; b) Des limitations d'installation de logiciels ; c) Des règles de protection contre les accès non autorisés ; d) Des règles d'utilisation des services et applications Internet ; e) Des règles de conduite en cas de perte ou de détérioration d'un appareil.
	P5.4.6	Protection de l'information dans les médias sortant de l'OSE

		L'OSE dispose de procédures pour le traitement des équipements de téléinformatiques retirés de l'exploitation courante. Notamment, les supports devant définitivement sortir de l'OSE (par exemple par la vente, le transfert ou après utilisation) doivent être illisibles, par écrasement des données, destruction des supports, ou toutes autres actions adéquates.
	P5.4.7	Mettre en place une procédure pour bloquer les médias non autorisés
		Les procédures doivent inclure le blocage des supports CD/DVD/USB non approuvés et le blocage des connexions aux téléphones, tablettes et appareils Bluetooth/Wi-Fi/3G/4G/5G non approuvés.
	P5.4.8	Contrôle de l'installation du logiciel en production
		L'OSE élabore, met en œuvre et décrit dans son PSO les procédures d'installation et de supervision des logiciels en environnement de production, qui doivent comprendre au moins : a) Les règles de mise à jour des logiciels en production, des applications et des bibliothèques ; b) Les règles d'admission des seuls codes exécutables acceptés et testés dans les systèmes en production (ne pas admettre les codes en compilation ou les codes en cours de développement) ; c) Les règles de restauration d'une version antérieure du système, y compris les comportements des versions antérieures des logiciels.

P5.5	**Identité numérique**	
Objectif	Protéger l'identité numérique de l'OSE	
Control	Mettre en place des certificats numériques de confiance	
Sub-Controls	P5.5.1	Mise en œuvre du certificat numérique approuvé
		Afin de garantir l'identité numérique de l'OSE, la fiabilité des services proposés et la confidentialité et l'intégrité des transactions, tous les sites web ou applications essentielles mis à dispositions des utilisateurs par l'OSE doivent être protégés par un certificat électronique émis par une autorité de certification approuvée par l'entité togolaise compétente.

P6 – Sécurité environnementale et physique

Protéger les actifs de l'environnement contre l'accès non autorisé et l'utilisation abusive des installations physiques abritant et traitant l'infrastructure numérique.

P6.1	**Accès physique**	
Objectif	Empêcher l'accès physique non autorisé, les dommages et les interférences aux installations de traitement de l'information de l'OSE.	
Contrôle	Mettre en place des contrôles physiques pour empêcher l'accès non autorisé aux locaux d'OSE, en particulier si ces lieux stockent et traitent des informations sensibles.	

Sous-contrôles	P6.1.1	Périmètre de sécurité physique
		Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones qui contiennent des informations sensibles ou critiques et les installations de traitement de l'information.
	P6.1.2	Contrôles d'entrée physiques
		Les zones sécurisées doivent être protégées par des contrôles d'entrée appropriés pour s'assurer que seul le personnel autorisé est autorisé à y accéder.
	P6.1.3	Sécurisation des bureaux, des chambres et des installations
		La sécurité physique des bureaux, des locaux et des installations doit être conçue et appliquée.
	P6.1.4	Protection contre les menaces extérieures et environnementales
		Une protection physique contre les catastrophes naturelles, les attaques malveillantes ou les accidents doit être conçue et appliquée.
	P6.1.5	Travailler dans des zones sécurisées
		Les procédures de travail dans des zones sécurisées doivent être conçues et appliquées.
	P6.1.6	Zone de livraison et de chargement
		Les points d'accès tels que les zones de livraison et de chargement et les autres points où des personnes non autorisées pourraient entrer dans les locaux doivent être contrôlés et, si possible, isolés des installations de traitement de l'information afin d'éviter tout accès non autorisé.

P6.2	**Équipements**	
Objectif	Prévenir la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des opérations de l'OSE	
Contrôle	Mettre en place des processus et des mécanismes pour protéger les équipements en tout temps.	
Sous-contrôles	P6.2.1	Emplacement et protection de l'équipement
		L'équipement doit être placé et protégé de manière à réduire les risques liés aux menaces et aux dangers environnementaux ainsi que les possibilités d'accès non autorisé.
	P6.2.2	Protection contre les pannes électriques
		L'équipement doit être protégé contre les pannes de courant et autres perturbations causées par des défaillances électriques.
	P6.2.3	Sécurité du câblage
		Les câbles d'alimentation et de télécommunications transportant des données ou soutenant des services d'information sont protégés contre l'interception, les interférences ou les dommages.
	P6.2.4	Entretien de l'équipement
		L'équipement doit être correctement entretenu pour assurer sa disponibilité et son intégrité continues.
	P6.2.5	Décommissionnement des actifs
		L'équipement, l'information ou le logiciel ne doivent pas être retirés du site sans autorisation préalable.
	P6.2.6	Sécurité de l'équipement et des biens hors site

		La sécurité doit être appliquée aux biens hors site en tenant compte des différents risques liés au travail à l'extérieur des locaux de l'OSE.
	P6.2.7	Élimination ou réutilisation sécuritaires de l'équipement
		Tous les équipements contenant des supports de stockage doivent être vérifiés pour s'assurer que toutes les données sensibles et les logiciels sous licence ont été supprimés ou écrasés en toute sécurité avant d'être éliminés ou réutilisés.
	P6.2.8	Équipement utilisateur sans surveillance
		Les utilisateurs doivent s'assurer que les équipements sans surveillance bénéficient d'une protection appropriée.
	P6.2.9	Nettoyer les bureaux et les écrans
		Une politique de bureau propre limitant les papiers et les supports de stockage amovibles et une politique d'écran propre doivent être adoptées.

D1 – Gestion des incidents de sécurité

La défense des réseaux et systèmes d'information consiste en une veille active de la sécurité informatique des Opérateurs de Services Essentiels et de leurs Infrastructures Essentielles. Pour la défense de ses réseaux et systèmes d'information, l'OSE élabore et met en œuvre un service spécialisé de surveillance, de détection, d'analyse et de qualification des évènements de sécurité, appelé service de Security Operations Center (SOC).

D1.1	**Journalisation et surveillance**	
Objectif	Enregistrer les événements et générer des preuves	
Contrôle	Consigner et surveiller les événements de sécurité	
Sous-contrôles	D1.1.1	Journalisation des événements
		Des journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défauts et les événements de sécurité de l'information doivent être produits, conservés et régulièrement examinés.
	D1.1.2	Protection des informations de journal
		Les activités de l'administrateur de réseau et du gestionnaire de réseau sont consignées et les journaux protégés et régulièrement révisés.
	D1.1.3	Synchronisation de l'horloge
		Les horloges de tous les systèmes de traitement de l'information pertinents au sein d'un OSE ou d'un domaine de sécurité doivent être synchronisées avec une source de temps de référence unique.

D1.2	**Surveillance de la sécurité**	
Objectif	Gérer les incidents de cybersécurité	
Contrôle	Assurer une approche cohérente et efficace de la gestion des incidents de sécurité	
Sous-contrôles	D1.2.1	Responsabilités et procédures
		Les responsabilités et les procédures de gestion doivent être établies pour assurer une réponse rapide, efficace et ordonnée aux incidents de sécurité de l'information.
	D1.2.2	Signalement des événements de cybersécurité
		Les événements liés à la sécurité de l'information doivent être signalés le plus rapidement possible par les canaux de gestion appropriés.
	D1.2.3	Signaler les faiblesses en matière de cybersécurité
		Les employés et les sous-traitants qui utilisent les systèmes et services d'information de l'OSE sont tenus de noter et de signaler toute faiblesse observée ou soupçonnée en matière de sécurité de l'information dans les systèmes ou les services.
	D1.2.4	Évaluation et décision sur les événements de sécurité de l'information

		Les événements liés à la sécurité de l'information sont évalués et il est décidé s'ils doivent être classés comme incidents de sécurité de l'information.
	D1.2.5	Réponse aux incidents de cybersécurité
		Les incidents de sécurité de l'information doivent être traités conformément aux procédures documentées.
	D1.2.6	Apprendre des incidents de cybersécurité
		Les connaissances acquises grâce à l'analyse et à la résolution des incidents de sécurité de l'information doivent être utilisées pour réduire la probabilité ou l'impact d'incidents futurs.
	D1.2.7	Collecte de preuves
		L'organisme doit définir et appliquer des procédures pour l'identification, la collecte, l'acquisition et la conservation de renseignements qui peuvent servir de preuve.

D1.3	**Surveillance des incidents de cybersécurité**	
Objectif	Surveiller les incidents de cybersécurité 24 heures sur 24, 7 jours sur 7	
Contrôle	Mettre en place des fonctions et des outils appropriés pour la surveillance des événements de sécurité en permanence	
Sous-contrôles	D1.3.1	Avoir un système de détection des incidents de sécurité
		L'OSE met en œuvre les dispositifs de détection capables d'identifier des événements caractéristiques d'un incident de sécurité notamment d'une attaque en cours ou à venir et de permettre la recherche de traces d'incidents antérieurs. A cet effet, ces dispositifs : a. Collectent les données pertinentes sur le fonctionnement de chaque IE (notamment les données « réseau » et les données « système ») à partir de capteurs positionnés de manière à identifier les événements de sécurité liés à l'ensemble des flux de données échangés entre les IE et les systèmes d'information tiers à ceux de l'OSE. b. Analysent les données issues des capteurs notamment en recherchant des indicateurs de compromission, dans le but d'identifier les événements de sécurité et de les caractériser. c. Archivent les métadonnées des événements identifiés afin de permettre une recherche a posteriori de marqueurs techniques d'attaques ou de compromission sur une durée d'au moins six (6) mois. L'OSE veille en particulier à ce que l'installation et l'exploitation des dispositifs de détection n'affectent pas la sécurité et le fonctionnement de ses IE.
	D1.3.2	Journalisation des événements
		L'OSE met en œuvre pour chaque Infrastructure Essentielle un système de journalisation, de corrélation et d'analyse, opérationnel 24h/24 et 7j/7 tous les jours de l'année, dédié exclusivement à des fins de détection d'évènements de sécurité, qui enregistre les

		événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité de l'IE ainsi qu'au fonctionnement de l'IE.
	D1.3.3	Systèmes pour générer des journaux
		Le système de journalisation porte sur les équipements suivants lorsqu'ils génèrent les événements mentionnés précédemment : a. Les serveurs applicatifs des IE ; b. Les serveurs d'infrastructure système ; c. Les serveurs d'infrastructure réseau ; d. Les équipements de sécurité ; e. Les postes d'ingénierie et de maintenance des systèmes industriels ; f. Les équipements réseau ; g. Les postes d'administration ; h. Les postes utilisateurs (dans la mesure du possible).
	D1.3.4	Contenu des journaux d'événements
		Le journal des événements doit contenir au minimum des informations sur : a. L'identifiant de chaque utilisateur ; b. La date, l'heure et les détails des événements importants, tels que le début et la fin du travail dans le système, y compris les tentatives de connexion infructueuses ; c. Les modifications de la configuration du système ; d. L'utilisation de privilèges ; e. Les modifications de privilèges ; f. L'utilisation d'utilitaires et d'applications système sélectionnés ; g. Les adresses réseau ; h. Les alarmes déclenchées par le système de contrôle d'accès ; i. L'activation et la désactivation des systèmes de protection tels que les logiciels antivirus.
	D1.3.5	Protection de l'intégrité des journaux
		Aucun droit de suppression ou de désactivation des journaux contenant des enregistrements de leurs propres actions ne doit être attribué aux administrateurs de systèmes informatiques. Concernant les systèmes pour lesquels ce n'est pas possible, un mécanisme de copie vers un dépôt externe doit être mis en place.
	D1.3.6	Horodatage des journaux d'événements
		Les événements enregistrés par le système de journalisation sont horodatés. Ils sont centralisés et archivés pendant une durée d'au moins six (6) mois. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.
	D1.3.7	Maintenir à jour l'état de surveillance
		L'OSE élabore et met en œuvre une procédure de veille, de surveillance, d'obtention et de mise en œuvre des informations les plus récentes concernant, les vulnérabilités, les menaces techniques et les mesures correctrices de sécurité concernant les ressources matérielles et logicielles utilisées pour les Infrastructures Essentielles.

D1.4	Gestion des vulnérabilités techniques	
Objectif	Prévenir l'exploitation des vulnérabilités techniques	
Contrôle	Identifier et gérer les vulnérabilités	
Sous-contrôles	D1.4.1	Gestion des vulnérabilités techniques
		Les informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues en temps utile. L'exposition de l'OSE à ces vulnérabilités est évaluée et les mesures appropriées prises pour faire face au risque associé des vulnérabilités sont identifiées.
	D1.4.2	Restrictions sur l'installation du logiciel
		Les règles régissant l'installation des logiciels par les utilisateurs sont établies et mises en œuvre.
	D1.4.3	Notation des vulnérabilités
		Les vulnérabilités identifiées sont notées sur la base de normes de notation communes de l'industrie. L'OSE élabore un plan d'action de remédiation fondé sur la notation de la vulnérabilité.
	D1.4.4	Vulnérabilités liées à Internet
		L'OSE identifie régulièrement toutes les vulnérabilités liées à l'internet au moins une fois par mois et corrige les vulnérabilités identifiées dans les deux semaines suivant leur identification.

R1 – Gestion de la continuité des activités

Ce domaine identifie les exigences pour les OSE afin de construire et d'exploiter des services essentiels durables contre des événements désastreux imprévus tels que des incendies, des inondations, des troubles politiques, etc.

R1.1	Sauvegarde	
Objectif	Se protéger contre la perte de données	
Contrôle	Réaliser la sauvegarde des informations	
Sous-contrôles	R1.1.1	Test des sauvegardes
		Des copies de sauvegarde des informations, des logiciels et des images système doivent être prises et testées régulièrement conformément à une politique de sauvegarde convenue.

R1.2	Continuité des opérations commerciales	
Objectif	Construire des services résilients et s'assurer que les OSE peuvent supporter des événements désastreux susceptibles d'avoir un impact sur les services et les opérations essentiels	
Contrôle	Avoir des opérations essentielles résilientes en cas d'événement désastreux impardonnable	
Sous-contrôles	R1.2.1	Politique de gestion de la continuité des activités
		Maintenir une politique de gestion de la continuité des activités couvrant la continuité et la redondance des informations en fonction de leur niveau de criticité.
	R1.2.2	Plan de continuité des activités
		Mettre en place un plan de continuité des activités de l'OSE et qui décrit ce qu'il faut faire en cas d'événement désastreux imprévu.
	R1.2.3	BIA (Business Impact Assessment)
		Effectuer une évaluation de l'impact sur l'entreprise pour tous les processus opérationnels et systèmes d'information critiques.

R1.3	Aspect cybersécurité de la continuité des activités	
Objectif	Disposer de contrôles et de services de cybersécurité résilients pour les OSE	
Contrôle	Avoir des opérations de cybersécurité résilientes en cas d'événement désastreux critiques tels que la corruption des données, l'indisponibilité du système critique.	
Sous-contrôles	R1.3.1	Planification de la continuité de la cybersécurité
		L'OSE doit déterminer ses exigences en matière de sécurité de l'information et de continuité de la gestion de la sécurité de l'information dans des situations défavorables, par exemple lors d'une crise ou d'une catastrophe.
	R1.3.2	Mise en œuvre de la continuité de la cybersécurité
		L'OSE doit établir, documenter, mettre en œuvre et maintenir des processus, des procédures et des contrôles afin d'assurer le niveau

		requis de continuité pour la sécurité de l'information dans une situation défavorable.
	R1.3.3	Vérifier, examiner et évaluer la continuité de la sécurité de l'information
		L'organisme doit vérifier les contrôles de continuité de la sécurité de l'information établis et mis en œuvre à intervalles réguliers afin de s'assurer qu'ils sont valides et efficaces dans des situations défavorables.

R1.4	**Test de la capacité de continuité des activités**	
Objectif	Avoir un processus de tests réguliers pour assurer la préparation en cas de catastrophe	
Contrôle	Avoir des plans de tests et effectuer des tests réguliers	
Sous-contrôles	R1.4.1	Élaborer un plan d'essai
		Développer des plans de tests complets pour toutes les opérations critiques simulant divers scénarios de catastrophe, y compris, sans s'y limiter, les inondations, les cyberattaques, les ransomwares, les incendies, etc.
	R1.4.2	Effectuer des tests réguliers
		Les tests doivent être effectués régulièrement au moins deux fois par an avec une période de quatre à six mois entre chaque test.

R1.5	**Gestion de crise**	
Objectif	Mettre en place un processus de gestion de crise pour répondre efficacement à un événement indésirable	
Contrôle	Élaborer des plans et une structure de gestion de crise	
Sous-contrôles	R1.5.1	Élaborer un processus et une procédure de gestion de crise
		Les OSE doivent disposer d'un processus et d'une procédure de gestion de crise pour répondre à un événement indésirable.
	R1.5.2	Construire une structure de gestion de crise
		L'OSE doit avoir une structure de gestion de crise en place comprenant la haute direction et couvrant toutes les ressources requises.

R1.6	**Reprise après sinistre**	
Objectif	Mettre en place un processus pour se remettre efficacement d'un événement indésirable	
Contrôle	Construire des processus et des systèmes redondants pour assurer la continuité des services	
Sous-contrôles	R1.6.1	Disponibilité des installations redondantes critiques

		Les OSE auront tous les services critiques identifiés pour disposer d'une infrastructure redondante afin d'assurer une prise de contrôle en douceur en cas d'événements indésirables.
	R1.6.2	Processus et procédures de récupération documentés
		Les OSE doivent avoir des processus et des procédures de rétablissement documentés alignés sur la politique globale de gestion de la continuité des activités

6. Références

L'élaboration de ces règles est fondée sur les normes de l'industrie et les pratiques exemplaires communes en matière de protection nationale de la cybersécurité, qui sont, mais sans s'y limiter :

1. ISO 27001:2013 - Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
2. PCI DSS (normes de sécurité des données pour l'industrie des cartes de paiement)
3. NIST 800-53 Révision 5 « Contrôles de sécurité et de confidentialité pour les systèmes d'information fédéraux et les organisations »
4. The 18 CIS Critical Security Controls
5. SANS Critical Security Controls (SANs Top 20)

7. Facteurs clés de succès

La mise en œuvre des règles détaillées de cybersécurité mentionnées dans le présent document dans l'ensemble des quatorze domaines devrait être caractérisée par les résultats ci-dessous :

1. Réduction significative du nombre d'incidents de sécurité mesurés sur une période de temps dans l'ensemble de l'OSE
2. Augmentation du niveau de sensibilisation aux cybermenaces pour tous les employés de l'OSE, mesurée par la diminution du nombre d'incidents de sécurité liés aux employés ainsi que par les résultats de scénarios d'attaque simulés.
3. Mener une sensibilisation, une formation et une éducation appropriées concernant ces règles de cybersécurité et des formations facilitées par l'industrie sur la cybersécurité pour tout le personnel de l'OSE
4. Existence d'un soutien et d'une implication visibles de la part des membres supérieurs de la direction de l'OSE pour défendre le cours de cybersécurité à l'OSE
5. L'OSE participe et contribue à l'industrie, au secteur et au partage à l'échelle nationale des meilleures pratiques en matière d'assurance de l'information et des leçons apprises avec l'ANCy et tout autre organisme de réglementation applicable.
6. Un budget indicatif prévoit toutes les activités de cybersécurité sur une base annuelle afin d'assurer des améliorations continues et la conformité.
7. L'OSE a une bonne compréhension et appréciation de la façon de mettre en œuvre les règles de cybersécurité en plus de la façon dont l'efficacité sera mesurée par ANCY et de mener une auto-évaluation
8. L'OSE a une voie d'escalade claire sur les incidents de sécurité critiques et sait comment et où demander de l'aide ainsi que signaler de tels incidents aux régulateurs et aux autorités.
9. Avoir un PSO clair et régulièrement mise à jour avec une ventilation détaillée des mesures que l'OSE entreprendra pour répondre aux exigences de conformité
10. Avoir des rapports d'évaluation des risques à jour détaillant la méthodologie utilisée et les détails des risques identifiés et des plans d'assainissement documentés.