REPUBLIQUE ISLAMIQUE DE MAURITANIE
Honneur – Fraternité – Justice

Ministère de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration

Programme des Nations Unies pour le Développement

ASSISTANCE À LA CRÉATION D'UNE AGENCE NATIONALE DE CYBERSÉCURITÉ ET DE CERTIFICATION

RAPPORT DÉFINITIF

SEPTEMBRE 2023

TABLE DE MATIERES

Liste des Acronymes I
I. Introduction 1
II. Contexte du développement du numérique en Mauritanie 2
2.1 Le Haut conseil du Numérique 4
2.2 L'Autorité de Protection des données à caractère personnel 4
2.3 L'Agence du Numérique de l'Etat 5
III. Analyse du contexte local afin de définir le positionnement de cette autorité ou agence et établir sa mission. 6
IV. Etude de benchmark des institutions similaires dans les pays de la sous-région. 8
4.1 Tunisie, ... 8
4.2 Sénégal 9
4.3 Maroc 10
4.4 France 10
4.5 Le Royaume de l'Arabie de Saoudite 10
4.6 Sultanat d'OMAN 11
4.7 Tableau récapitulatif 11
V. Analyse des principaux risques et facteurs de réussite 13
VI. Conception de l'Agence à travers la proposition de scénarios de mission, d'Ancrage institutionnels et d'organisation motivés par les résultats du benchmark international et la connaissance de bonnes pratiques dans le domaine 15
6.1 Objectifs et missions de l'agence 16
6.2 Ancrage institutionnel 17
6.3 Structure organisationnelle 19
VII. Analyse des investissements nécessaires à la création de l'Agence. 22
7.1 Installation de l'agence 22
7.2 MAURI-CERT 22
7.3 L'unité de gestion des certifications 24
7.4 Le Centre de Formation 25
7.5 Les ressources humaines 26
VIII. Elaboration du cadre juridique et des exigences réglementaires et organisationnelles nécessaires à la création de l'Agence 28
IX. Chronogramme de mise en place de l'agence 30
Annexes 31

Annexe 1: .....Projet de décret portant création, organisation et fonctionnement de l'Agence de Certification et de Cybersécurité de l'Etat « ACC-ETAT »..... 32

Liste des Acronymes

ACC-ETAT	Agence de Cybersécurité et de Certification de l'Etat
ANAPEJ	Agence Nationale de Promotion de l'Emploi des Jeunes
AN-ETAT	Agence Numérique de l'Etat
ANRPTS	Agence Nationale du Registre des Populations et des Titres Sécurisés
ANRSI	Agence Nationale de la Recherche Scientifique et de l'Innovation
ANSADE	Agence Nationale de la Statistique et de l'Analyse Démographique et Economique
ANSI	Agence Nationale de la Sécurité Informatique (Tunisie)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (France)
APD	Autorité de Protection des données à caractère personnel
APIM	Agence de promotion des investissements en Mauritanie
BCM	Banque Centrale de Mauritanie
CERT	Computer Emergency Response Team (Equipe d'intervention en cas d'urgence informatique)
CSIRT	Computer Security Incident Response Team
CTA-HCN	Comité Technique d'Appui au Haut Conseil du Numérique
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information (Maroc)
HCN	Haut Conseil du Numérique
MDEC	Ministère de l'Intérieur et de la Décentralisation
MDN	Ministère de la Défense Nationale
MEDD	Ministère de l'Economie et du Développement Durable
MTNIMA	Ministère de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration
OCWAR-C	West African Response on Cybersecurity and Fight against Cybercrime (Réponse de l'Afrique de l'Ouest sur la Cybersécurité et la lutte contre la Cybercriminalité)
ODD	Objectifs le développement durable
OIV	Opérateurs d'Importance Vitale
ONN	Observatoire national du Numérique
PKI	Infrastructure à Clé Publique

RIADE	Réseau des administrations publiques
SCAPP	Stratégie de Croissance Accélérée et de Prospérité Partagée
SIEM	Security Incident and Event Management
SNSN	Stratégie Nationale de Sécurité Numérique
SOC	Centre des Opérations de Sécurité (Security Operations Center)
TIC	Technologies de l'Information et de la Communication
WARCIP	West Africa Regional Communications Infrastructure Project
WARDIP	Projet Régional d'Intégration Numérique en Afrique de l'Ouest

I. Introduction

La croissance d'Internet a été le plus grand changement social et technologique de ces derniers temps ; elle a facilité le commerce et joue un rôle énorme dans le soutien du développement durable.

Conscient de cet enjeu, le Gouvernement Mauritanien, avec l'appui de ses partenaires au développement en particulier la Banque Mondiale et la Banque Européenne d'Investissement, a investi de manière significative dans l'infrastructure numérique et les applications des technologies de l'information et de la communication (TIC), en tant que pierre angulaire de la croissance économique nationale. Il compte ainsi faire de celles-ci un catalyseur clé de la croissance économique et de la mobilité sociale pour améliorer le niveau de vie des Mauritaniens dans le cadre de la Stratégie de Croissance et de Prospérité Partagée 2016-2030.

Cette volonté s'est traduite par l'élaboration d'un Agenda de Transformation Numérique 2022 2025 visant à «faire du Numérique et de l'Innovation un levier clé de Modernisation de l'Administration, d'Inclusion Sociale et de Renforcement de la Compétitivité »

La généralisation croissante de l'utilisation des technologies numériques, permettra la modernisation de l'Administration Publique et des services rendus aux citoyens, et une numérisation de l'économie, créant ainsi une dépendance croissante à l'égard du cyberespace engendrant des nouveaux risques et augmentant la vulnérabilité aux cybermenaces (la cybercriminalité, le cyberespionnage, le hacktivisme, le cyberterrorisme, la cyberguerre, etc.) de plus en plus nombreuses, sophistiquées et difficiles à atténuer.

Les institutions financières sont exposées aux cyberattaques pouvant entraîner des dommages, parfois à répétition. Il s'agit d'abord de fraudes sur les cartes bancaires ou de hameçonnage – une méthode qui consiste à pousser la personne à révéler ses informations personnelles, les atteintes au « core banking » : les infections virales et les intrusions dans les systèmes d'information. Les banques peuvent aussi être touchées par des fuites d'informations, des usurpations d'identité, des fraudes par transfert d'argent ou des retraits sur des faux chèques.

Face à ces cybermenaces croissantes, des politiques sont mises en place par les états pour l'amélioration de la cybersécurité des particuliers, des entreprises, et des infrastructures nationales essentielles.

Pour cela, le Gouvernement se doit de créer et maintenir un environnement qui assurera la confiance lors de l'utilisation des installations TIC et garantira que la Mauritanie soit capable de protéger ses intérêts de manière autonome et de faire respecter la sécurité nationale. Cet environnement garantira la confidentialité et l'intégrité des actifs informationnels et des informations sensibles du gouvernement, des entreprises et des particuliers.

A cette fin, la Mauritanie a élaboré et adopté avec l'appui de OCWAR-C «West African Response on Cybersecurity and Fight against Cybercrime» (Réponse de l'Afrique de l'Ouest sur la Cybersécurité et la lutte contre la Cybercriminalité), une stratégie nationale de sécurité numérique 2022-2025, dont l'objectif est de «renforcer la sécurité et la résilience de son

cyberespace, ainsi que de lutter contre les atteintes aux systèmes numériques du pays et les utilisations malveillantes du cyberespace».

Pour assurer la cohérence des activités et optimiser les ressources nationales, tant en matière d'infrastructures, de ressources financières et de compétences humaines, il est proposé de confier le pilotage de la politique nationale et la mise en œuvre de la stratégie nationale de sécurité numérique à Autorité nationale de cybersécurité.

Le Programme des Nations Unies pour le Développement, a décidé d'accompagner le MTNIMA, dans l'analyse des conditions de mise en place d'une telle autorité en :

- définir le schéma institutionnelle de l'Agence Nationale du Numérique, sa mission et son organisation ;
- établir l'ensemble des documents juridiques, administratifs et organisationnels nécessaires à sa création et à son bon fonctionnement ;
- accompagner le Gouvernement pour la traduction en arabe des textes préparés et pour leur approbation.

II. Contexte du développement du numérique en Mauritanie

Le cadre de référence de la planification stratégique du développement économique, social et environnement à l'horizon 2030 de la Mauritanie est défini par la Stratégie de Croissance Accélérée et de Prospérité Partagée (SCAPP), qui intègre également l'Agenda 2030 des nations unies pour le développement durable (ODD). Sa mise en œuvre se fait par des plans d'action quinquennaux, dont le second a été élaboré en en 2021 pour couvrir la période 2021-2025. Trois leviers convergents constituent les objectifs stratégiques retenus pour assurer la croissance projetée, à même de réaliser une prospérité profitable à tous. Ainsi au sein du levier 1, «promotion d'une croissance forte, durable et inclusive», les infrastructures liées aux nouvelles technologies jouent un rôle important dans le soutien à la croissance économique. Dans le domaine des nouvelles technologies, les objectifs fixés sont :

- la mise en place un système national d'innovation à même de libérer les esprits et initiatives d'innovation en faveur du développement inclusif ;
- le développement d'infrastructures de télécommunication et de technologie de l'information ;
- la mise à niveau les bases réglementaires et institutionnelles de «la Société Mauritanienne de l'Information » et du « secteur des télécoms ».

Dans le cadre du premier Plan d'action de la SCAPP, la Mauritanie a entrepris la mise en place la connectivité internationale par câble sous-marin, la construction de tronçons de dorsales internet en fibre optique et le lancement de la 4G sur le territoire national. Ces chantiers ont permis une amélioration considérable de la connectivité des mauritaniens. Cette amélioration se matérialise par un taux de couverture en réseau mobile (toutes technologies confondues) de 95% et un taux de couverture en 4G de 31% (en 2019), bien que de nombreuses communes soient uniquement couvertes en réseau 2G, et certaines se situent encore en zone blanche. Par

ailleurs, 20% du trafic international de la Mauritanie en 2021 est destiné aux pays voisins[1]. Cependant, le secteur des TICs connait des contraintes conséquentes relatives à la cyber sécurité qui mettent en danger le progrès réalisé mais aussi des contraintes par rapport au taux élevé d'analphabétisme digital qui impactent négativement le rendement des actions mises en œuvre pour promouvoir et développer le secteur.

De ce contexte, découlent des enjeux capitaux liés aux nouvelles technologies qui se matérialisent par l'accroissement de la sensibilisation de la population vis-à-vis des TICs afin de maximiser les résultats des différentes actions entreprises et de développer une économie numérique qui contribue au développement socio-économique du pays. L'intégration des nouvelles technologies à l'administration publique constitue, elle aussi, un enjeu primordial pour le secteur dans le cadre de la décentralisation de l'administration et l'accroissement de la connectivité régionale et nationale.

Pour conduire à l'émergence d'un secteur des TIC encourageant l'innovation, favorisant la croissance et l'accès à l'information, et s'inscrivant dans le cadre de la Transformation numérique en Mauritanie, le Gouvernement a adopté un Agenda de Transition Numérique pour la période 2022 2025 dont la vision est de « Faire du Numérique et de l'Innovation un levier clé de Modernisation de l'Administration, d'Inclusion Sociale et de Renforcement de la Compétitivité ». Il se fixe comme objectifs de doubler l'usage de l'internet et la taille du secteur numérique, de tripler le nombre d'emploi et l'usage du paiement mobile, et devenir le 1er pays numérique de la région du Sahel.

Cet agenda a défini 3 leviers de mise en œuvre pour atteindre cet objectif :

- ✓ « Gouvernance et Cadre réglementaire & juridique »
- ✓ « Compétences Numériques »
- ✓ « Culture & Confiance Numérique »

Dans le cadre de la mise en œuvre du premier levier, et pour soutenir et porter le développement du secteur du numérique sur la période 2022 2025, un Haut Conseil du Numérique (HCN) a été mis en place pour suivre l'exécution de l'Agenda numérique 2022 2025, ainsi qu'une Agence Numérique de l'Etat (AN ETAT), et une Autorité de Protection des données à caractère personnel (APD). Il est prévu également la mise en place d'un Observatoire national du Numérique (ONN) et une Agence Nationale de la Cybersécurité et de Certification électronique (ANCC).

La mise en œuvre du 3ème levier de cet Agenda vise l'instauration de la confiance numérique par une garantie d'un haut niveau de confiance régissant les transactions dans l'espace cybernétique afin de permettre aux usagers, citoyens et entreprises, de bénéficier des services en ligne et d'accepter le partage à distance de leurs données. A cet effet, le gouvernement s'est doté d'une stratégie nationale de sécurité numérique et d'un cadre juridique permettant de lutter contre la cybercriminalité et aussi de protéger les données à caractère personnel. Parmi, les actions prévues pour l'opérationnalisation de cette stratégie figurent la mise en place d'un

[1] Source : MTNIMA, Agenda National de Transformation Numérique

CERT Computer Emergency Response Team, l'opérationnalisation d'un SOC et la mise en place d'une infrastructure publique (PKI)

2.1 LE HAUT CONSEIL DU NUMERIQUE

Le Haut Conseil du Numérique (HCN) a été créé le 26 mars 2020 par le Décret n°2020/45/PM pour conseiller le Gouvernement sur toutes les questions relatives au secteur des Technologies de l'Information et de la Communication (TIC) et plus largement des usages numériques qui se diffusent dans l'ensemble de la société et de l'économie.

Il est placé sous l'autorité du Premier Ministre, et comprend les Ministres chargés des principaux secteurs en relation avec le numérique (Défense Nationale, Intérieur, Économie, Finances, et Numérique) ainsi sept personnalités, dont 4 du secteur privé et 3 du milieu académique et de la société civile, nommées par arrêté du Premier Ministre pour un mandat de 3 ans.

Le Ministre chargé du Numérique assure les fonctions de Secrétaire Permanent du HCN et de Rapporteur Général de ses travaux.

Le Haut conseil du numérique est assisté par un Comité Technique d'Appui (CTA-HCN), composé de responsables du Département chargé des TIC, des sociétés et structures du domaine du numérique et des représentants de haut niveau des Départements ministériels.

Un projet de décret est en cours d'adoption qui devrait :

- reformuler et compléter les missions du HCN, notamment pour inclure explicitement dans son champ de compétence les risques et menaces potentiellement associés à l'usage des technologies numériques ;
- élargir sa composition du HCN aux présidents de deux régulateurs : le Gouverneur de la Banque Centrale de Mauritanie et le Président du Conseil National de Régulation ;
- prévoir une réunion annuelle du HCN au moins pour traiter de la sécurité numérique, dans ses deux volets (cybersécurité et lutte contre la cybercriminalité), afin notamment de conseiller le Gouvernement sur l'adoption et la mise en œuvre de sa Stratégie nationale de sécurité numérique ;
- préciser le rôle du CTA-HCN, en le chargeant notamment explicitement de la préparation des réunions du HCN ;
- la création de commissions sectorielles spécialisées et la définition les grands principes de leur fonctionnement ;
- le renforcement de la confidentialité des informations traitées par le HCN, le CTA-HCN et les commissions sectorielles.

2.2 L'AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'Autorité de Protection des Données à caractère personnel, a été créée dans le cadre de l'application de la loi 2017-020 du 22 Juillet 2017 portant sur la protection des données à caractère personnel, pour veiller à ce que les traitements des données à caractère personnel, soient mis en œuvre conformément aux dispositions de la loi. Le décret n° 2022-13 du 18 février 2022 fixe sa composition, son organisation et son fonctionnement. C'est est une

personne morale de droit public, indépendante, dotée de l'autonomie financière et de gestion. Elle est rattachée au Premier Ministre. Elle informe les personnes concernées et les responsables de traitement de leurs droits et obligations et s'assure que l'utilisation des Technologies de l'Information et de la Communication ne comporte pas de menace au regard des libertés publiques et de la vie privée.

Le mandat des membres de l'Autorité de Protection des Données à caractère personnel, est de quatre (4) ans, renouvelable, une seule fois.

Elle est dirigée par un Président, assisté dans le cadre de l'exercice de ses fonctions par un Secrétaire général qui dirige les services administratifs, financiers et techniques de l'APD et peut, à ce titre, outre les pouvoirs qu'il exerce par délégation du Président, signer tous les actes et décisions d'ordre administratif.

Les services administratifs, financiers et techniques de l'APD sont regroupés au sein des départements suivants :

- Le département administratif et financier ;
- Le département juridique ;
- Le département technique ;
- Le département de la communication ;
- Le département des systèmes d'information.

L'autorité est en cours de mise en place.

2.3 L'AGENCE DU NUMERIQUE DE L'ETAT

L'Agence du Numérique de l'Etat, créée par le décret n°2023-074 du 26 avril 2023, est un établissement public à caractère administratif, dont la mission principale est de contribuer à la mise en œuvre de la stratégie de l'État en matière de transformation numérique. L'AN-ETAT est l'instrument principal du Ministère en charge du numérique pour la mise en œuvre des programmes de transformation numérique aussi bien dans l'Administration Publique que dans les secteurs socio-économiques pour une meilleure productivité au profit de l'ensemble de la société. Ses actions visent à :

- Contribuer au développement et à la promotion des outils et services numériques ainsi que leur usage auprès de l'administration, des entreprises et des citoyens ;
- Développer des standards et bonnes pratiques digitales et veiller à leur application dans l'administration publique et par les différents acteurs économiques et sociaux au niveau national;
- Mettre en place avec les autorités et les organismes concernés, les normes techniques concernant les produits et les services numériques et veiller à leur application par tous ;
- Procéder, dans le cadre des programmes e-Gouvernement, en coordination avec les organismes concernés, à la mise en place et au suivi de projets de l'administration électronique et de développement des services publics numériques et garantir leur interopérabilité et leur intégration ;
- Promouvoir la diffusion des connaissances et compétences numériques au sein de l'Administration et dans l'ensemble de la société mauritanienne ;

- Encourager la réutilisation, l'évolutivité et l'interopérabilité des ressources informatiques au sein de l'Administration publique et œuvrer pour l'atteinte des objectifs de performance dans ce domaine ;
- Promouvoir les partenariats publics-privés dans le numérique ;
- Réaliser des études préalables à la mise en œuvre de ses missions.

La mise en place de l'AN-ETAT est engagée avec la mise en place de la Direction Générale.

III. Analyse du contexte local afin de définir le positionnement de cette autorité ou agence et établir sa mission.

La mise en œuvre de la stratégie nationale de sécurité des systèmes d'information met en jeu les principaux acteurs institutionnels suivants :

1. Le Ministère de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration, créé le **26 mai 2021 (**décret 127-2021 du 27 Juillet 2021) dont la principale mission est **d'assurer une Transformation numérique rapide et sûre, de promouvoir l'innovation et de développer l'e-Gouvernement**. A ce titre, il est chargé de concevoir, coordonner, suivre et évaluer les politiques nationales en matière de numérique, d'Innovation et de Modernisation de l'Administration. Il a élaboré et assure le suivi de la mise en œuvre de la stratégie nationale de cybersécurité qui a définit les orientations stratégiques, les objectifs et les priorités pour renforcer la cybersécurité au niveau national. Il assure la surveillance et la veille technologique en matière de cybersécurité et la mise en place des solutions de sécurité pour le DATA CENTER de l'administration, le renforcement des capacités nationales en matière de cybersécurité à travers la mise en place de programmes de formation et de sensibilisation à la cybersécurité pour les fonctionnaires. Il représente la Mauritanie dans les initiatives internationales, les forums et les initiatives internationales liés à la cybersécurité, et en participant aux négociations internationales, aux accords de coopération et aux échanges de bonnes pratiques pour renforcer la sécurité dans le cyberespace à l'échelle mondiale. Il a piloté la mise en place du cadre législatif et réglementaire dans le domaine de la cybersécurité.

1. Le Ministère de la Justice a pour mission générale, l'élaboration et la mise en œuvre de la politique judiciaire ainsi que l'administration de la justice. Il est responsable de l'élaboration et de la révision des lois et réglementations en matière lutte contre la criminalité en général et de la cybercriminalité en particulier. Il est donc acteur clé dans la création de cadres juridiques solides pour lutter contre les crimes informatiques, protéger les systèmes d'information et prévenir les atteintes à la vie privée, la protection des droits et des libertés fondamentales des citoyens, la veille à ce que les enquêtes et les poursuites judiciaires respectent les normes juridiques, y compris en matière de respect de la vie privée, de la liberté d'expression et du droit à un procès équitable. A travers, les institutions judiciaires, il est chargé de mener des enquêtes sur les infractions cybercriminelles et de coordonner les poursuites judiciaires contre les auteurs de ces actes. Il collabore avec les forces de l'ordre, les services de renseignement et d'autres organismes compétents pour

rassembler les preuves nécessaires à la poursuite des cybercriminels, ainsi que la coordination de l'assistance judiciaire internationale, notamment en facilitant l'échange d'informations, la remise de preuves et l'extradition des suspects.

2. Le MIDEC et le MDN exercent une compétence générale en matière de lutte contre le terrorisme, la répression de toute forme d'ingérence étrangère, à travers la protection des infrastructures critiques (les réseaux électriques, les systèmes de transport, les réseaux de communication et les services financiers, etc.), la conduite d'opérations offensives et défensives, la collecte de renseignements, la formation et la sensibilisation, ainsi que la coopération internationale en matière de cybersécurité. Leur implication est essentielle pour garantir la sécurité nationale dans le cyberespace. Elles doivent être à même de surveiller les activités en ligne, analyser les schémas d'attaques et identifier les acteurs malveillants pour anticiper les futures cybermenaces. Dans notre environnement géographique actuel, les forces de défense et de sécurité ont vocation à mener des opérations cybernétiques offensives pour contrer les menaces provenant de groupes terroristes, d'États hostiles ou d'autres acteurs malveillants.

3. Le Ministère des Affaires Etrangères, de la Coopération et des Mauritaniens à l'Etranger est chargé de la conduite des processus d'élaboration de traités, conventions et accords internationaux. A ce titre, il supervise les négociations relatives à la conclusion des traités, conventions, accords et autres protocoles internationaux à caractère politique et diplomatique, et coordonner les aspects liés aux obligations extérieures de la Mauritanie à caractère économique, commercial, financier, technique, social et culturel. Il est également chargé d'interpréter les traités, accords et autres documents juridiques internationaux qui engagent la Mauritanie, en accord avec les autorités nationales compétentes.

4. Le Ministère de l'Enseignement Supérieur et de la Recherche Scientifique, en plus de sa responsabilité de la promotion de la sécurité informatique dans l'enseignement supérieur, contribue par la formation des professionnels compétents et conscients des enjeux de la sécurité informatique, et favorise l'innovation et le développement de solutions adaptées aux défis de cybersécurité.

5. Le Ministère des Finances est concerné par tous les aspects concernant la protection des informations financières telles que les données fiscales, les informations sur les transactions financières et les données personnelles des contribuables. Il se doit également de prévenir toute forme de fraude fiscale, dans le contexte de digitalisation de ses services et de leur mise en ligne. Ces fraudes en ligne généralement utilisent des méthodes sophistiquées telles que l'usurpation d'identité, la manipulation des déclarations fiscales et le blanchiment d'argent. Il doit mettre en place des mécanismes de détection précoce et des procédures de vérification rigoureuses pour prévenir et combattre ces fraudes ainsi que des mesures de sécurité robustes pour protéger ces informations contre les attaques cybercriminelles, telles que les vols de données, les fraudes financières et les attaques par rançongiciel.

6. La Banque Centrale (la criminalité financière) joue un rôle essentiel dans la lutte contre la cybercriminalité, en particulier en ce qui concerne la protection du système financier et la

préservation de la stabilité économique. Elle est chargée de protéger le système financier contre les attaques cybernétiques en supervisant les institutions financières, en gérant les incidents, en sensibilisant et en formant les acteurs financiers, en développant des réglementations appropriées et en favorisant la coopération internationale dans la lutte contre la cybercriminalité.

7. Les opérateurs télécoms sont en première ligne dans la sécurité informatique, en particulier en ce qui concerne la protection des réseaux de communication contre les attaques, les intrusions et les compromissions et la surveillance de l'activité sur ces réseaux pour détecter toute activité suspecte, anomalie ou attaque en cours, et celles des données sensibles, telles que les informations personnelles des utilisateurs et les données de communication contre les accès non autorisés, les fuites ou les vols. Ils doivent également assurer la sécurité des services qu'ils fournissent tels que la téléphonie, l'accès à Internet, la messagerie et les services cloud le cas échéant.

IV. Etude de benchmark des institutions similaires dans les pays de la sous-région.

Dans un souci d'identifier les meilleures pratiques en matière de mise en place des agences nationales de cybersécurité, il a demandé dans les termes de référence d'étudier le processus de mise en place et le fonctionnent dans d'autres pays et comment celles-ci sont intégrées dans le dispositif national de gouvernance numérique.

D'une façon générale, les institutions sont responsables de plusieurs domaines clés de la cybersécurité. Cela comprend la protection des infrastructures critiques, la supervision des opérations de sécurité, la gestion des incidents, la sensibilisation et l'éducation du public, la coordination avec les acteurs du secteur public et privé, et la promotion de la recherche et du développement dans le domaine de la cybersécurité, ainsi que la coopération aux échelles régionales et internationale.

Le choix s'est porté sur les pays suivants :

4.1 TUNISIE,

L'Agence nationale de la sécurité informatique (ANSI) a été créée en 2003 par la loi n° 2003-58. Elle était placée sous l'autorité du Premier ministre et rattachée au ministère des Technologies de la Communication et de l'Économie Numérique. Son objectif était de coordonner les efforts de sécurité informatique en Tunisie, de promouvoir la sensibilisation à la sécurité des systèmes d'information et de protéger les infrastructures critiques du pays contre les cyberattaques. Au fil des années, les responsabilités de l'ANSI ont évolué pour s'adapter aux défis changeants de la cybersécurité.

En 2015, avec l'adoption de la loi organique n° 2015-26 sur la cybersécurité qui vise à renforcer le cadre juridique de la cybersécurité en Tunisie, les pouvoirs de l'ANSI dans la prévention, la détection et la répression des infractions liées à la cybercriminalité ont été renforcés.

En 2023, un nouveau décret-loi relatif à la cybersécurité (Décret-loi n° 2023-17) a été adopté le 11 mars 202. Il réglemente le domaine de la cybersécurité, transforme l'ANSI en Agence Nationale de la Cybersécurité, fixe les missions et les mécanismes qui lui sont attribués pour assurer la sécurité de l'espace cybernétique tunisien dans le cadre de ses attributions.

L'Agence nationale de la cybersécurité (AN-CYBER) est placée sous la tutelle du ministère chargé des technologies de la communication. En coordination avec les différentes structures impliquées dans le domaine, elle est chargée de la supervision de la sécurité des systèmes d'information et de communication des structures publiques et privées de l'espace cybernétique tunisien à l'exclusion des *systèmes d'informations et équipements électroniques par lesquels sont traitées des données relatives à la sécurité publique ou à la défense nationale et qui affectent la sécurité nationale et l'intérêt suprême de l'Etat*.

L'autorité en charge de la certification électronique est l'Agence Nationale de Certification Electronique (Tuntrust). Elle est sous la tutelle du Ministère des technologies de la communication et ses missions portent :

- La sécurisation des transactions et des échanges électroniques dans le domaine du e-commerce, e-gouvernement (déclaration des impôts, CNSS, TTN...), e-banking (opérations interbancaires,...) e-procurement system (tuneps), messagerie sécurisée,
- L'établissement des accords de confiance mutuelle avec les autorités de certification étrangères.
- La gestion des certificats électroniques (génération, publication et révocation de certificats).
- La recherche, formation et études dans le domaine de la certification et du commerce électronique.
- Le développement des solutions de sécurité qui se basent sur la certification électronique.
- L'octroi d'autorisations d'activité de fournisseur de service de certification électronique.
- L'homologation des systèmes de chiffrement et vérification de la conformité des équipements homologués.

4.2 SENEGAL

La Direction Générale du Chiffre et de la Sécurité du Système d'Information a été créée par le Décret 2021-35 du 14 Janvier 2021. Elle est rattachée au Secrétariat Général de la Présidence de la République. Elle est chargée de la mise en œuvre de la politique de sécurisation et de défense des systèmes d'information. Plus spécifiquement, elle assure la coordination opérationnelle, sur le plan national, des activités concourant à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information, ainsi que la coordination nationale des activités de détection, d'alerte et de réponse aux cyberattaques, en collaboration avec tout organisme national ou international intervenant dans ce domaine. La certification électronique est assurée par SunTrust

4.3 MAROC

La sécurité des systèmes d'information est gérée par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), structure créée an 2011 et rattachée à l'Administration de la Défense Nationale. Elle a pour missions principales la protection des systèmes d'information du gouvernement et des infrastructures critiques, la gestion des incidents de sécurité, la sensibilisation et la formation en matière de cybersécurité, la veille technologique et réglementaire, ainsi que la coopération nationale et internationale pour renforcer la sécurité des infrastructures numériques du pays et lutter contre les cybermenaces. Elle est l'autorité en matière de certification électronique.

4.4 FRANCE

L'Agence nationale de la sécurité des systèmes d'information est l'héritière de la Direction centrale de la sécurité des systèmes d'information (DCSSI) créée par le décret n° 2001-693 du 31 juillet 2001 au sein du Secrétariat général de la défense nationale. Elle a été par le décret n° 2009-834 du 7 juillet 2009 qui lui confère, en plus de la sécurité des systèmes d'informations de l'État, une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN) qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. C'est l'autorité de certification électronique, qui établit les politiques et les référentiels de sécurité pour la certification électronique et coordonne le processus de certification au niveau national et international. Les évaluations de la conformité des prestaires aux normes établies par l'ANSSI et la délivrance des certifications de sécurité sont déléguées à la société LSTI (prestataire privé).

4.5 LE ROYAUME DE L'ARABIE DE SAOUDITE

L'Autorité Nationale de Cybersécurité a été créée en 2017 et est directement rattachée au Roi. Son mandat couvre, entre autres missions, l'élaboration de la stratégie nationale de cybersécurité et la supervision de sa mise en œuvre ; l'établissement des normes en matière de cybersécurité, les contrôles et la conformité en matière de cybersécurité ; la construction et l'exploitation des centres d'opérations de cybersécurité ; le développement des capacités humaines en cybersécurité ; la sensibilisation à la cybersécurité; la stimulation de la croissance du secteur de la cybersécurité et l'encouragement de l'innovation et de l'investissement dans ce secteur ; et l'établissement des liens avec des agences similaires à l'étranger et des entités privées pour l'échange mutuel de connaissances et d'expertise en matière de cybersécurité. Avec la création de l'ANC, l'équipe d'intervention en cas d'urgence informatique (CERT) a été transférée de la Commission des technologies de l'information et des communications (CITC) à l'Autorité nationale de la cybersécurité (NCA).

Parmi, les structures rattachées à l'Autorité, il faut noter l'Académie Nationale de cybersécurité qui vise la formation et le perfectionnement des cadres nationaux spécialisés dans ce domaine.

L'accès à l'Académie est ouvert aux employés d'entités nationales travaillant dans le domaine de la cybersécurité et des domaines connexes, et étudiants fraîchement diplômés des universités et instituts saoudiens dans les programmes d'informatique et de cybersécurité.

La certification électronique est assurée par le National Center for Digital Certification (NCDC), agence sous la tutelle du Ministère de la Communication et des Technologies de l'Information.

L'autorité est dirigée par un président qui a rang de ministre.

4.6 SULTANAT D'OMAN

Le Sultanat d'OMAN a créé en 2010, le Centre National de la Sécurité Informatique et l'a rattaché au Ministère des Transports, Télécommunications et des Technologies de l'Information. C'est une structure autonome, qui a pour missions de renforcer les capacités de cybersécurité du pays dans la détection des incidents de sécurité, la gestion des incidents et les réponses d'urgence à de tels incidents et également d'assurer la veille en fournissant des informations précises et opportunes sur les menaces et les vulnérabilités de sécurité actuelles et émergentes, la sensibilisation à la cybersécurité dans les organisations des secteurs public et privé, y compris les citoyens et les résidents, et promouvoir la R&D en sécurité de l'information.

4.7 TABLEAU RECAPITULATIF

Les missions des différentes structures dans les pays comparés sont globalement les mêmes à savoir définir et mettre en œuvre les politiques nationales en matière de cyber sécurité. Elles assurent toutes la fonction d'équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et de centre d'opérations de cyber sécurité (SOC).

Les différences fondamentales résident dans la forme d'organisation et la structure de rattachement.

Globalement, les organigrammes de ces institutions comportent en plus du management (Directeur Général ou Président ainsi que du ou des adjoints), des chargées de la gestion administrative, comptable et financières, des départements chargés :

1. des opérations de cybersécurité et comprennent :
    - un centre de surveillance et d'alerte : Surveille les menaces et les incidents de cybersécurité, et fournit une réponse rapide en cas d'attaque,
    - Une équipe d'intervention d'urgence : Répond aux incidents de cybersécurité en temps réel, coordonne les activités de réponse et de récupération,
    - Centre de veille : Analyse les tendances, les vulnérabilités et les risques émergents en matière de cybersécurité, et fournit des rapports et des recommandations.
2. la protection des systèmes d'information :
    - Évaluation de la sécurité : Évalue la sécurité des systèmes d'information des organismes gouvernementaux, des infrastructures critiques et des entités privées.

- Certification et accréditation : Établit des normes de sécurité, effectue des audits et délivre des certifications de sécurité pour les systèmes d'information.
- Sensibilisation à la cybersécurité : Mène des campagnes de sensibilisation et de formation pour promouvoir les bonnes pratiques en matière de cybersécurité.

3. la recherche et le développement :
    - Recherche en cybersécurité : Mener des recherches avancées sur les nouvelles technologies, les méthodologies d'attaque et les techniques de défense.
    - Développement de solutions de cybersécurité : Concevoir et développer des solutions de sécurité innovantes, telles que des outils de détection d'intrusion, des pare-feu avancés, etc.
4. La formation et le perfectionnement des intervenants dans la cybersécurité (aussi bien publics que privés) et la vulgarisation des normes guides et bonnes pratiques dans le domaine,
5. la coopération et partenariat avec les structures nationales et étrangères (bilatérales et multilatérales) :
    - Coordination avec d'autres agences nationales de cybersécurité : Échange d'informations, de bonnes pratiques et de ressources avec d'autres agences de cybersécurité au niveau national.
    - Partenariats internationaux : Collabore avec des organisations internationales et des partenaires étrangers pour renforcer la cybersécurité à l'échelle mondiale.
6. le juridique et réglementaire pour l'élaboration et la diffusion des textes liés à la cybersécurité, et proposer des modifications législatives pour lutter contre les cybermenaces, et veiller à ce que les organisations respectent les réglementations en matière de cybersécurité et mener des enquêtes sur les infractions,
7. la sensibilisation pour éduquer et informer le public sur les risques et les bonnes pratiques en matière de cybersécurité, et gérer les relations avec les médias, les communiqués de presse et les informations publiques liées à la cybersécurité.

Pays	Dénomination	Type	Tutelle	Date de création	SOC National	Certification électronique
Tunisie	Agence nationale de la Cybersécurité	Agence	Ministère chargé du Numérique	2009	Oui	Non
France	Agence nationale de Sécurité des Systèmes informatiques	Direction Générale	Secrétaire général de la défense et de la sécurité nationale (Premier Ministère)	7 Juillet 2009	Oui	Oui

Pays	Dénomination	Type	Tutelle	Date de création	SOC National	Certification électronique
Sénégal	Direction Générale du Chiffre et de la Sécurité du Système d'Information	Direction Générale	Présidence de la République (le poste de premier Ministre n'existait pas)	14 Janvier 2021	Oui	Non
Maroc	Direction Générale de de la sécurité des systèmes d'information	Direction Générale	Administration de la Défense Nationale	Septembre 2011	Oui	Oui
Oman	Centre national pour la sécurité informatique	Autorité indépendante	Ministère des Transports, Télécommunications et des Technologies de l'Information	Avril 2010	Oui	Oui
Arabie Saoudite	Autorité Nationale de Cyber sécurité	Autorité indépendante (Rang de Ministre)	Cabinet royal	Novembre 2017	Oui	Non

V. Analyse des principaux risques et facteurs de réussite

La mise en place d'une agence nationale de cybersécurité en Mauritanie fait face à plusieurs défis parmi lesquels :

- le manque de ressources humaines : Comme dans de nombreux autres pays, la Mauritanie fait face à une pénurie de compétences en cybersécurité. Il y a une demande croissante de professionnels qualifiés, mais l'offre en professionnels dans ce domaine est limitée voire inexistante. Pour son fonctionnement l'ACC-ETAT aura besoin de profils variés comprenant des analystes en cybersécurité, des ingénieurs en sécurité des systèmes, d'experts en tests de pénétration, d'architectes de sécurité, des spécialistes en gestion des risques, des experts en cryptographie et des spécialistes en conformité et en réglementation. Cela est d'autant plus pertinent que les enjeux liés à la cybersécurité sont souvent très techniques et évoluent rapidement. Il est essentiel que l'agence dispose d'une expertise technique solide pour faire face aux menaces et aux attaques complexes. Un manque de connaissances techniques peut entraîner des lacunes dans la détection, la prévention et la réponse aux incidents de cybersécurité,
- le faible niveau de coordination intersectorielle jusqu'à présent malgré la mise en place de structures telles que le Haut Conseil National du Numérique : La cybersécurité est

un domaine transversal qui nécessite une coordination efficace entre différents secteurs et acteurs, tels que les organismes gouvernementaux, les entreprises, les fournisseurs de services et les organisations de la société civile. Le risque de manque de coordination et de collaboration entre ces acteurs peut affaiblir la capacité de l'agence à protéger efficacement les infrastructures critiques et à lutter contre les menaces cybernétiques.

- ➔ l'évolution des menaces : les menaces et les attaques cybernétiques évoluent rapidement, ce qui peut rendre difficile pour une agence de cybersécurité de rester constamment à jour. Il est essentiel d'adopter une approche proactive en matière de veille technologique, de renseignement sur les menaces et de développement de capacités pour faire face aux nouvelles techniques d'attaque.

Parallèlement à cela on note des facteurs qui pourront contribuer à la réussite de cette initiative :

1. L'adaption par le gouvernement d'un agenda numérique et d'une stratégie nationale de sécurité numérique traduisant un engagement politique fort du gouvernement et de ses partenaires au développement et leur reconnaissance de l'importance stratégique de la cybersécurité, ce qui devrait faciliter l'allocation des ressources adéquates et la mise en place d'un cadre législatif favorable pour soutenir les activités de l'agence.

2. L'existence d'un cadre juridique et réglementaire robuste portant sur la cybercriminalité, la protection des données, la surveillance des communications, la responsabilité des fournisseurs de services et d'autres aspects juridiques liés à la cybersécurité pour encadrer les activités de l'agence de cybersécurité et qui permet de définir les pouvoirs et les responsabilités de l'agence, ainsi que les mécanismes de coopération avec d'autres acteurs. On peut en citer :

- les différents textes de loi (loi 2013-025 du 15 juillet 2013 portant sur les transactions électroniques, loi sur la protection des données à caractère personnel, loi n°2016-006 d'Orientation relative à la Société Mauritanienne de l'Information (SMI), loi n°2016- 007 sur la cybercriminalité)
- le Décret n°2020/45/PM du 26 mars 2020 relatif à la création, aux missions et modalités de fonctionnement du « Haut Conseil du Numérique » ;
- le décret relatif à la composition, l'organisation et le fonctionnement de l'APD «Autorité de Protection des Données à caractère personnel » ;
- le décret relatif à la conservation des données électroniques et au filtrage,
- le décret relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives,
- le projet de décret de certification,
- l'arrêté créant le Comité Technique d'Appui du HCN et en précisant ses attributions et son fonctionnement,

3. les opportunités de coopération régionale et internationale permettant à l'agence de bénéficier des meilleures expériences de mise en place d'agence, d'élaboration de normes et

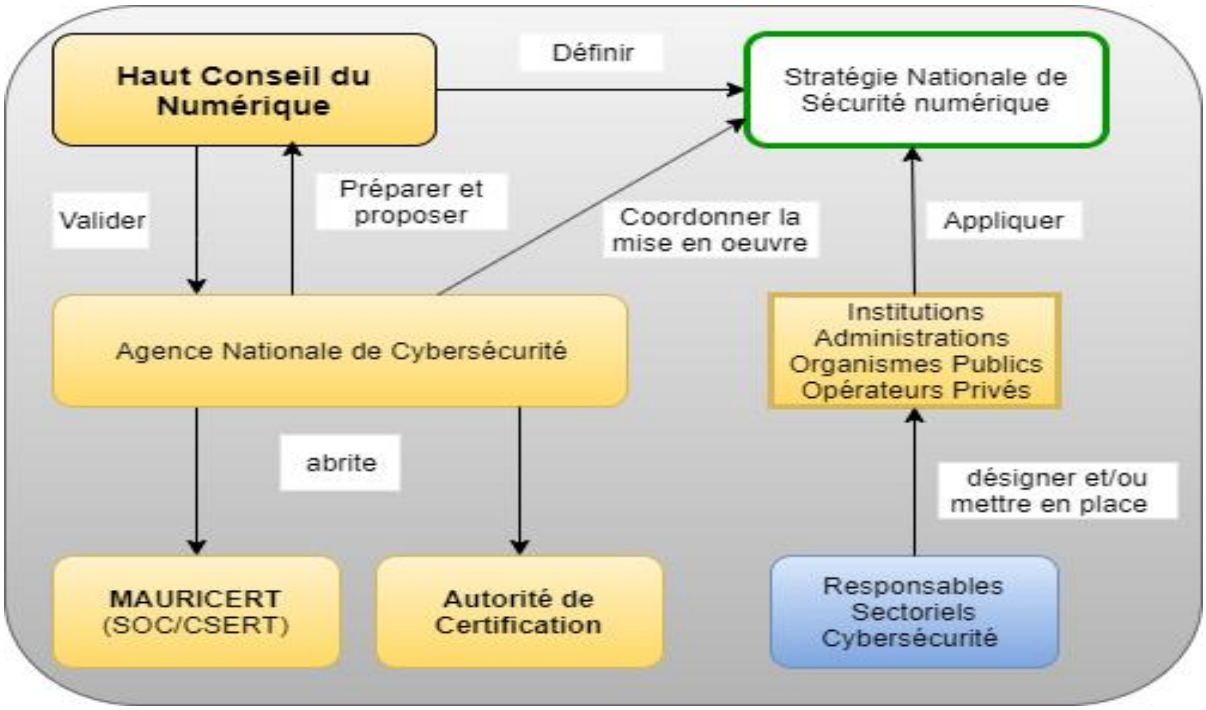
aussi des meilleures pratiques en matière de cybersécurité qui est un défi mondial nécessitant une coopération internationale étroite,

4. les expériences réussies de mise en place de structures analogues au niveau national traitant de thématiques transversales qui nécessitent une coordination intersectorielle. Parmi ces expériences, on peut citer l'ANSADE, l'Agence du Numérique de l'Etat, etc. La mise en place de l'ACC-ETAT devrait bénéficier de leur expérience en matière d'organisation et de processus de mise en œuvre,

VI. Conception de l'Agence à travers la proposition de scénarios de mission, d'Ancrage institutionnels et d'organisation motivés par les résultats du benchmark international et la connaissance de bonnes pratiques dans le domaine

L'objectif (1) de la stratégie nationale de sécurité numérique est de doter la Mauritanie d'institutions nécessaires à sa sécurité numérique. Parmi celles-ci, une structure opérationnelle pour la mise en œuvre de la cybersécurité ou « Agence nationale de la cybersécurité ». La mission de cette Agence telle que définie par la stratégie nationale de sécurité numérique (SNSN) est d'être l'autorité nationale de cybersécurité, d'assurer le pilotage au quotidien des actions de l'État en matière de cybersécurité, et abriter notamment un centre opérationnel, le Centre national de veille, d'alerte et de réaction aux attaques informatiques (CSIRT) ». Elle sera aussi l'autorité nationale en matière de certification électronique.

L'Agence devra s'inscrire dans le dispositif national de sécurité numérique.



6.1 OBJECTIFS ET MISSIONS DE L'AGENCE

Ainsi, la mise en place de l'Agence devra répondre aux objectifs stratégiques suivants :

En matière de cybersécurité

- Améliorer la gouvernance de la cybersécurité au niveau national en renforçant les cadres juridiques et réglementaires du cyberespace national et en veillant à leur application.
- Gérer efficacement les cybermenaces en recueillant des informations sur les menaces émergentes et les tendances des cyberattaques pour mieux comprendre et anticiper les risques de cybersécurité.
- Déterminer l'infrastructure critique et les exigences pour sa protection.
- Effectuer des évaluations de sécurité (Pentest) périodiques et à la demande de l'ensemble l'infrastructure critique nationale et des réseaux et applications du gouvernement.
- Sécuriser les systèmes et réseaux informatiques qui prennent en charge les infrastructures critiques.
- Coordonner et diriger la réponse aux cybermenaces et aux incidents pour minimiser les dommages et assurer un rétablissement rapide des services digitales nationaux.
- Surveiller les cyberactivités pour détecter et prévenir les cyberattaques potentielles.
- Développer les capacités nationales de recherche en cybersécurité.
- Diffuser la culture de cybersécurité et sensibiliser aux bonnes pratiques en matière de cybersécurité et aux risques associés aux cybermenaces auprès des différents acteurs dans le domaine de la cybersécurité.
- Renforcer la coopération locale, régionale et internationale dans le domaine de la cybersécurité afin d'échanger des informations avec d'autres pays et organisations internationales, partager les bonnes pratiques et lutter ensemble contre les cybermenaces transfrontalières.

En matière de certification électronique :

- Définir et appliquer la politique de certification électronique en Mauritanie.
- Installer et gérer l'infrastructure à clé publique (PKI) du gouvernement mauritanien.
- Accréditer et surveiller les fournisseurs de services de certification nationaux qualifiés.
- Émettre, gérer, maintenir et réglementer les certificats électroniques utilisés dans les transactions et les communications électroniques pour garantir leur sécurité, leur authenticité et leur intégrité. Ces opérations peuvent être réalisées directement ou par l'intermédiaire de prestataires publics de services de certification électronique.
- Établir et gérer des accords de reconnaissance mutuelle avec des parties étrangères.

6.2 ANCRAGE INSTITUTIONNEL

Les différents scénarii qui s'offrent pour l'ancrage institutionnel de l'Agence au vu du positionnement des organismes chargés de la cybersécurité dans les autres pays et aussi des structures analogues en Mauritanie sont :

- La Présidence, le Cabinet Royal, le Premier Ministère, (cas de la France, du Sénégal, de l'Arabie Saoudite)
- Le Ministère sectoriel (cas du Maroc, de la Tunisie, du Sultanat d'OMAN).

Le rattachement de l'Agence au niveau supérieur (Présidence de la République, Primature) présente les avantages suivants :

- renforcer l'importance accordée à la protection des systèmes informatiques et des réseaux, réaffirmer que la cybersécurité est devenue aujourd'hui une préoccupation majeure et faire bénéficier l'Agence d'une attention et d'une priorité élevées,
- bénéficier d'une meilleure coordination et d'une plus grande cohérence dans les politiques et les initiatives en matière de cybersécurité, en s'appuyant sur le rôle de coordination stratégique entre les différents ministères et organismes gouvernementaux que joue la primature,
- accéder direct aux décideurs politiques et aux principaux responsables gouvernementaux. Cela facilite la communication, la sensibilisation et l'obtention du soutien nécessaire pour mettre en œuvre des mesures de cybersécurité efficaces,
- avoir une influence accrue dans les processus décisionnels, en participant activement aux discussions politiques, aux négociations internationales et aux initiatives nationales liées à la cybersécurité, et ainsi contribuer à façonner les politiques et les mesures de protection des systèmes informatiques et des réseaux,
- avoir une grande agilité dans la prise de décisions et la réponse aux incidents de cybersécurité. Elle peut travailler en étroite collaboration avec les services de renseignement, les forces de sécurité et les organismes gouvernementaux concernés pour prendre des mesures rapides et efficaces en cas de menace.

Cependant, le rattachement d'agences au plus haut niveau, présente des risques inhérents à ce type d'organisation :

- une concentration du pouvoir ce qui peut entraîner un manque de supervision indépendante et de contrôle, qui peut compromettre la transparence et la reddition de comptes,
- une vulnérabilité aux influences politiques et le risque d'une prépondérance des considérations politiques plutôt que par celles dictées par des besoins techniques ou stratégiques. Cela peut limiter l'efficacité et l'objectivité des mesures de cybersécurité mises en place,
- une certaine rigidité organisationnelle rendant les processus décisionnels plus longs et moins flexibles en raison de la hiérarchie et de la bureaucratie a Cela peut rendre difficile la prise de décisions rapides et la réponse agile aux incidents de cybersécurité.

- un manque d'expertise technique ce qui peut limiter la capacité de l'Agence de Cybersécurité à élaborer et à mettre en œuvre des politiques et des mesures adaptées aux défis technologiques complexes auxquels sont confrontés les systèmes informatiques et les réseaux.
- un éloignement du secteur privé et de la société civile avec lesquels une collaboration étroite est nécessaire pour l'élaboration de politiques et de mesures de cybersécurité qui peut conduire à des politiques unilatérales.

La deuxième option aurait été de rattacher l'ACC-ETAT au Ministère chargé de la Transformation Numérique. Les avantages d'un tel choix sont de garantir une approche intégrée et efficace de la cybersécurité dans le contexte de la transformation numérique en :

- une meilleure coordination et intégration des efforts de cybersécurité avec les actions définies dans le cadre de l'agenda numérique de transformation numérique. Cela permet une approche plus holistique, où les aspects de sécurité sont pris en compte dès la conception des projets numériques,
- une capitalisation de l'expérience acquise à travers la gestion de la sécurité des Datacenter de l'Administration
- une synergie des ressources car le ministère dispose de ressources humaines, et technologiques pouvant être partagées et mises à profit particulièrement dans la phase de démarrage de l'Agence et renforcer les capacités et les compétences en matière de cybersécurité, Partage d'expertise : En travaillant aux côtés d'autres experts de la transformation numérique, l'agence de cybersécurité peut bénéficier d'un échange régulier d'expertise et de connaissances. Cela favorise le développement de compétences complémentaires et la mise en place de synergies entre les différentes parties prenantes impliquées dans la transformation numérique
- un alignement stratégique des activités de l'Agence avec la stratégie nationale de cybersécurité et digitalisation de l'Etat, ce qui garantit que les mesures de cybersécurité soient intégrées dès les premières étapes des projets et que les initiatives de transformation numérique tiennent compte des enjeux de sécurité
- Renforcement de la confiance : Le fait d'être rattaché à un ministère chargé de la transformation numérique peut renforcer la confiance des acteurs du secteur public et privé dans les initiatives de cybersécurité. Cela peut faciliter les partenariats public-privé et encourager une plus grande coopération entre les différentes parties prenantes pour faire face aux défis de la cybersécurité

Les inconvénients éventuels du rattachement de l'Agence de cybersécurité au ministère chargé de la transformation numérique :

- Priorités concurrentes : Le ministère chargé de la transformation numérique peut avoir d'autres priorités, telles que l'innovation technologique, l'expansion numérique, la connectivité, etc. Cela peut entraîner une concurrence pour les ressources et l'attention, ce qui pourrait réduire l'importance accordée à la cybersécurité au sein de l'agence et affaiblir sa position.

- Une Agence rattachée au niveau d'un ministère spécifique fera face à des défis pour assumer son rôle de coordination interministérielle ;
- Confusion des responsabilités pour déterminer clairement qui est chargé de la gouvernance et de la prise de décision en matière de cybersécurité, ce qui peut ralentir les processus de prise de décision et nuire à l'efficacité de l'agence.
- Manque d'indépendance : L'indépendance est un élément crucial pour une agence de cybersécurité efficace. Si elle est rattachée directement à un ministère, il existe un risque que son indépendance soit compromise. Des pressions politiques ou bureaucratiques pourraient influencer ses décisions et ses actions, ce qui pourrait limiter sa capacité à agir de manière objective et proactive.
- Manque de spécialisation : Les ministères chargés de la transformation numérique sont souvent responsables d'un large éventail de questions liées à la technologie et à la numérisation. Cela signifie que les équipes travaillant au sein de ces ministères peuvent ne pas avoir une expertise approfondie en matière de cybersécurité. Par conséquent, l'agence de cybersécurité pourrait se retrouver isolée ou être la seule source d'expertise en la matière, ce qui pourrait entraîner des lacunes dans la prise de décision et la mise en œuvre des mesures de cybersécurité.
- Difficultés de coordination : Bien que le rattachement puisse favoriser la coordination, il peut également entraîner des difficultés supplémentaires en matière de coordination et de collaboration avec d'autres ministères ou agences impliqués dans la cybersécurité. Des processus de coordination complexes et des divergences de priorités pourraient entraver la capacité de l'agence de cybersécurité à travailler efficacement avec d'autres parties prenantes clés.

Le choix du Gouvernement a été de placer l'Agence sous l'autorité du Premier Ministre sous l'égide du HCN. Ce choix a été acté lors a été validé dans une réunion du HCN.

6.3 STRUCTURE ORGANISATIONNELLE

L'analyse des structures organisationnelles des différentes entités montre la nécessité d'avoir les structures suivantes :

- Des structures d'appui (administration, finances, ressources humaines, contrôle de gestion, etc.)

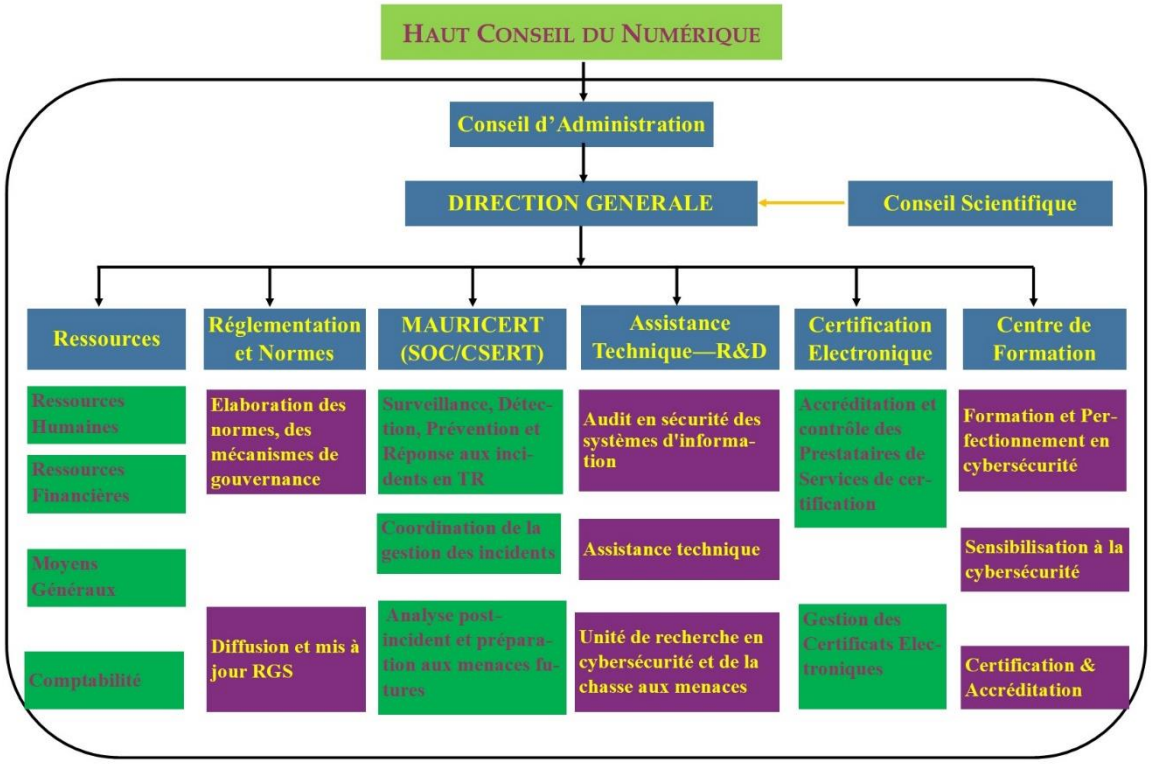
- Une structure en charge du SOC/CSIRT. Le SOC/CSIRT devra être responsable de la coordination et de la gestion des incidents de sécurité informatique survenant dans les réseaux des administrations publiques (RIADE), des opérateurs d'importance vitale (OIV) dont la liste sera définie par voie règlementaire. L'étude en cours « **de faisabilité de la mise en place d'une équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et d'un centre d'opérations de cyber sécurité (SOC) » déterminera** les structures qui devraient avoir leur propre équipe de sécurité, l'ACC-ETAT se chargeant de surveiller l'infrastructure publique partagée par toutes ces entités,

- Une structure en charge de l'accréditation et du contrôle des prestataires de services de certification qualifiés, ainsi que la délivrance, la gestion, la conservation et la

réglementation des certificats électroniques utilisés dans les transactions et les communications électroniques pour garantir leur sécurité, leur authenticité et leur intégrité. Le champ d'action de cette structure sera défini par l'étude en cours lancée par le WARDIP,

- Une structure en charge de l'expertise technique à travers laquelle l'agence fournira son assistance aux institutions nationales (publiques ou privées), réalisera les audits de sécurité des systèmes d'informations pour s'assurer de leur conformité aux règles et normes de cybersécurité, de leur mise en œuvre des consignes,
- Une structure en charge de la recherche en cybersécurité et de la chasse aux menaces (threat hunting). Cette structure définira les thématiques de recherche en cybersécurité et conduira des projets de chasse aux menaces avancées.
- Un Centre de Formation dont l'objectif est de développer les compétences nationales en cybersécurité en dispensant des formations continues et ciblées en cybersécurité pour combler la pénurie actuelle de spécialistes en cybersécurité, et faire face aux menaces en constante évolution. Ce centre sera destiné au personnel de l'Agence, à ceux des institutions nationales (publiques et privées) notamment celles gérant des infrastructures critiques, et aux diplômés en informatique des institutions nationales de formation (ESP, FST, ISCAE, etc.) souhaitant se spécialiser dans la cybersécurité. En plus de dispenser des formations, le Centre de formation sera chargé de préparer des programmes de formation et de sensibilisation, d'élaborer et de diffuser des normes professionnelles pertinentes, de qualifier et de certifier des cadres nationaux spécialisés dans la cybersécurité.
- Une structure en charge d'élaborer, mettre à jour et diffuser la réglementation, les mécanismes de gouvernance, les cadres de gestion des risques et des réponses aux incidents de cybersécurité, les normes et directives liées à la cybersécurité. Elle sera également chargée d'identifier et de classer les infrastructures critiques et les entités associées, et d'identifier les secteurs et entités prioritaires en matière de cybersécurité.

  Des SOC/CSIRT sectoriels devront être mis en place dans toutes les entités publiques ou privées qui gèrent des infrastructures critiques et qui ne sont pas couvertes par l'ACC-ETAT. Ces entités devront définir des points focaux qui seront les vis-à-vis du MAURICERT. Toutes les entités publiques mais aussi privées devront désigner des responsables en charge de la sécurité des systèmes d'information, voire mettre en place des SOC/CERT dans un délai, maximum, d'une (1) année. Ces responsables devront constituer le niveau opérationnel en appliquant à leurs niveaux la stratégie nationale de sécurité.



Comme tous les établissements publics, l'Agence aura un organe délibérant (le conseil d'administration) et un exécutif (Direction Générale). Le caractère hautement scientifique et technologique de l'Agence militerait vers la mise en place d'un conseil scientifique qui servirait d'organe consultatif de réflexion et de proposition, pour l'accompagner dans l'anticipation des grands défis technologiques et socio-économiques de la cybersécurité, et orienter et répartir au mieux les efforts et les ressources.

Le conseil scientifique propose ainsi des thèmes de recherche, s'exprime sur le programme scientifique de l'agence, et est consulté sur toute question d'ordre scientifique entrant dans le cadre des missions de l'agence relatives aux activités de recherche et développement dans le domaine de la sécurité des systèmes d'information, et de la veille technologique menée. Il donne son avis et ses recommandations sur :

- la cohérence des programmes et des projets proposés par le directeur général de l'agence ;
- les modalités de mise en œuvre des programmes et projets de recherche et développement ;
- le choix et l'acquisition de la documentation scientifique ;
- l'organisation et la participation aux évènements et manifestations à caractère scientifique dans le domaine de la sécurité des systèmes d'information ;
- les actions de formation scientifique, de perfectionnement et recyclage au profit du personnel de l'agence ainsi que du personnel en charge de la sécurité des systèmes d'information, au sein des administrations, institutions et organismes publics ;

Le conseil devra rassembler des personnalités scientifiques, choisis *intuitu personae*, principalement dans le monde académique, l'administration et les experts dans le domaine de la cybersécurité.

VII. Analyse des investissements nécessaires à la création de l'Agence.

Les principaux investissements liés à la mise en place de l'Agence porteront sur :

- L'installation de l'agence,
- La création du SOC/CSIRT ou MAURICERT,
- L'unité de gestion des certifications
- La mise d'un centre de formation,
- Le réseau local de l'ACC-ETAT,
- Les ressources humaines

7.1 INSTALLATION DE L'AGENCE

La mise en place de l'Agence nécessitera des investissements classiques pour toute structure à savoir :

- les locaux adaptés et sécurisés,
- les équipements bureautiques et les mobiliers de bureau,
- le réseau local de l'agence ainsi que les outils de gestion,
- les équipements de sécurité physique avec des dispositifs de contrôle d'accès, des caméras de surveillance pour protéger l'accès aux équipements et aux ressources de l'agence,
- des équipements pour la continuité en alimentation électrique (onduleurs, groupe électrogène).

7.2 MAURI-CERT

Le SOC et le CSIRT sont complémentaires pour assurer une approche globale de sécurité. Le SOC est axé sur la surveillance en temps réel et la détection proactive des menaces, tandis que le CSIRT intervient lorsque des incidents de sécurité sont confirmés pour les gérer, les analyser et en tirer des leçons afin d'améliorer la sécurité globale. Le tandem SOC/CSIRT est le centre névralgique de l'Agence, et pour sa mise en œuvre, il doit être équipé de systèmes avancés de surveillance et de détection des incidents de sécurité. Cela comprend des outils de surveillance du réseau, des systèmes de détection et de prévention des intrusions (IDS/IPS), des solutions de gestion des journaux (SIEM ou Security Incident and Event Management), des applications d'investigation numérique et de réponse aux incidents (DFIR ou Digital Forensics and Incident Response) et des solutions d'analyse de la sécurité (par exemple, des scanners de réseau et/ou de cloud, des scanners de mémoire, etc.). Pour la composante des certificats numériques, un ensemble de matériel est requis. En particulier, un module matériel de sécurité (ou HSM) doit être acquis. Cela permettra à l'ACC-ETAT de stocker et de gérer en toute sécurité les informations critiques et les clés des différents certificats qu'il traitera.

L'installation et la configuration de l'infrastructure SOC/CSIRT, y compris l'acquisition, l'installation et l'intégration du matériel et des logiciels généreront des coûts initiaux. Les principaux coûts sont ici liés à la mise en place de l'infrastructure réseau, au déploiement des outils de sécurité et à leur personnalisation. Ces investissements vont se traduire par l'acquisition :

(1) de matériels informatiques (Serveurs : serveurs hautes performances dotés d'une puissance de traitement, d'une mémoire et d'une capacité de stockage suffisantes pour gérer la collecte, l'analyse et le stockage des données, les Périphériques réseau : routeurs, commutateurs, pare-feu et équilibreurs de charge pour établir une infrastructure réseau sécurisée et fiable au sein du SOC, et Systèmes de stockage : systèmes de stockage robustes et évolutifs, tels que le stockage en réseau (NAS) ou le réseau de stockage (SAN), pour prendre en charge le volume croissant de journaux et de données de sécurité),

(2) un ensemble d'outils logiciels comprenant des outils d'analyse de sécurité, des systèmes de détection d'intrusion, des laboratoires de recherche, etc. L'élément central sera un système de gestion des informations et des événements de sécurité (SIEM) ou plate-forme SIEM qui regroupe, normalise et analyse les événements de sécurité et les journaux provenant de diverses sources, offrant des capacités de surveillance en temps réel, de détection des menaces et de réponse aux incidents, incluant également des outils d'automatisation et d'orchestration pour rationaliser les tâches répétitives, accélérer la réponse aux incidents et s'intégrer aux outils et systèmes de sécurité existants.

Plusieurs choix s'offrent entre des solutions open source (Elastic Security , OSSIM (Open Source Security Information Management) de AlienVault, Security Onion distribution de Linux open source, etc.) et des solutions propriétaires (Splunk Enterprise Security, IBM QRadar, McAfee Enterprise Security Manager (ESM), Sumo Logic, etc.).

(3) des éléments matériels et logiciels pour la connectivité du réseau afin d'assurer

- la sécurisation de la segmentation du réseau : mise en place de réseaux segmentés pour isoler l'infrastructure SOC des autres systèmes métier critiques, empêchant tout accès non autorisé et réduisant le risque de déplacement latéral en cas de violation.
- la mise en œuvre de connexions VPN pour un accès à distance sécurisé à l'infrastructure SOC, permettant aux analystes de sécurité distants ou aux équipes de réponse aux incidents de se connecter en toute sécurité à partir d'emplacements externes.
- le déploiement de systèmes de détection et de prévention des intrusions (IDPS) pour surveiller le trafic réseau, détecter et prévenir les intrusions potentielles et fournir une couche de défense supplémentaire pour l'infrastructure SOC,

(4) des outils pour l'intégration des solutions de détection et de réponse aux points terminaux Endpoint Detection and Response (EDR) pour collecter les données de sécurité des terminaux, détecter les logiciels malveillants et identifier les activités suspectes sur les terminaux.

- Scanners de vulnérabilité : intégration d'outils d'analyse de vulnérabilité pour recevoir les résultats de l'analyse, corréler les vulnérabilités avec les événements de sécurité et hiérarchiser les efforts de remédiation.
- Intégration du flux d'intelligence sur les menaces (Threat Intelligence Feeds) dans le SIEM ou d'autres outils de sécurité pour enrichir l'analyse des événements de sécurité et améliorer les capacités de détection des menaces.

(5) des outils pour la gestion des incidents de sécurité et des données des investigations numériques. Le rôle principal de ces outils est de collecter, conserver et analyser les preuves technico-légales dans les incidents de cybersécurité. Les outils DFIR comprendront également une fonction de collecte d'informations sur un incident après qu'il se soit produit et d'analyse et de préservation des preuves pour une utilisation future. L'ensemble d'outils DFIR comprendra des outils pour la récupération d'images de disque complètes, de copie partiels ou complets de la mémoire (RAM), d'analyse du système de fichiers et du trafic réseau.

L'étude envisagée dans le cadre du WARDIP «**de faisabilité de la mise en place d'une équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et d'un centre d'opérations de cyber sécurité (SOC) »** élaborera le cahier de charges avec la liste et les spécifications détaillées des fournitures et services à acquérir pour l'établissement du CSIRT et du SOC. Elle déterminera également les profils nécessaires.

7.3 L'UNITE DE GESTION DES CERTIFICATIONS

Bien qu'à priori, certains équipements peuvent paraitre redondant avec ceux déjà utilisé pour le MAURICERT, ceux de l'infrastructure à clé publique (PKI) devront être distincts en raison de leurs rôles et de leurs besoins spécifiques en matière de sécurité et de fonctionnalité. Ces équipements devront comprendre des composants matériels (serveurs, des éléments de sécurité matérielle (des pares-feux, des dispositifs de prévention des intrusions (IDS/IPS) et des systèmes de détection de logiciels malveillants), des dispositifs de stockage sécurisés, tels que des coffres-forts électroniques, des modules de sécurité matérielle (HSM) ou des systèmes de stockage chiffrés, des dispositifs matériels tels que des lecteurs de cartes à puce, des matériels de vérification d'identité (lecteurs d'empreintes digitales ou d'autres dispositifs biométriques), des outils de surveillance et de gestion du réseau et des systèmes pour surveiller l'activité, détecter les anomalies et garantir le bon fonctionnement de l'ensemble du système.

Des connexions réseau sécurisées, telles que des VPN (Virtual Private Networks) ou des liaisons chiffrées, sont nécessaires pour communiquer avec d'autres entités et pour assurer la confidentialité des données sensibles.

Une solution logicielle devra être acquise (commerciale ou open source) pour mettre en place une infrastructure à clés publiques (PKI), qui comprendra les modules pour :

- la gestion des certificats numériques (émission, validation, révocation et stockage),
- la vérification de l'identité des demandeurs de certificats,
- la gestion des clés logiciels pour générer, stocker et gérer les paires de clés cryptographiques (publiques et privées) associées aux certificats,
- un gestionnaire de base de données pour stocker les certificats émis, ainsi que les informations de révocation,
- des modules logiciels de chiffrement, souvent intégrés dans les systèmes d'exploitation, sont utilisés pour exécuter les opérations cryptographiques nécessaires à la création et à la validation des certificats,
- les outils d'interfaces graphiques et des outils en ligne de commande facilitant la gestion des certificats, la surveillance de l'infrastructure et la résolution des problèmes.

L'Etude de **faisabilité sur les conditions de création d'une infrastructure à clés publiques (ICP) nationale** déterminera les besoins en matériels et logiciels ainsi que leurs spécifications techniques. Elle déterminera également les profils nécessaires.

7.4 LE CENTRE DE FORMATION

Le centre de formation sera une réplique de l'environnement du SOC/CSIRT. L'emploi d'une même plateforme SIEM pour le SOC/CSIRT et le centre de formation comporte plusieurs risques qui peuvent atténuer l'utilisation de deux instances distinctes de la plateforme SIEM : une dédiée au SOC/CSIRT pour les activités de surveillance en temps réel et une autre pour le centre de formation pour les exercices de simulation et les scénarios de formation. Cela permet de maintenir une séparation claire entre les activités de production et de formation, tout en garantissant la continuité des opérations et la sécurité des données. Une seconde option comportant plus de sécurité est l'utilisation d'une plateforme distincte pour le centre de formation pour une séparation physique du SOC/CSIRT et du centre de formation,

- les ordinateurs pour que les participants puissent suivre les cours, réaliser des exercices pratiques et des laboratoires, et effectuer des simulations d'attaques et de défense,
- le réseau local pour permettre aux participants de se connecter aux serveurs, aux équipements réseau, aux machines virtuelles et aux autres ressources du centre de formation,
- des serveurs pour héberger des machines virtuelles, des environnements de test, des applications de formation et des outils de cybersécurité,
- les machines pour créer des environnements de test et des scénarios d'apprentissage, en permettant aux participants de s'exercer dans des environnements contrôlés et isolés,
- les équipements réseau tels que des commutateurs, des routeurs, des firewalls, des sondes de surveillance, etc., sont utilisés pour simuler des environnements réseaux réels et enseigner les concepts de sécurité réseau,
- les environnements de simulation d'attaques et de défense pour permettre aux participants de s'exercer à résoudre des scénarios réalistes d'attaques et de défense.
- les projecteurs et les écrans pour présenter le matériel de formation, les démonstrations et les instructions aux participants.

Le centre utilisera les ressources des différentes structures en tant que formateurs.

7.5 LES RESSOURCES HUMAINES

Pour le démarrage de ses activités, l'ACC-ETAT, devra pourvoir les principaux postes de son organigramme. Comme indiqué plus haut, les ressources humaines qualifiées constituent l'une des principales contraintes de l'ACC-ETAT.

Le personnel d'encadrement technique devra être composé d'ingénieurs en cybersécurité avec des spécialisations dans les divers métiers de la cybersécurité : architecte de la cybersécurité, des administrateurs des systèmes de sécurité, des analystes en renseignement sur les menaces, des auditeurs, des spécialistes en gestion des incidents, en tests de pénétration, cryptologie, etc.

Les profils que l'agence devront recruter devront avoir une formation de base de niveau bac + 5 en informatique ou des domaines connaissances. Ils devront avoir des spécialisations dans les différents domaines de la cybersécurité.

A terme, le personnel de l'ACC-ETAT devra être constitué de :

- des analystes de la sécurité informatique qui surveillent généralement les réseaux pour détecter les vulnérabilités de sécurité et les étudient, en mettant en œuvre des logiciels de sécurité. Ils doivent avoir des compétences en réseau, programmation (Python, Java, C/C++ ou script comme PowerShell), différentes méthodes d'attaque, logiciels malveillants, attaques par déni de service (DDoS) et outils de sécurité (scanners de vulnérabilité, pare-feu). -incendie, outils d'analyse du trafic réseau, systèmes de détection d'intrusion (IDS) et systèmes de prévention d'intrusion (IPS), etc.).
- des testeurs d'intrusion qui joueront le rôle du méchant et tenteront de s'introduire dans les systèmes et les réseaux. Les testeurs d'intrusion tentent d'examiner les systèmes de sécurité existants pour aider une organisation à découvrir les vulnérabilités et à les éliminer. Ces professionnels sont aussi parfois appelés hackers éthiques ou validateurs d'assurance. Il faut beaucoup de compétences et de savoir-faire pour être un testeur d'intrusion efficace. Il est recommandé de rechercher des candidats ayant une formation formelle axée sur la cybersécurité ou les technologies de l'information ainsi qu'une expérience significative dans des rôles connexes.
- des Architectes en cybersécurité qui auront en charge la conception des applications et des systèmes de sécurité de haute technologie d'une organisation. Ils seront chargés d'analyser et de valider les solutions techniques du point de vue de la sécurité informatique. Le rôle exige une connaissance approfondie de l'architecture d'application moderne et des systèmes et réseaux avancés. Cela nécessite également une compréhension globale des différents types et classes de cyberattaques, de risques et de vulnérabilités.
- des professionnels de la récupération de données sont les personnes nécessaires pour sauvegarder ou reconvertir les informations des disques durs endommagés ou d'autres supports. Ils s'occupent également du matériel informatique, résolvent les problèmes mécaniques, effectuent des analyses médico-légales et créent des plans de récupération des données après sinistre. Dans le contexte de la cybersécurité, ces professionnels concentrent souvent leur travail sur la récupération des données d'entreprise à grande échelle et les

efforts d'atténuation des dommages. Dans une grande organisation, beaucoup de données sont générées en peu de temps. Pour minimiser le risque de perte de données, des sauvegardes sont régulièrement créées pour éviter une perte catastrophique.

- des Cryptographes : bien qu'il ne s'agisse pas du titre de poste le plus courant dans le domaine de la cybersécurité, les cryptographes jouent un rôle important dans la sécurité des données en créant et en craquant des codes et des algorithmes de cryptage. Les cryptographes sont les experts qui concevront et mettront en œuvre des algorithmes de renforcement de la sécurité. Ces professionnels sont souvent recherchés par les organisations qui traitent des données hautement sensibles, telles que les institutions financières, les prestataires de soins de santé, les agences gouvernementales et l'armée. Leur travail nécessite une solide formation en mathématiques et une compréhension des principes de l'informatique. Spécialiste de la formation en sensibilisation à la sécurité : même les systèmes de sécurité les mieux conçus peuvent tomber en panne si quelqu'un laisse un intrus franchir la porte d'entrée.
- des spécialistes de la formation en sensibilisation à la sécurité : les professionnels de la cybersécurité savent que le maillon le plus faible d'un plan de sécurité numérique est l'élément humain. Les spécialistes de la formation en sensibilisation à la sécurité ou les agents de sensibilisation à la sécurité seront chargés de dispenser une formation en sensibilisation à la sécurité. Ils réduisent les risques en apprenant aux employés à comprendre les menaces de sécurité et à suivre le protocole de sécurité. Ces professionnels doivent comprendre la cybersécurité de fond en comble, et ils doivent également comprendre les gens. Ils développeront des programmes de sensibilisation à la sécurité, organiseront des formations, évalueront les risques et travailleront avec des personnes du monde entier pour encourager les comportements les plus sûrs possibles.
- des chercheurs en cybersécurité qui étudieront les programmes malveillants tels que les logiciels malveillants et les processus qu'ils utilisent pour exploiter les systèmes, puis utiliseront ces informations pour traiter et éliminer les vulnérabilités. Ils compilent des informations et des analyses sur les menaces, et créent des solutions basées sur les données ou proposent des actions recommandées qui peuvent protéger contre ces programmes malveillants. Ils identifient, suivent et étudient également des itérations spécifiques de logiciels malveillants ou de menaces et leurs créateurs, afin de mieux comprendre leurs stratégies et d'anticiper les menaces futures. Ils compilent et évaluent les analyses pour identifier et résumer les tendances et les modèles connexes. Les chercheurs en cybersécurité ont généralement au moins un diplôme d'ingénieur dans un domaine informatique et une vaste expérience en matière de sécurité informatique et de protection contre les menaces. Ils doivent avoir une expérience pratique des outils et programmes de détection. Ces rôles nécessitent des compétences analytiques avancées et des capacités de résolution de problèmes.
- des juristes spécialisés en cybersécurité traitent des questions légales liées à la protection des données et à l'application des lois et réglementations liées à la cybersécurité. Ils devront avoir une formation de base de juriste et être familiarisés avec les principaux concepts de cybersécurité, les menaces courantes, les vulnérabilités informatiques et les meilleures pratiques de sécurité

Comme toute structure disposant d'un système informatique, l'ACC-ETAT devra aussi disposer d'ingénieurs réseaux, de développeurs, d'administrateurs de système, de base de données et de réseaux.

- les ingénieurs réseaux devront avoir des compétences en réseaux informatiques, en sécurité informatique, en gestion des incidents et en cryptographie. Les certifications ont essentielles pour renforcer les compétences (Certified Information Systems Security Professional (CISSP), le Certified Ethical Hacker (CEH), le Certified Network Defender (CND), le Cisco Certified CyberOps Associate, etc.)
- les administrateurs de systèmes et de bases de données sécurisés qui doivent posséder des connaissances approfondies en administration de systèmes (Windows, Linux, etc.), des réseaux, des protocoles courants et en gestion de bases de données, des compétences en sécurité informatique, et être familiers avec les principaux systèmes de gestion de bases de données (SGBD) (MySQL, Microsoft SQL Server, Oracle, PostgreSQL, etc)
- les ingénieurs développeurs possédant une solide expertise dans les langages de programmation les plus utilisés (comme Python, Java, C++, JavaScript, etc.) et être à l'aise avec les concepts de développement logiciel, les frameworks et les outils de développement pertinents

Le nombre et les profils des différents spécialistes devra être déterminé par **les études de faisabilité de SOC/CERT et d'une ICP nationale**.

La difficulté d'obtenir les profils adéquats sur le marché devra conduire l'agence à recruter des n'ayant pas nécessairement les compétences en matière de cybersécurité mais dans les domaines en rapport avec celle-ci tels que l'administration système & réseau, l'administration des bases de données, le développement web, l'analyse de données, etc. C'est pourquoi elle devra élaborer et mettre en œuvre un programme de formation des personnels recrutés pour répondre aux exigences des différents postes. Ce programme de formation devra aussi être renforcé par les voyages d'études et d'échanges avec les entités en charge de la cybersécurité partenaires.

VIII. Elaboration du cadre juridique et des exigences réglementaires et organisationnelles nécessaires à la création de l'Agence

Les différentes agences publiques créées en Mauritanie l'ont été sous forme d'Etablissement Public à caractère Administratif conformément à l'Ordonnance n° 90-09 du 4 avril 1990 portant statut des établissements publics et les sociétés à capitaux publics, et régissant les relations de ces entités avec l'État. C'est le cas notamment de :

- l'Agence du numérique de l'Etat créée par le décret 2023-074 du 26 Avril 2023,
- l'Agence de promotion des investissements en Mauritanie» (APIM) créée par le Décret n° 2021-017 du 08 février 2021,
- l'Agence nationale de la statistique et de l'analyse démographique et économique (ANSADE),
- l'Agence nationale de promotion de l'emploi des jeunes (ANAPEJ),

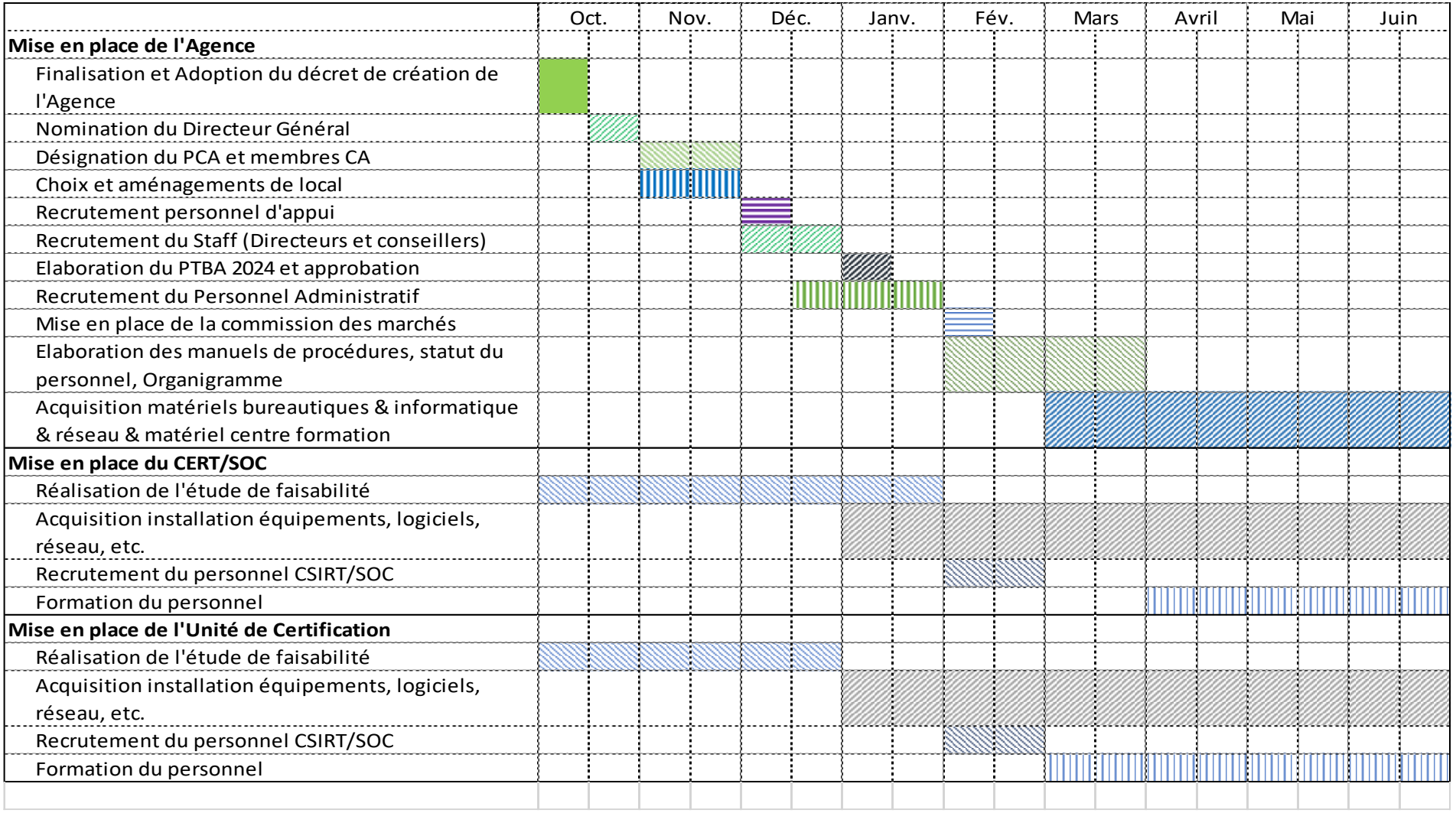
- l'Agence nationale du registre des populations et des titres sécurisés (ANRPTS),
- l'Agence nationale de la recherche scientifique et de l'innovation (ANRSI).

L'Agence de Cyber Sécurité de l'Etat, ne devrait pas déroger à la règle dans la mesure où ce statut lui confère les avantages nécessaires pour la réalisation de la mission publique qui lui est confiée tout en lui garantissant le soutien politique et l'autonomie nécessaire dans la gestion et particulièrement dans celle des ressources humaines.

Elle pourra ainsi recruter en toute transparence les compétences dont elle a besoin et mettre en place un système de rémunération et d'incitation lui garantissant la qualité des ressources humaines et leur offrir les avantages à même de leur assurer une carrière au sein de l'agence. Cette flexibilité dans la gestion des ressources humaines est importante dans la mesure où les profils recherchés par l'Agence risquent de ne pas être disponibles sur le marché du travail et qu'elle devrait recourir au recrutement de profils généraux et investir dans la formation.

Ce statut lui permet aussi de rendre des prestations de services en relation avec ses missions à l'État, à des collectivités territoriales ou à des tiers.

IX. Chronogramme de mise en place de l'agence



Annexes

ANNEXE 1: PROJET DE DECRET PORTANT CREATION, ORGANISATION ET FONCTIONNEMENT DE L'AGENCE DE CERTIFICATION ET DE CYBERSECURITE DE L'ETAT « ACC-ETAT »

REPUBLIQUE ISLAMIQUE DE MAURITANIE
Honneur – Fraternité – Justice

PREMIER MINISTERE

VISAS: DGLTEJO **BOM**

Projet de Décret n°……/PM portant création, organisation et fonctionnement de l'Agence de Cybersécurité de l'Etat « ACC-ETAT »

Le Premier Ministre,

Sur rapport conjoint des Ministres de la Transformation numérique, de l'innovation et de la Modernisation de l'Administration ; de l'Economie et du Développement Durable, des Finances, et du Secrétaire Général du Gouvernement ;

- Vu la Constitution du 20 juillet 1991, révisée en 2006, 2012 et 2017 ;
- Vu la loi n° 2018-022 du 12 juin 2018 portant sur les transactions électroniques ;
- Vu la loi n° 2016-006 du 20 janvier 2016 portant loi d'orientation de la Société de l'Information ;
- Vu la loi n° 2016-007 du 20 janvier 2016 relative à la cybercriminalité ;
- Vu la loi n° 2017-020 du 22 juillet 2017 sur la protection des données à caractère personnel ;
- Vu l'ordonnance n° 90-09 du 04 avril 1990, modifiée, portant statut des établissements publics et des sociétés à capitaux publics et régissant les relations de ces entités avec l'État ;
- Vu l'ordonnance n° 89-012 du 23 janvier 1989, modifiée, portant règlement général de la comptabilité publique ;
- Vu le décret n°157-2007 du 06 septembre 2007 relatif au Conseil des Ministres, et aux attributions du Premier Ministre et des Ministres ;
- Vu le décret n° 90-118 du 18 août 1990, modifié, fixant la composition, l'organisation et le fonctionnement des organes délibérants des établissements ;
- Vu le décret n° _____ du _____ portant nomination du Premier ministre ; Gouvernement ;
- Vu le décret n° _____ du _____ portant nomination des membres du Gouvernement ;
- Vu le décret n° 127-2021 du 27 juillet 2021 fixant les attributions du Ministre de la Transformation numérique, de l'Innovation et de la Modernisation de l'Administration et l'organisation de l'administration centrale de son département ;
- Vu le décret n° _____ du _____ fixant les attributions du Ministre des Finances et l'organisation de l'administration centrale de son Département ;

- Vu le décret n° _____ du _____ fixant les attributions du Ministre de l'Economie et du Développement Durable et l'Organisation de l'Administration centrale de son Département ;
- Vu le décret n° 2020-045 du 26 mars 2020 portant création, missions et modalités d'organisation et du fonctionnement du Haut Conseil du Numérique (HCN) ;

Le conseil des Ministres, entendu le…….

Décrète :

CHAPITRE I : DISPOSITIONS GENERALES

Article premier : Il est créé, conformément aux dispositions de l'Ordonnance n° 90-09 du 04 avril 1990, portant statut des établissements publics et des sociétés à capitaux publics et régissant les relations de ces entités avec l'État, un établissement public à caractère administratif, doté de la personnalité morale et de l'autonomie administrative et financière, dénommé « **Agence de Certification et de Cybersécurité de l'État** » appelée ci-après l'ACC-ETAT. Par dérogation aux règles régissant les établissements publics à caractère administratif, l'ACC-ETAT bénéficie des assouplissements prévus au présent décret et portant notamment sur la gestion administrative et ce, conformément à l'alinéa 3 de l'article 5 de l'Ordonnance n°90-09 du 04 avril 1990.

Article 2 : L'ACC-ETAT est placée sous la tutelle technique du Premier Ministère (Ministère Secrétariat du Gouvernement) et la tutelle financière du Ministère chargé des Finances.

Article 3 : L'ACC-ETAT est créée dans le cadre de la mise en œuvre des stratégies nationales relatives au numérique, à l'innovation et à la modernisation de l'Administration en vue de l'opérationnalisation de ces stratégies, en particulier la stratégie nationale de sécurité numérique. Elle est l'instrument principal du gouvernement pour la mise en œuvre de la politique nationale en matière de cybersécurité.

Elle est chargée, en coordination avec les différentes structures intervenant dans le domaine, d'effectuer le contrôle de l'intégrité des systèmes d'information et de communication des structures publiques et privées du cyberespace national, et exerce principalement les tâches suivantes :

<u>En matière de cybersécurité</u>

- Proposer au Haut Conseil du Numérique (HCN) les actions nécessaires pour renforcer le dispositif national de sécurité numérique et la cybersécurité des systèmes numériques déployés en Mauritanie ;
- Piloter et suivre la réalisation des actions décidées par le HCN en matière de cybersécurité et l'informer régulièrement de l'état d'avancement de ces actions ;
- Animer les travaux du sous-comité du Comité Technique d'Appui du Haut Conseil du Numérique spécifiquement dédié à la sécurité numérique, et les restituer au HCN ;
- Animer et coordonner les travaux interministériels en matière de cybersécurité ;

- Élaborer et proposer les mesures de cybersécurité, diffuser les mesures adoptées et veiller à leur application ;
- Conseiller et assister les services de l'État et les opérateurs d'infrastructures critiques pour la sécurisation de leurs systèmes numériques sensibles ;
- Apporter son concours aux organismes de l'État chargés du développement des services numériques et de la protection des données à caractère personnel ;
- Conduire des audits de sécurité des systèmes numériques, notamment dans les services de l'État et chez les opérateurs d'infrastructures critiques ;
- Coordonner les actions de sensibilisation et de formation en matière de sécurité numérique ;
- Promouvoir le développement d'un écosystème de cybersécurité en Mauritanie ;
- Mener et soutenir les activités de recherche dans le domaine de la cybersécurité ;
- Qualifier les produits de cybersécurité et les prestataires de service de cybersécurité ;
- Entretenir des liens avec ses homologues régionaux et internationaux dans le domaine opérationnel et pour le développement des capacités ;
- Conseiller les autorités gouvernementales en cas de crise liée à la cybersécurité,

En matière de certification électronique

- Définir et appliquer la politique de certification en Mauritanie,
- Accréditer et contrôler les prestataires de services de certification qualifiés,
- Délivrer, gérer, conserver et réglementer les certificats électroniques utilisés dans les transactions et les communications électroniques pour garantir leur sécurité, leur authenticité et leur intégrité. Ces opérations peuvent être effectuées directement ou à travers des fournisseurs de services de certification électronique publics ;
- Etablir et gérer les conventions de reconnaissance mutuelle avec les parties étrangères,
- Participer aux activités de recherche, de formation et d'étude afférentes aux échanges et commerce électroniques

Article 4 : L'ACC-ETAT accomplit sa mission dans le respect des orientations générales définies par l'État en matière de cybersécurité et de certification électronique.

L'agence collabore avec les institutions publiques et privées pour renforcer la confiance dans l'économie numérique, accroître la résilience des infrastructures critiques de l'Etat et, à terme, préserver la sécurité numérique des citoyens mauritaniens. Elle veille au partage de connaissances, au développement des structures et à la formation du personnel, et mène des actions de sensibilisation à la cybersécurité.

L'ACC-ETAT peut être chargée par le Gouvernement d'émettre des recommandations sur la politique générale de l'État en matière de sécurité numérique. L'ACC-ETAT peut également rendre des prestations de services en relation avec ses missions à l'État, à des collectivités territoriales ou à des tiers.

L'ACC-ETAT peut également, à titre onéreux, assurer toute fonction ou action en relation avec ses missions à la demande et pour le compte de l'État, des collectivités locales, des établissements publics, des associations professionnelles, des entreprises, des organisations de la société civile et de tout autre partenaire national ou international intéressé.

Les modalités d'intervention de L'ACC-ETAT seront précisées dans le cadre du contrat-programme.

CHAPITRE II : DE L'ORGANISATION DE L'ACC-ETAT

Article 5 : L'ACC-ETAT est administrée par un organe délibérant, dénommé Conseil d'Administration, régi par les dispositions du Décret n° 90-118 du 19 août 1990 modifié, fixant la composition, l'organisation et le fonctionnement des organes délibérants des établissements publics.

Article 6 : Le Conseil d'Administration de l'ACC-ETAT comprend, outre le président, les membres suivants :

- Un représentant du Ministère chargé de la Justice ;
- Un représentant du Ministère chargé de la Défense Nationale,
- Un représentant du Ministère chargé de l'Intérieur ;
- Un représentant du Ministère chargé de l'Économie ;
- Un représentant du Ministère chargé des Finances ;
- Un représentant du Ministère chargé de la Transformation Numérique ;
- Un représentant du Ministère chargé de l'Enseignement Supérieur ;
- Un représentant élu du personnel.

Le Conseil d'Administration peut inviter à assister à ses réunions toute personne dont il juge l'avis, les compétences ou la qualité utile à la discussion des points inscrits à l'ordre du jour.

Article 7 : Le Président et les membres du Conseil d'Administration sont nommés par Décret pris en Conseil des ministres pour un mandat de trois (3) ans renouvelable une seule fois. Toutefois, lorsqu'un membre du conseil perd, en cours de mandat, la qualité en vertu de laquelle il a été nommé, il est procédé à son remplacement dans les mêmes formes pour le reste du mandat restant à courir.

Article 8 : Le Conseil d'Administration est investi de tous les pouvoirs nécessaires pour orienter, impulser et contrôler les activités de l'ACC-ETAT, sous réserve des pouvoirs reconnus à l'autorité de tutelle et au ministre chargé des Finances par l'Ordonnance n° 90-09 du 4 avril 1990 portant statut des établissements publics et des sociétés à capitaux publics et régissant les relations de ces entités avec l'État. Dans ce cadre, le Conseil d'Administration délibère sur les questions suivantes :

- Le budget prévisionnel ;
- L'organisation administrative ;
- L'organigramme, le statut du personnel et l'échelle de rémunération ;
- Les indemnités des sessions et avantages accordés aux présidents et aux membres des organes délibérants ;
- Le manuel de procédures ;
- Le règlement opérationnel, financier et comptable conformément aux textes en vigueur ;
- Les états financiers des exercices comptables et l'affectation de leur résultat ;

- Le règlement intérieur de l'ACC-ETAT ;
- L'acceptation des dons et legs ;
- Le placement des Fonds ;
- L'autorisation de l'acquisition ou la cession d'éléments du patrimoine immobilier de l'ACC-ETAT ;
- La composition interne de la commission des marchés ;
- Le rapport annuel du commissaire aux comptes ;
- La nomination aux hauts postes de responsabilité de l'ACC-ETAT;
- Les référentiels de services et de prestations que l'ACC-ETAT peut fournir à des tiers à titre onéreux ;
- Autorisation de la signature et l'approbation des accords et des conventions par le Directeur Général. Cette autorisation prend la forme d'une délégation accordée au Directeur Général ;
- Approbation des propositions de parrainage ;
- Approbation du rapport annuel d'activités, qui comprend le bilan, le compte de gestion de l'année écoulée et le projet pour l'année à venir, présenté par le Directeur Général ;
- Délibération dans le respect de la réglementation en vigueur en matière de marchés publics, sur les achats et les acquisitions des biens et services.

Article 9 : Le Conseil d'Administration se réunit au moins trois (3) fois par an en session ordinaire, sur convocation du président, et, en tant que de besoin, en session extraordinaire, sur convocation de son président ou à la demande de la majorité des membres. Les convocations, l'ordre du jour et les documents de travail doivent être adressés aux membres du Conseil huit (8) jours au moins avant la tenue de la session. Le Conseil ne peut valablement délibérer qu'en présence de deux tiers de ses membres. Si ce quorum n'est pas atteint, une deuxième réunion du Conseil peut être valablement tenue, à quatorze (14) jours d'intervalle, sans condition de quorum. Le Conseil prend ses décisions et adopte ses avis à la majorité simple des membres présents. En cas de partage égal de voix, celle du président est prépondérante. Le Secrétariat du Conseil d'Administration est assuré par le Directeur Général. Le Président du Conseil d'Administration peut inviter toute personne qualifiée à participer aux délibérations du Conseil, sans droit de vote. Les procès-verbaux des réunions sont cosignés par le Président et par deux membres du Conseil d'Administration désignés, à cet effet, au début de chaque session. Ces procès-verbaux sont portés sur un registre spécial coté et paraphé par le président du Conseil d'Administration et ouvert à cet effet.

Article 10 : Pour l'exécution de sa mission, le Conseil d'Administration est assisté par un comité de gestion qu'il désigne en son sein, composé de quatre (4) membres dont obligatoirement son Président. Le comité de gestion est chargé de la surveillance et du suivi permanent de l'exécution des délibérations et des orientations du Conseil d'Administration. Il se réunit une fois tous les deux (2) mois et chaque fois que de besoin.

Le Président et les membres du Conseil d'Administration de l'ACC-ETAT perçoivent, en vertu des dérogations prévues à l'article 1 du présent Décret, des indemnités des sessions et avantages conformément à la réglementation en vigueur.

Article 11 : L'autorité des tutelles technique et financière exerce les pouvoirs d'autorisation et d'approbation sur les délibérations du Conseil d'Administration portant sur :

- Le programme d'action, annuel et pluriannuel ;
- Le budget prévisionnel ;
- Le rapport annuel et les comptes de fin d'exercice ;
- Les échelles de rémunération et le statut du personnel ;
- Les tarifs des prestations et des services ;
- L'acquisition et l'aliénation des biens immobiliers. L'autorité de tutelle dispose du pouvoir de substitution, dans les conditions prévues à l'article 20 de l'Ordonnance nº 90-09 du 04 avril 1990, portant statut des établissements publics et des sociétés à capitaux publics et régissant les relations de ces entités avec l'État.

Les procès-verbaux des réunions du Conseil d'Administration sont transmis à l'autorité de tutelle dans la huitaine qui suit la session correspondante. Sauf opposition dans un délai de quinze (15) jours, les délibérations du Conseil sont réputées exécutoires, sous réserve du respect des dispositions réglementaires applicables aux décisions ayant une incidence financière.

Article 12 : L'organe exécutif de l'ACC-ETAT comprend un Directeur Général et un Directeur Général Adjoint. L'ACC-ETAT est dirigée par un Directeur Général nommé par Décret en Conseil des ministres sur proposition du Ministre Secrétaire Général du Gouvernement. Il est assisté dans l'exercice de ses fonctions par un Directeur Général Adjoint nommé dans les mêmes conditions que lui. Il est mis fin aux fonctions du Directeur Général et du Directeur Général Adjoint dans les mêmes formes.

Article 13 : Le Directeur Général est investi de tous les pouvoirs lui permettant d'assurer l'organisation, le fonctionnement et la gestion de l'ACC-ETAT conformément à sa mission, sous réserve des pouvoirs reconnus au Conseil d'Administration aux termes des dispositions du présent Décret et sans préjudice à celles du Décret nº 90- 118 du 19 août 1990, modifié, fixant la composition, l'organisation et le fonctionnement des organes délibérants des établissements publics. Il veille à l'application des lois et règlements et à l'exécution des décisions du Conseil d'Administration.

Article 14 : Dans le cadre de sa mission générale définie à l'article 13 du présent Décret, le Directeur Général a pour mission de :

- Participer à l'élaboration du plan stratégique de développement et la politique de l'ACC-ETAT ;
- Exécuter la politique générale de l'ACC-ETAT dans le cadre des orientations définies par le Conseil d'Administration et les pouvoirs publics ;
- Élaborer le plan d'action annuel et pluriannuel de l'ACC-ETAT ;
- Élaborer et soumettre à l'approbation du Conseil d'Administration l'organigramme de l'ACC-ETAT ;
- Présenter un rapport annuel d'activité au Conseil d'Administration ;
- Veiller à la bonne gestion de l'ensemble des ressources de l'ACC-ETAT ;

- Préparer les réunions du Conseil d'Administration et assurer l'exécution de ses délibérations ;
- Préparer et exécuter le budget en sa qualité d'ordonnateur du budget de l'ACC-ETAT ;
- Représenter l'ACC-ETAT en justice et dans tous les actes de la vie civile ;
- Conclure les conventions et marchés conformément aux lois et règlements en vigueur ;
- Veiller à la préservation de l'équilibre financier de l'ACC-ETAT.

Article 15 : Aux fins d'exécution de sa mission, le directeur général exerce l'autorité hiérarchique et le pouvoir disciplinaire sur l'ensemble du personnel ; il recrute, nomme, note et révoque le personnel conformément à l'organigramme, aux définitions d'emplois et de profils liés à ces emplois et dans les formes et conditions prévues par les procédures internes propres à l'ACC-ETAT approuvées par le Conseil d'Administration. Il nomme aux postes de responsabilité au rang hiérarchique immédiatement inférieur à celui du directeur général adjoint. Les chefs de ces échelons hiérarchiques immédiatement inférieurs à celui du directeur général adjoint, sont choisis au terme d'un appel à la concurrence. Il délègue l'autorité hiérarchique aux personnels d'encadrement concernés dans les formes et conditions prévues par les procédures internes propres à l'ACC-ETAT, approuvées par le Conseil d'Administration. Il peut déléguer à toute personne placée sous son autorité le pouvoir d'agir au nom et pour le compte de l'ACC-ETAT, notamment, de signer certains actes. Les actes accomplis dans le cadre de telles délégations engagent l'ACC-ETAT auprès des tiers.

En cas d'absence ou d'empêchement, il est suppléé dans l'exercice de ses fonctions par le Directeur Général Adjoint.

Article 16 : Il est créé auprès du Directeur Général de l'ACC-ETAT, un conseil scientifique de dix (10) membres pour l'accompagner, en tant qu'organe consultatif de réflexion et de proposition, dans l'anticipation des grands défis technologiques et socio-économiques de la cybersécurité, et orienter et répartir au mieux les efforts et les ressources.

Le conseil scientifique propose ainsi des thèmes de recherche, s'exprime sur le programme scientifique de l'agence, et est consulté sur toute question d'ordre scientifique entrant dans le cadre des missions de l'agence relatives aux activités de recherche et développement dans le domaine de la sécurité des systèmes d'information, et de la veille technologique menée. Il donne son avis et ses recommandations sur :

- la cohérence des programmes et des projets proposés par le directeur général de l'agence ;
- les modalités de mise en œuvre des programmes et projets de recherche et développement ;
- le choix et l'acquisition de la documentation scientifique ;
- l'organisation et la participation aux évènements et manifestations à caractère scientifique dans le domaine de la sécurité des systèmes d'information ;
- les actions de formation scientifique, de perfectionnement et recyclage au profit du personnel de l'agence ainsi que du personnel en charge de la sécurité des systèmes d'information, au sein des administrations, institutions et organismes publics ;

Article 17 : Le Conseil scientifique est composé de personnalités scientifiques, choisis *intuitu personae*, principalement dans le monde académique, l'administration et les experts dans le domaine de la cybersécurité et la transformation numérique.

Les membres du Conseil scientifique sont nommés par arrêté du Premier Ministre, sur proposition du Directeur Général de l'ACC-ETAT. Le président du conseil scientifique est élu par ses pairs. Le conseil scientifique peut faire appel à toute personnalité scientifique ou expert pouvant contribuer utilement à ses travaux en raison de ses compétences dans le domaine de la transformation numérique et la cybersécurité.

Au titre de leurs fonctions, le Président et les membres du Conseil Scientifique perçoivent des indemnités ou avantages particuliers fixés par le Conseil d'Administration.

Article 18 : Le Conseil Scientifique se réunit en session ordinaire deux fois par an, sur convocation de son président.

Il peut se réunir en session extraordinaire, chaque fois que de besoin, sur convocation de son président. Le secrétariat du comité scientifique est assuré par les services de l'agence. Le Directeur Général de l'ACC-ETAT participe aux réunions du Conseil avec voix consultative.

CHAPITRE III – BUDGET, COMPTABILITÉ ET CONTRÔLE

Article 19 : Le budget de l'ACC-ETAT comprend :

En recettes :

- ♣ Les subventions et dotations du budget de l'État ou autres personnes publiques ;
- ♣ Les recettes propres provenant des prestations de services et de travaux d'expertise ;
- ♣ La compensation résultant de la fourniture de services et d'expérience ;
- ♣ Les recettes et produits divers ;
- ♣ Les dons, legs et aides financières.

En dépenses :

- Les salaires, les indemnités et allocations servis aux personnels ;
- Les dépenses de fonctionnement de toute nature ;
- Les dépenses d'investissement de toute nature ;
- Les dépenses de formation et de prestation de services ;
- Les dépenses des engagements de coopération et de partenariat ;
- Les dépenses autorisées par les lois et règlements en vigueur ;
- Les remboursements des dettes.

Le budget prévisionnel de l'ACC-ETAT est préparé par un comité présidé par le Directeur Général et comprenant les responsables concernés de l'ACC-ETAT.

Article 20 : La comptabilité de l'ACC-ETAT est tenue suivant les règles de la comptabilité publique par un agent comptable public, nommé par le ministre chargé des Finances. L'agent

comptable exécute les recettes et les dépenses de l'ACC-ETAT. Il est responsable de ses actes devant le ministre chargé des Finances. Il est justiciable devant les juridictions compétentes.

Article 21 : L'exercice budgétaire et comptable de l'ACC-ETAT commence le 1er janvier et se termine au 31 décembre. Par dérogation aux dispositions de l'alinéa ci-dessus, le premier exercice budgétaire et comptable de l'ACC-ETAT commence à compter de la signature du présent décret.

Article 22 : L'autorité de tutelle financière nomme un commissaire aux comptes ayant pour mandat de vérifier les livres, les caisses et le portefeuille de l'ACC-ETAT et de contrôler la régularité et la sincérité des inventaires, des bilans et des comptes. Le Commissaire aux Comptes est convoqué aux réunions du Conseil d'Administration ayant pour objet l'arrêt et l'approbation des comptes. A cet effet, l'inventaire, le bilan et les comptes de chaque exercice doivent être mis à la disposition du Commissaire aux Comptes avant la réunion du Conseil d'Administration consacrée à ces documents comptables qui se tient dans un délai de trois mois suivant la clôture de l'exercice.

Article 23 : Le Commissaire aux Comptes établit un rapport dans lequel il rend compte du mandat qui lui a été confié et signale, le cas échéant, les irrégularités et inexactitudes qu'il aurait relevées. Ce rapport est transmis à l'autorité de tutelle ainsi qu'au Conseil d'Administration. Les honoraires du Commissaire aux Comptes sont fixés par le Conseil d'Administration conformément à la réglementation en vigueur.

CHAPTITRE IV – DU PERSONNEL DE L'ACC-ETAT

Article 24 : Le personnel de l'ACC-ETAT est régi conformément aux dispositions du Code du Travail et de la Convention Collective par un statut du personnel approuvé par le Conseil d'Administration et des procédures internes qui seront approuvées par le Conseil d'Administration.

CHAPITRE V : DISPOSITIONS FINALES

Article 25 : Sont abrogées Toutes les dispositions antérieures contraires au présent Décret.

Article 26 : Le Ministre Secrétaire Général du Gouvernement, Le Ministre de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration, le Ministre de l'Economie et du Développement Durable et le Ministre des Finances sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret qui sera publié au Journal Officiel de la République Islamique de Mauritanie.

Le Premier Ministre

Le Ministre de l'Economie et du Développement Durable

Le Ministre des Finances

Le Ministre de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration

Le Ministre, Secrétaire Général du Gouvernement