RÉPUBLIQUE TOGOLAISE

CYBER DEFENSE AFRICA

La Protection du Cyberespace Africain

Sommaire

- Nos valeurs
- Cyber menaces & cybersécurité
- CDA en bref
- Nos services

Nos valeurs

Excellence

1. **COMPETENCE – aptitude technique**
2. **ETHIQUE – rectitude morale**
3. **PATRIOTISME – dévouement pour son pays**
4. **PASSION – enthousiasme pour son travail**
5. **EFFICACITE – soin du résultat**
6. **EQUIPE – esprit de cohésion et de sacrifice**

Cyber menaces & Cybersécurité

6 types de cyber attaques

	HACTIVISME	CRIME	INTERNE	ESPIONNAGE	TERRORISME	CYBERGUERRE
Menaces						
Motivations	Les hacktivistes exploitent les réseaux informatique dans le but de militer pour une cause politique ou sociale (défiguration de sites Internet, déni de service, etc…)	Certains individus ou groupes organisés volent des informations personnelles des victimes pour en tirer un gain financier (rançongiciels, hameçonnage, vol de données personnelles)	Vol ou exfiltration de données par un personnel de confiance pour des raisons idéologiques, financières ou personnelles	Accès furtif à pendant le plus longtemps possible afin d'accéder à des données ou des renseignements précieux	Les cyber terroristes s'attaquent aux infrastructures critiques des pays cibles pour en perturber le fonctionnement et créer la panique	Le cyberespace est devenu un champ de bataille majeur entre les armées et autres organisations gouvernementales car la cyberguerre nécessite relativement peu de moyens financiers et humains

The Cyber Threat Spectrum (source: FBI Cyber Division)

Ne vous demandez pas si vous allez être attaqués ou pas… mais quand et comment!

Cybersécurité

→ Une stratégie face à la complexité évolutive des menaces

→ Un ensemble de lois, décrets, règlements…

- Loi sur la Cybersécurité et la Lutte contre la Cybercriminalité
- Décret portant attributions et organisation de l'ANCy, autres…

→ Un centre national spécialisé sur les questions cybersécurité – CERT

- Centralise les informations sur les risques et organise les réponses
- Participe à la sécurité intérieure du pays

→ Une protection des Opérateurs de Services Essentiels (publiques et privés) et de leurs Infrastructures Essentielles jugées vitales pour le pays

- Protection spécifique et ciblée sous la responsabilité du *Security Operations Center* (SOC)

CERT : Computer Emergency Response Team

CDA en bref

Cyber Defense Africa

Votre partenaire cybersécurité

S.A.S au capital de 1.965.000.000 F CFA entièrement libéré

Mandaté par la République Togolaise pour assurer la SSI au Togo

Une équipe hautement qualifiée (ISO 27001, CISSP, CEH, CyberOps,…)

Plusieurs années d’expérience dans la SSI

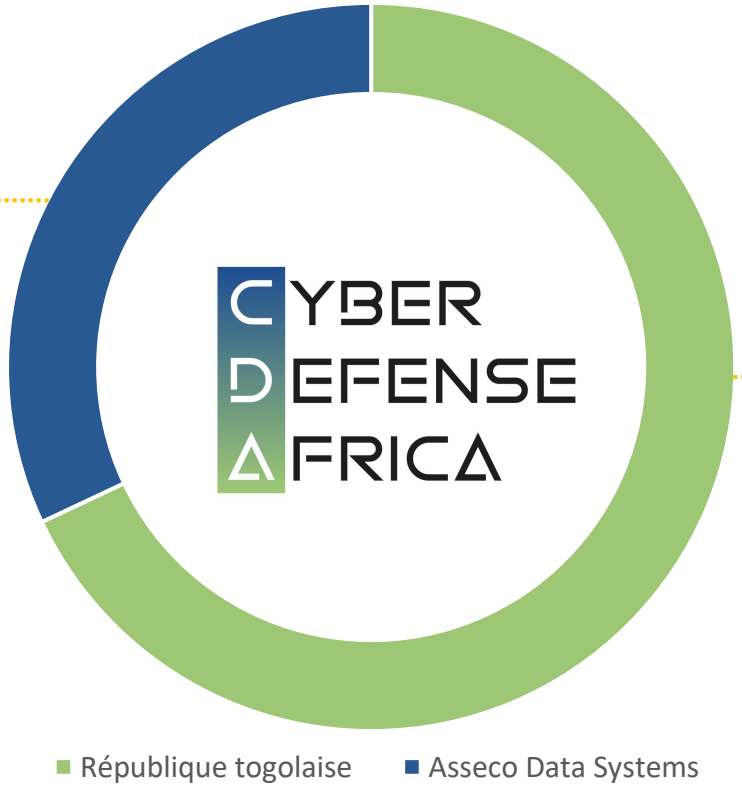
Cyber Defense Africa

Votre partenaire cybersécurité

Asseco Data Systems

- 1/3 du capital
- Leader Cybersécurité en Europe Centrale
- 29.000 Salariés
- 50 pays
- 3.2 Milliards EUR de CA
- Intégrateur systèmes
- *Vendor agnostic*
- Secteurs : Services Publics (Militaire, Civil), Secteur Financier, Telecoms, Utilities, Entreprises

Partenariat Public Privé

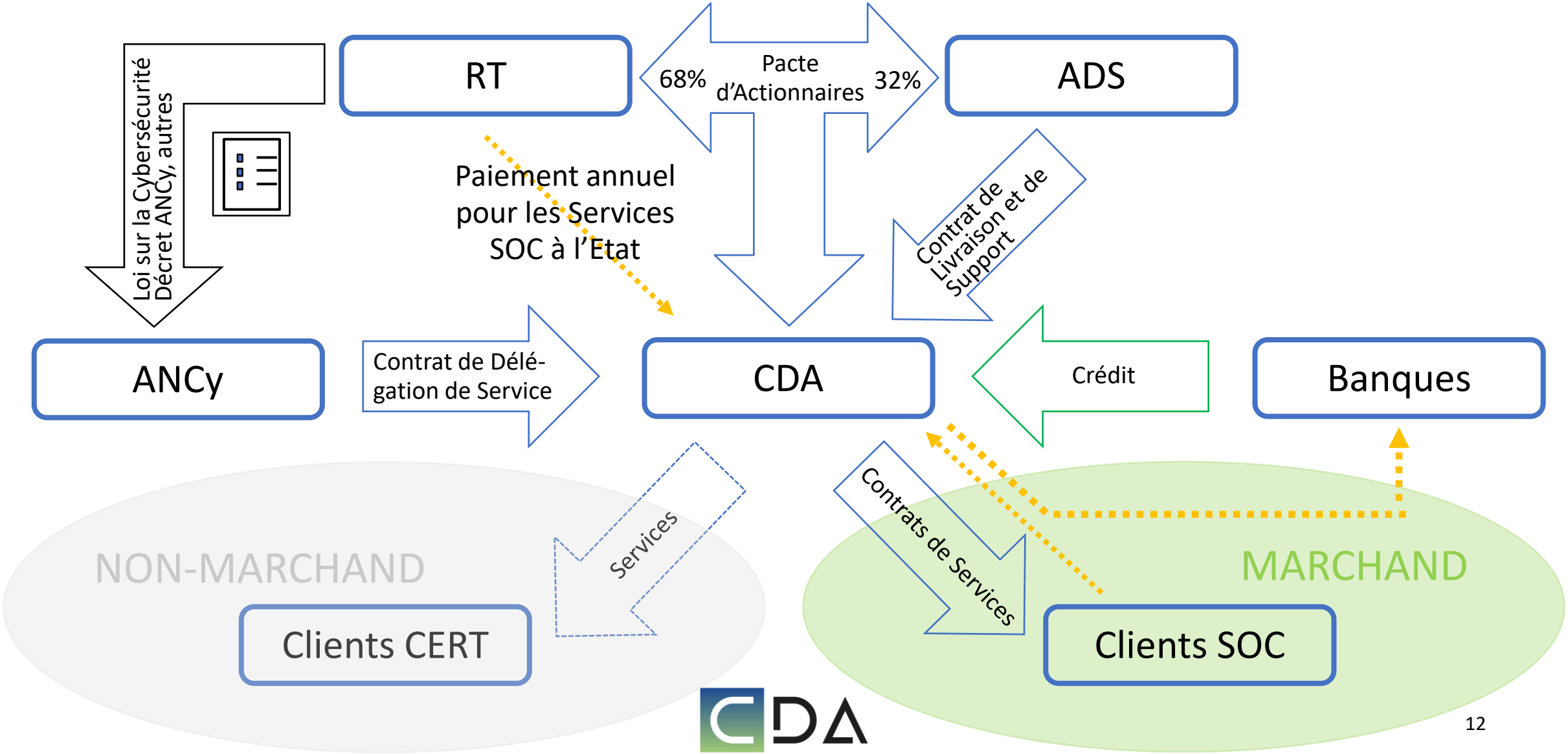


République togolaise

- 2/3 du capital
- Leader régional en cybersécurité
- Stabilité politique & sécuritaire
- Plan ambitieux de développement via le numérique & l'économie du savoir
- Mise en place du cadre légal & réglementaire

CDA

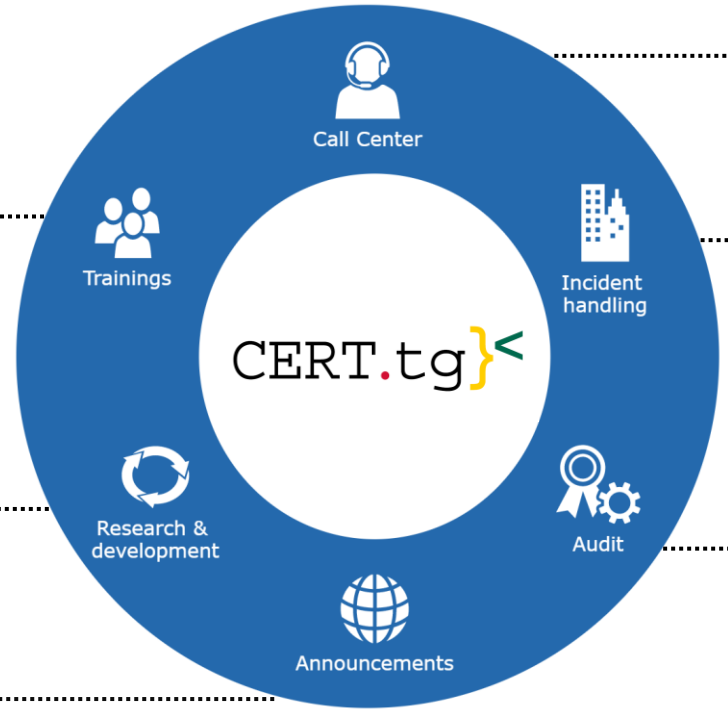
Lien ANCy - CDA



Nos services

Centre national de réponse aux incidents

Services CERT TOGO



Service de support en 24/7

Traitement, réponse et coordination de vos incidents de sécurité

Audits de Conformité des OSE
Audits Organisationnels

Annonce des intrusions et des vulnérabilités, bulletins de sécurité

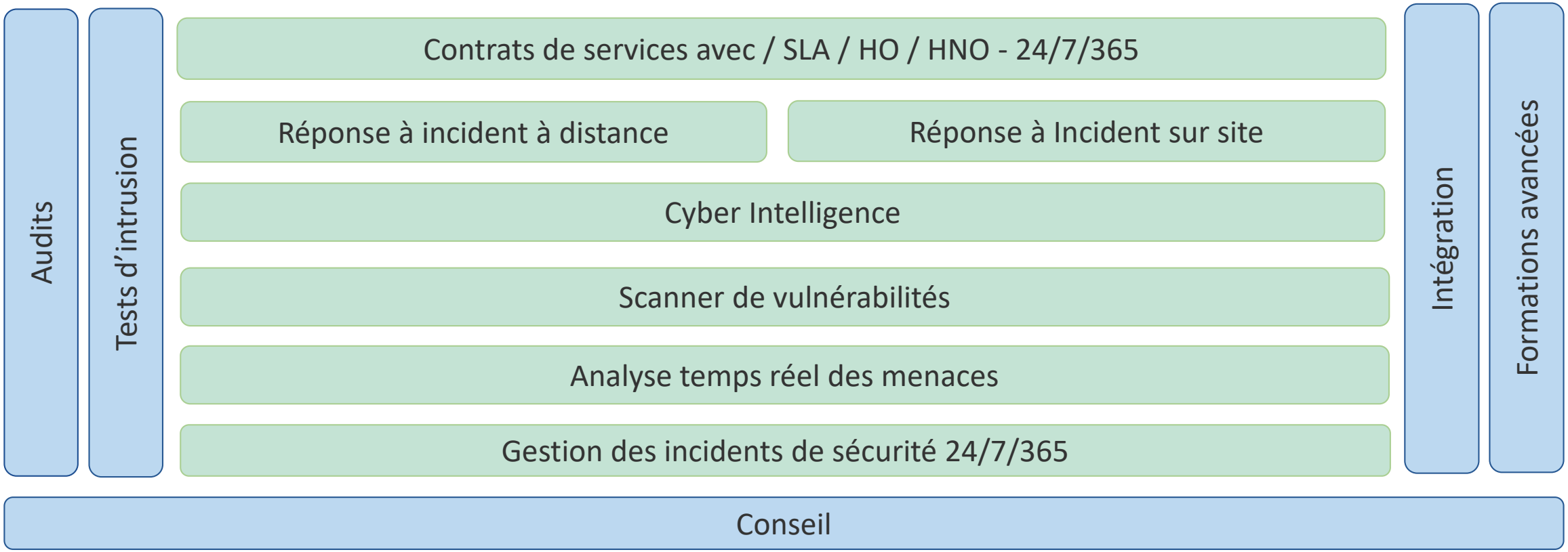
R&D sur les nouvelles techniques et les tendances du secteur

Sensibilisation pour les citoyens, écoles, universités, formations professionnelles

www.cert.tg

Centre national de défense en cybersécurité

Services SOC et prestations de services à la demande



SOC as a Service

Professional Services

www.cda.tg

MERCI

PRÉSENTATION DES RÈGLES DE CYBERSÉCURITÉ

Sommaire

- Définition – Mots clés
- Introduction
- Domaines et sous-domaines
- Contrôle et audit de conformité
- Facteurs clés de succès

Définitions – Mots-clés

- La loi sur la Cybersécurité : référence sur les définitions des termes et mots-clés
- Autres acronymes et termes du document
  - **Délégataire de l'ANCy** : contrat de délégation de service public entre CDA et l'ANCy
  - **CERT National** : Equipe nationale de gestion des incidents de cybersécurité fournissant des services de CERT (*Computer Emergency Response Team*)
  - **Personnel Essentiel** : Personnel de l'OSE interne ou externe 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 S.I des administrations ou des OSE et (ii) de tout matériel, logiciel ou S.I destiné à traiter des informations couvertes par le secret de la défense nationale.
  - **SOC :** désigne un Security Operation Center ou Centre opérationnel de sécurité

Références

- Normes de l'industrie et pratiques communes en matière de cybersécurité
  - ISO 27001:2013 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences
  - PCI DSS (normes de sécurité des données pour l'industrie des cartes de paiement)
  - NIST 800-53 Révision 5 « Contrôles de sécurité et de confidentialité pour les systèmes d'information fédéraux et les organisations »
  - Center for Internet Security(CIS) Critical Security Controls

Introduction

Introduction

- ANCy
  - Autorité nationale en matière de réglementation de la sécurité des SI
  - Aligner et diriger les efforts nationaux pour la cybersécurité
  - Combattre de façon systématique et coordonnée la cybercriminalité
  - Elaboration des règles et obligations des OSE
- Les règles de la Cybersécurité (Article 11 du décret OSE)
  - 4 domaines – **Gouvernance, protection, défense des réseaux et S.I. et résilience des activités**
  - 14 sous-domaines
  - 216 contrôles appropriés dans chacun des sous-domaines

Domaines et sous-domaines

Gouvernance de la sécurité des réseaux et systèmes d'information (G)

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.

Gouvernance de la sécurité des réseaux et systèmes d'information (G)

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..

Protection des réseaux et systèmes d'information (P) 1/2

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.

Protection des réseaux et systèmes d'information (P) 2/2

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.

Défense des réseaux et systèmes d'information (D)

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.

Résilience des activités (R)

R1	Gestion de la continuité des activités	Assure la résilience et la continuité des opérations face aux événements désastreux imprévus pour les OSE.

Contrôle de conformité de la sécurité IE

Contrôles - Gouvernance

G1 – Gouvernance, gestion et leadership	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
	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.
G2 – Politique de sécurité et plan de sécurité d'opérateur (PSO)	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

Contrôles - Gouvernance

G3 – Conformité, audit et performance	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
	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
	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
	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

Contrôles - Gouvernance

G4 – Gestion des risques de cybersécurité	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
	G4.2 Évaluation du risque	
	Objectif	Effectuer une évaluation régulière des risques conformément à la méthodologie approuvée
	Contrôle	Effectuer une évaluation régulière des risques
	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
	G4.4 Acceptation des risques	
	Objectif	Avoir un processus formel en place pour l'acceptation des risques
	Contrôle	Gérer les risques acceptés

Contrôles - Gouvernance

G5 – Ressources Humaines	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
	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
	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

Contrôles - Gouvernance

G6 – Relation fournisseur	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
	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
	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
	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

Contrôles - Protection

P1 – Contrôle d'accès	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
	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
	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
	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

Contrôles - Protection

P2 – Gestion des actifs	P2.1 Responsabilité des actifs	
	Objectif	Identifier les actifs de l'OSE et définir la protection et les responsabilités appropriées
	Contrôle	Gérer les actifs
	P2.2 Classification des actifs	
	Objectif	S'assurer que les actifs informationnels bénéficient d'un niveau de protection approprié
	Contrôle	Classifier les 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
	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
	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

Contrôles - Protection

P3 – Sécurité des communications	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.
	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
	P3.3 Filtrage réseau	
	Objectif	Filtrer le trafic réseau non autorisé et autoriser uniquement le trafic requis
	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
	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

Contrôles - Protection

P4 – Systèmes d'information, acquisition et maintenance	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
	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
	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
	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

Contrôles - Protection

P5 – Sécurité des opérations	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
	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
	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
	P5.4 Configuration	
	Objectif	Garantir des configurations sécurisées de tous les systèmes OSE
	Contrôle	Avoir des pratiques de configuration sécurisées
	P5.5 Identité numérique	
	Objectif	Protéger l'identité numérique de l'OSE
	Control	Mettre en place des certificats numériques de confiance

Contrôles - Protection

P6 – Sécurité environnementale et physique	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
	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

Contrôles - Défense

D1 – Gestion des incidents de sécurité	D1.1 Journalisation et surveillance	
	Objectif	Enregistrer les événements et générer des preuves
	Contrôle	Consigner et surveiller les événements de sécurité
	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
	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
	D1.4 Gestion des vulnérabilités techniques	
	Objectif	Prévenir l'exploitation des vulnérabilités techniques
	Contrôle	Identifier et gérer les vulnérabilités

Contrôles - Résilience

R1 – Gestion de la continuité des activités	R1.1 Sauvegarde	
	Objectif	Se protéger contre la perte de données
	Contrôle	Réaliser la sauvegarde des informations
	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
	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

Contrôles - Résilience

R1 – Gestion de la continuité des activités	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
	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
	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

Contrôle et Audit de conformité

- Contrôle annuel : CDA par contrat de délégation de service avec l'ANCy
  - Vérification de l'efficacité et de l'application des mesures de sécurité du Plan de Sécurité Opérateur
  - Rapport d'audit de conformité
    - Constatations sur les mesures appliquées
    - Respect du PSO et des règles de cybersécurité
    - Recommandations de remédiation
    - Confidentiel
  - Mise à jour du PSO avec redéfinition des objectifs, de la stratégie et des mesures mises en place

Facteurs clés de succès

Indicateur clés de performance

- Réduction significative du nombre d'incidents de sécurité mesurés sur une période de temps
- Augmentation du niveau de sensibilisation pour tous les employés de l'OSE
  - Nombre d'incidents de sécurité liés aux employés
  - Résultats de scénarios d'attaque simulée
- Sensibilisation, formation et éducation appropriées concernant ces règles de cybersécurité
- Soutien et implication visibles de la part de la direction de l'OSE pour augmenter la posture cybersécurité
- Participation et contribution à l'industrie et au partage à l'échelle nationale des meilleures pratiques et leçons apprises
- Budget indicatif annuel prévu pour les activités de cybersécurité
- Bonne compréhension et appréciation de la mise en œuvre des règles de cybersécurité et des critères d'évaluation
- Voie d'escalade claire sur les incidents de sécurité critiques
- Maîtrise du processus de demande d'assistance et de signalement d'incidents
- PSO clair et régulièrement mis à jour avec les mesures de mise en conformité
- Rapports d'évaluation des risques à jour et des plans documentés de gestion

Tableau d’évaluation du niveau de conformité

Domaine	Réf.	Sous-domaine	Réf.	Contrôle	Réf	Sous-contrôles	Conformité de l'OSE
Gouvernance (G)	G1	Gouvernance, gestion et leadership	G1.1	Faire preuve de leadership et d’engagement en matière de cybersécurité	G1.1.1	Conseil d’administration	Conforme
					G1.1.2	PDG/Directeur Général	Conforme
					G1.1.3	Comité de direction de la cybersécurité	Conforme
			G1.2	S’assurer que la visibilité de la cybersécurité et les relations pertinentes sont établies ou renforcées.	G1.2.1	Contact avec les autorités	Conforme
					G1.2.2	Dossier d’accréditation	Conforme
					G1.2.3	Contact avec les groupes d’intérêts spéciaux	Conforme
					G1.2.4	La cybersécurité dans la gestion de projet	Non Conforme
					G1.2.5	Séparation des tâches	Conforme
					G1.2.6	Rôles et responsabilités en matière de cybersécurité	Non Conforme

Tableau de bord du niveau de conformité

TABLEAU DE BORD DE CONTRÔLE DES REGLES DE CYBERSECURITE DE L'OSE

CDA

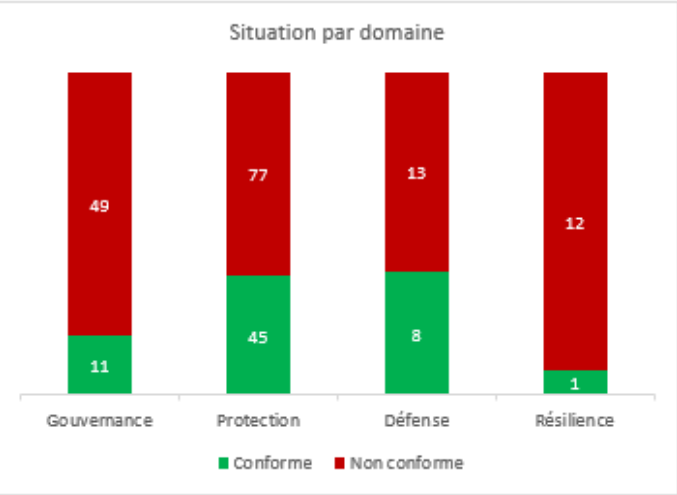
Nom de l'OSE :	OSE1
Numéro OSE :	N/A
Personne contact :	Nom RSSI
Période :	2022
Date :	22/09/2022

Evaluation finale

NON SATISFAISANT

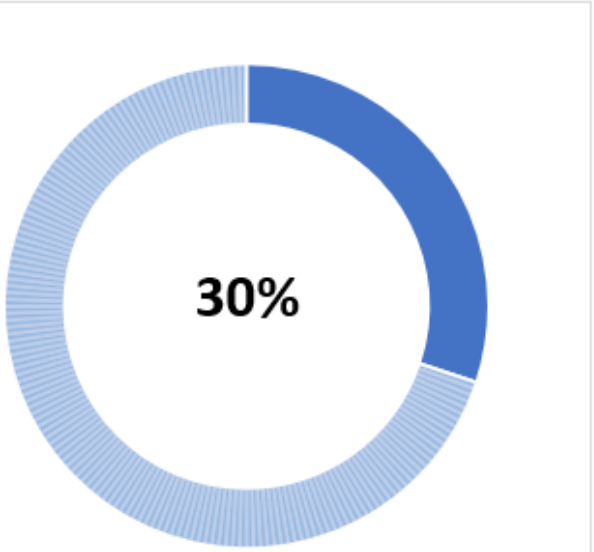
Conformité par domaine de règles de cybersécurité

Domaines	Conforme	Non Confome	Total
Gouvernance (G)	11	49	60
Protection (P)	45	77	122
Défense (D)	8	13	21
Résilience (R)	1	12	13
TOTAL	65	151	216

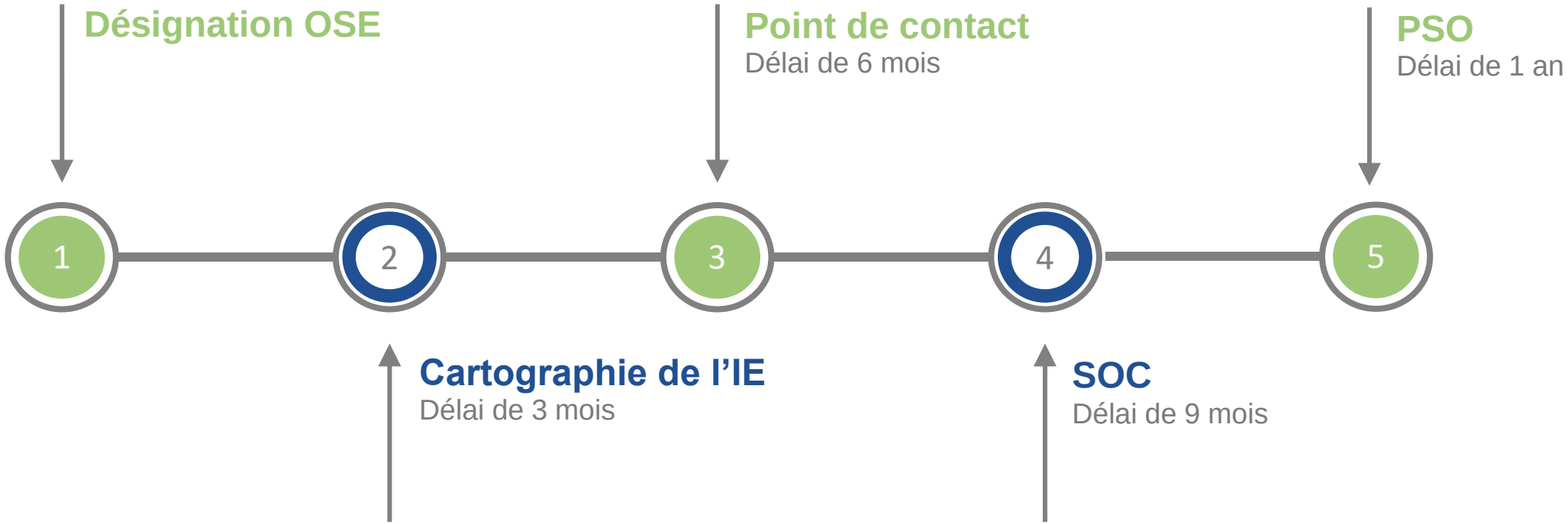


Pourcentage de conformité aux règles de cybersécurité

30% CONFORME
70% NON CONFORME



Etapes de mise en conformité



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

La Protection du Cyberespace Africain

cda.tg
twitter.com/CDA_tg
info@cda.tg
22 53 59 83

CYBER DEFENSE AFRICA

cert.tg
twitter.com/cert_tg
contact@cert.tg
22 53 59 83