ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE
CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2024-1133

DU CONSEIL DE REGULATION DE L'AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE CÔTE D'IVOIRE

EN DATE DU 18 SEPTEMBRE 2024

DEFINISSANT LES CONDITIONS ET LES PROCEDURES D'AGREMENT DES PRESTATAIRES D'AUDIT DE SECURITE DES SYSTEMES D'INFORMATION (PASSI)

Conseil de Régulation : 31 Av Nogués, Imble Broadway 2ème étage 17 BP 110 Abj 17 Tél: +225 27 20 34 43 04 - Fax: +225 27 20 34 43 02
Siège Direction Générale : Marcory Anoumabo, 18 BP 2203 Abj 18 Tél: +225 27 20 34 43 73 / 74 - Fax: + 225 27 20 34 43 75
www.artci.ci

LE CONSEIL DE REGULATION,

Vu la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;

Vu la Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques ;

Vu la Loi n°2017-803 du 07 décembre 2017 d'orientation de la société de l'information en Côte d'Ivoire ;

Vu la Loi n°2024-352 du 06 juin 2024 relative aux communications électroniques ;

Vu l'Ordonnance n°2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre autorités administratives ;

Vu le Décret n°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;

Vu le Décret n°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;

Vu le Décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

Vu le Décret n°2019-947 du 13 novembre 2019 portant nomination du Président du Conseil de Régulation de l'Autorité de Régulation des Télécommunication /TIC de Côte d'Ivoire ;

Vu le Décret n°2019-985 du 27 novembre 2019 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunication/TIC de Côte d'Ivoire en abrégé ARTCI ;

Vu le Décret n°2020-128 du 29 janvier 2020 portant création, organisation et fonctionnement du Centre de veille et de réponse aux incidents de sécurité informatique dénommé Côte d'Ivoire Computer Emergency Response Team ;

Vu le Décret n°2021-913 du 22 décembre 2021 portant adoption du référentiel général d'interopérabilité des systèmes d'information ;

Vu le Décret n°2021-915 du 22 décembre 2021 portant adoption de la politique de sécurité des systèmes d'information de l'administration publique ;

Vu le Décret n°2021-916 du 22 décembre 2021 portant adoption du référentiel général de sécurité des systèmes d'information et du plan de protection des infrastructures critiques ;

Vu le Décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information ;

Vu le Décret n°2022-265 du 13 avril 2022 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunication/TIC de Côte d'Ivoire en abrégé ARTCI ;

Vu le Décret n°2022-783 du 12 octobre 2022 portant renouvellement partiel du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire, en abrégé ARTCI ;

Vu la Décision n°2013-0003 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 20 septembre 2013 portant Règlement intérieur ;

Par les motifs suivants :

Considérant qu'aux termes des dispositions de l'article 50 de la loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques, l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) est chargée de veiller à la sécurité des réseaux et systèmes d'information ;

Qu'à ce titre, elle procède notamment à l'audit et à la certification des systèmes d'information des personnes morales établies en Côte d'Ivoire exerçant des activités de transactions électroniques ;

Considérant que, suivant l'article 5 du décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information, les missions d'audit de sécurité sont effectuées par l'ARTCI ;

Considérant que, dans le cadre de l'exercice de cette mission d'audit de sécurité des systèmes d'information, l'ARTCI peut, en application de l'article 6 du même décret, confier les missions d'audit de sécurité à des Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI) ;

Considérant que les PASSI, pour être des vecteurs de confiance dans les activités d'audit de sécurité, doivent justifier de compétences techniques, de savoir-faire et d'habilitation ;

Considérant le nombre important d'organismes à auditer, il y a lieu d'agréer des PASSI pour assurer l'exercice des activités d'audit de sécurité des systèmes d'information ;

Considérant également que, pour la gestion de l'audit, il est fait distinction entre les PASSI publics et les PASSI privés ;

Considérant la sensibilité des informations détenues par les administrations publiques, les PASSI publics sont habilités à auditer les administrations publiques et les organismes privés, tandis que les PASSI privés sont habilités à auditer exclusivement les organismes privés ;

Considérant que, conformément aux dispositions de l'article 5 du décret susvisé, les conditions et les procédures d'agrément des PASSI sont fixées par décision de l'ARTCI ;

Après en avoir délibéré,

DECIDE :

Article 1 :

Le Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) adopte les conditions et procédures d'agrément des prestataires d'audit de sécurité des systèmes d'information (PASSI) telles que fixées en annexe de la présente décision dont il fait partie intégrante.

Article 2 :

Le prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI) est tenu de se conformer aux conditions et procédures d'obtention d'agrément définies en annexe de la présente décision.

Article 3 :

La demande d'agrément pour l'exercice de l'activité de Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI) est soumise au paiement de frais de dossier et d'étude dont le montant est fixé à deux cent mille (200.000) francs CFA.

Article 4 :

L'exercice de l'activité de Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI) est soumis au paiement de la redevance au titre de l'audit, contrôle et certification des systèmes d'information conformément à l'article 51 de la loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques.

Article 5 :

L'ARTCI se réserve le droit de procéder à la révision des conditions et procédures d'agrément des prestataires d'audit de sécurité des systèmes d'information (PASSI) annexées à la présente décision, en cas de modification de l'environnement technique et réglementaire dans les activités d'audits de sécurité.

Article 6 :

Le Directeur Général est chargé de l'exécution de la présente décision, qui sera publiée au Journal Officiel de la République de Côte d'Ivoire et sur le site internet de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire.

Fait à Abidjan, le 18 Septembre 2024
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ARTCI

AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

PROCEDURE D'AGREMENT DES PRESTATAIRES D'AUDIT DE SECURITE DES SYSTEMES D'INFORMATION

Sommaire

1. **Introduction** 4
   - 1.1 **Objet et Identification du document** 4
   - 1.2 **Champ d'application** 4
   - 1.3 **Date d'application** 4
   - 1.4 **Elaboration, mise à jour et diffusion** 4
   - 1.5 **Documents de références** 4
2. **Procédures** 4
   - 2.1 **Présentation Générale** 4
   - 2.2 **Principaux acteurs** 5
   - 2.3 **Procédure d'obtention d'agrément** 6
     - 2.3.1 **Descriptif** 7
       - 2.3.1.1 Dépôt de la demande d'obtention d'agrément 7
       - 2.3.1.2 Etude et examen de la demande 7
       - 2.3.1.3 Décision 8
       - 2.3.1.4 Publication de la liste des PASSI agréés 8
   - 2.4 **Procédure de renouvellement d'agrément** 9
     - 2.4.1 **Descriptif** 10
       - 2.4.1.1 Dépôt de la demande de renouvellement d'agrément 10
       - 2.4.1.2 Etude et examen de la demande de renouvellement 10
       - 2.4.1.3 Décision 11
       - 2.4.1.4 Mise à jour de la liste publiée des PASSI agréés 11
3. **Formulaires et supports liés** 12

Références

Descriptif du Document	
Titre du document :	**ARTCI –Guide d'agrément des PASSI**
Version du document :	**1.0**
Statut du document :	**En cours** / Revu / Validé
Auteur :	

Historique		
Version	**Date**	**Motif et nature de la modification**
1.0	01 JUIN 2024	Création du document

1. Introduction

1.1 Objet et identification du document

Le présent document décrit le processus d'agrément liminaire ou de renouvellement d'agrément des Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI).

Le présent document est dénommé « Procédure d'agrément des PASSI ». Il est identifiable par son nom, sa référence, son numéro de version et sa date de mise à jour.

1.2 Champ d'application

Cette procédure s'applique à toute demande d'agrément initiale ou de renouvellement, reçue de la part d'une personne morale en tant que PASSI.

1.3 Date d'application

Ce présent document s'applique à compter de la date de publication.

1.4 Elaboration, mise à jour et diffusion

Ce document a été rédigé, mis à jour et publié par l'ARTCI qui fixe les dispositions transitoires et la date d'entrée en vigueur de chaque mise à jour.

1.5 Documents de références

- **RGSSI** : Référentiel Général de Sécurité des Systèmes d'Information ;
- **RACSI** : Référentiel d'Audit de sécurité et de Certification des Systèmes d'Information ;
- **RE-PASSI** : Référentiel d'exigences des PASSI ;
- **CA** : Cahier de charge des PASSI.

2. Procédures

2.1 Présentation Générale

Dans le cadre de son mandat de régulateur des TIC, et conformément à l'article 50 de la loi N°2013-456 du 30 juillet 2013 relative aux transactions électroniques, l'ARTCI est appelée à procéder *« à l'audit et à la certification des systèmes d'information des personnes morales établies en Côte d'Ivoire et exerçant des activités de transactions électroniques ».*

Aussi, selon les dispositions du décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information, les organismes relevant du secteur public ainsi que les entreprises du secteur privé se trouvant sur le territoire national, doivent faire auditer régulièrement leurs systèmes par des prestataires de services d'audit agréés par l'Autorité de Régulation des télécommunications de Côte d'Ivoire (ARTCI).

L'objectif est de doter les systèmes d'information de ces organisations de capacités défensives et

résilientes capables de créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information.

Pour ce faire, et conformément au RGSSI, l'ARTCI est responsable de la mise en place de l'agrément et la qualification de Prestataires de Services d'Audit de Sécurité des Systèmes d'Information (PASSI) qui sont amenés à auditer les systèmes d'information de ces organisations. Dans ce contexte, l'ARTCI doit agréer des personnes morales ou renouveler leurs agréments, suite à leurs demandes formulées et suivant les exigences et des critères prédéfinis, en qualité de Prestataire de service d'audit de sécurité des systèmes d'information.

Cet agrément délivré représente une certification des personnes morales en tant que PASSI, pour réaliser tout ou partie des missions d'audit et pour contribuer au processus de certification des systèmes d'information des organismes.

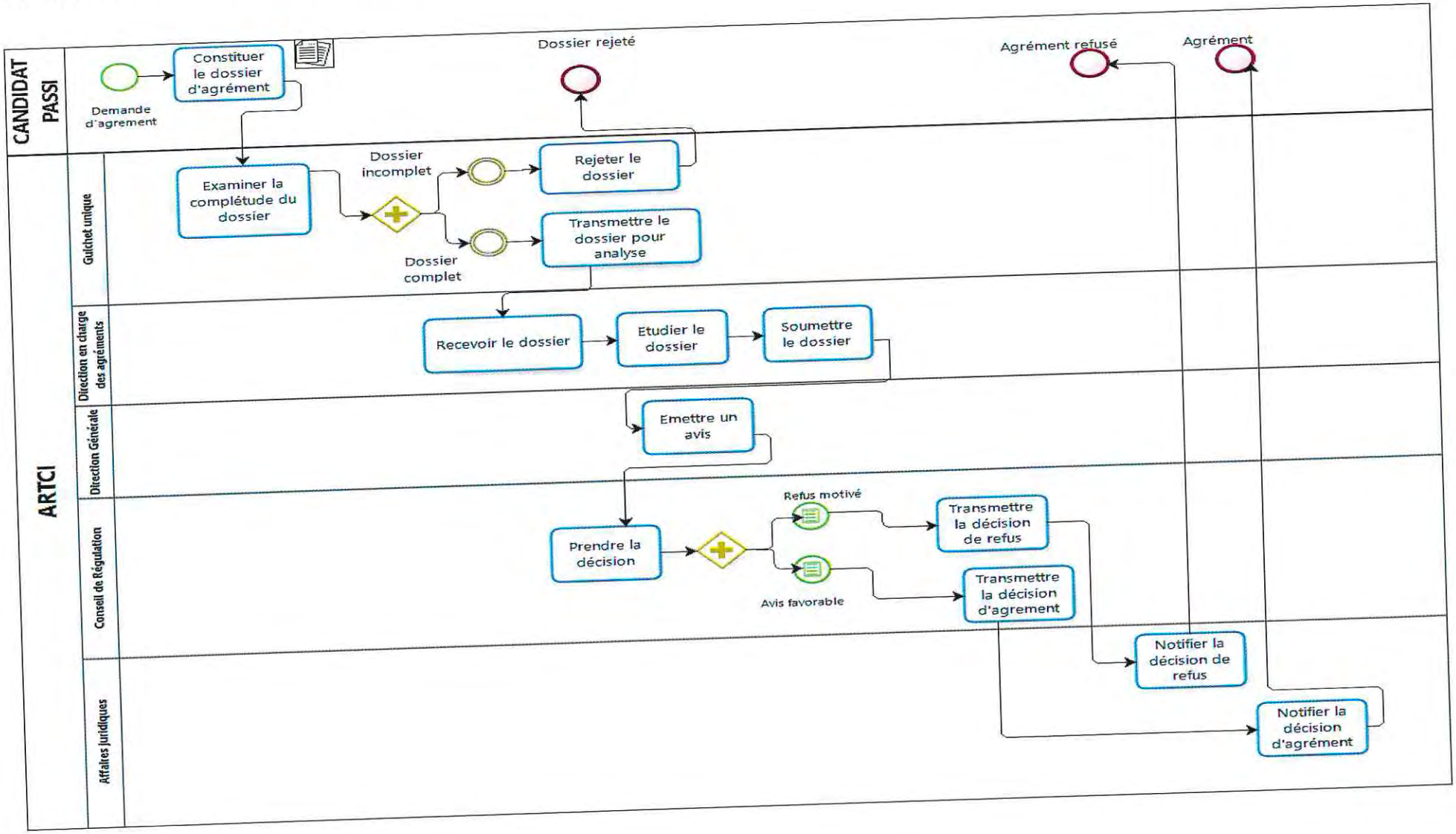
2.2 Les principaux acteurs

Les acteurs du processus d'agrément ou de renouvellement d'agrément des PASSI sont :

- La personne morale demanderesse de l'agrément ou de son renouvellement ;
- Guichet Unique ;
- La Direction en charge des audits de sécurité des Systèmes d'Information ;
- La Direction en charge des affaires juridiques ;
- Le Directeur Général de l'ARTCI ;
- Le Conseil de Régulation de l'ARTCI.

2.3 Procédure d'obtention d'agrément

2.3.1 Schéma



2.3.2 Descriptif

2.3.2.1 Dépôt de la demande d'obtention d'agrément

Les demandes d'obtention d'agrément sont adressées à l'ARTCI par dépôt physique auprès des services du Guichet Unique contre accusé de réception.

L'accusé de réception du dossier de demande d'agrément ne vaut pas acceptation de la demande.

Les frais d'étude du dossier de demande d'agrément s'élèvent à deux cent mille francs CFA (200 000 FCFA) par type d'agrément.

L'obtention de l'agrément se fait sur décision du Conseil de Régulation de l'ARTCI. Après décision favorable par le Conseil de Régulation, un agrément est délivré et celui-ci donne aux PASSI l'autorisation d'exercer des prestations d'audits de sécurité des systèmes d'information.

La délivrance de l'agrément est subordonnée au paiement des frais d'agrément, dont le montant, les conditions et les modalités de paiement seront fixés par décision du Conseil de Régulation.

La demande d'obtention d'agrément des PASSI doit obligatoirement impliquer un audit organisationnel et physique et un audit de tests d'intrusion.

Toutefois nous aurons des agréments d'audit optionnel :

- Agrément en audit de code source ;
- Agrément en audit d'architecture ;
- Agrément en audit de configuration.

Le dossier de candidature doit, obligatoirement, comprendre les documents suivants :

- Un formulaire de demande d'agrément établi par l'ARTCI, dûment rempli et signé par le représentant légal du demandeur de l'agrément,
- Une copie de la carte d'identité nationale du représentant légal de la personne morale,
- Une copie du registre de commerce et du crédit mobilier (RCCM),
- Un extrait de casier judiciaire du représentant légal du demandeur de l'agrément datant de moins de trois (3) mois,
- Une copie certifiée conforme du contrat de travail conclu avec l'auditeur,
- Une copie certifiée conforme de la certification du domaine de l'auditeur,
- Une copie certifiée conforme des statuts juridiques,
- Une attestation de régularité fiscale,
- Le justificatif du paiement des frais d'étude de dossier,
- Les attestations de bonne exécution d'audit de sécurité des systèmes d'information le cas échéant,
- La politique de sécurité du système d'information du PASSI,
- Le code déontologique des PASSI dûment signé.

2.3.2.2 Etude et examen de la demande

Le délai de traitement de la demande d'agrément est de deux mois maximums à compter de la date de réception du dossier complet.

Le dossier de candidature est soumis à la direction en charge des audits de sécurité qui doit se prononcer sur les demandes d'obtention d'agrément des Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI).

Après examen du dossier, la direction en charge des audits de sécurité soumet un rapport de traitement à la Direction Générale de l'ARTCI, qui émet un avis pour décision au Conseil de Régulation.

2.3.2.3 Décision

Le Conseil de Régulation de l'ARTCI, sur avis de la Direction Générale octroie ou refuse l'agrément par décision qui sera notifiée au demandeur.

La décision d'agrément est notifiée à l'organisme demandeur par la direction en charges des affaires juridiques de l'ARTCI sous forme agrément PASSI. Il précise les domaines pour lesquels l'organisme est agréé. La date de validité de l'agrément est de à trois (03) ans à compter de sa date de signature.

L'agrément de Prestataire d'Audit de Sécurité des Systèmes d'Information, délivré par l'ARTCI est strictement personnel à la personne morale. Cet agrément ne peut être ni cédé, ni mis en gage, ni transmis à un tiers.

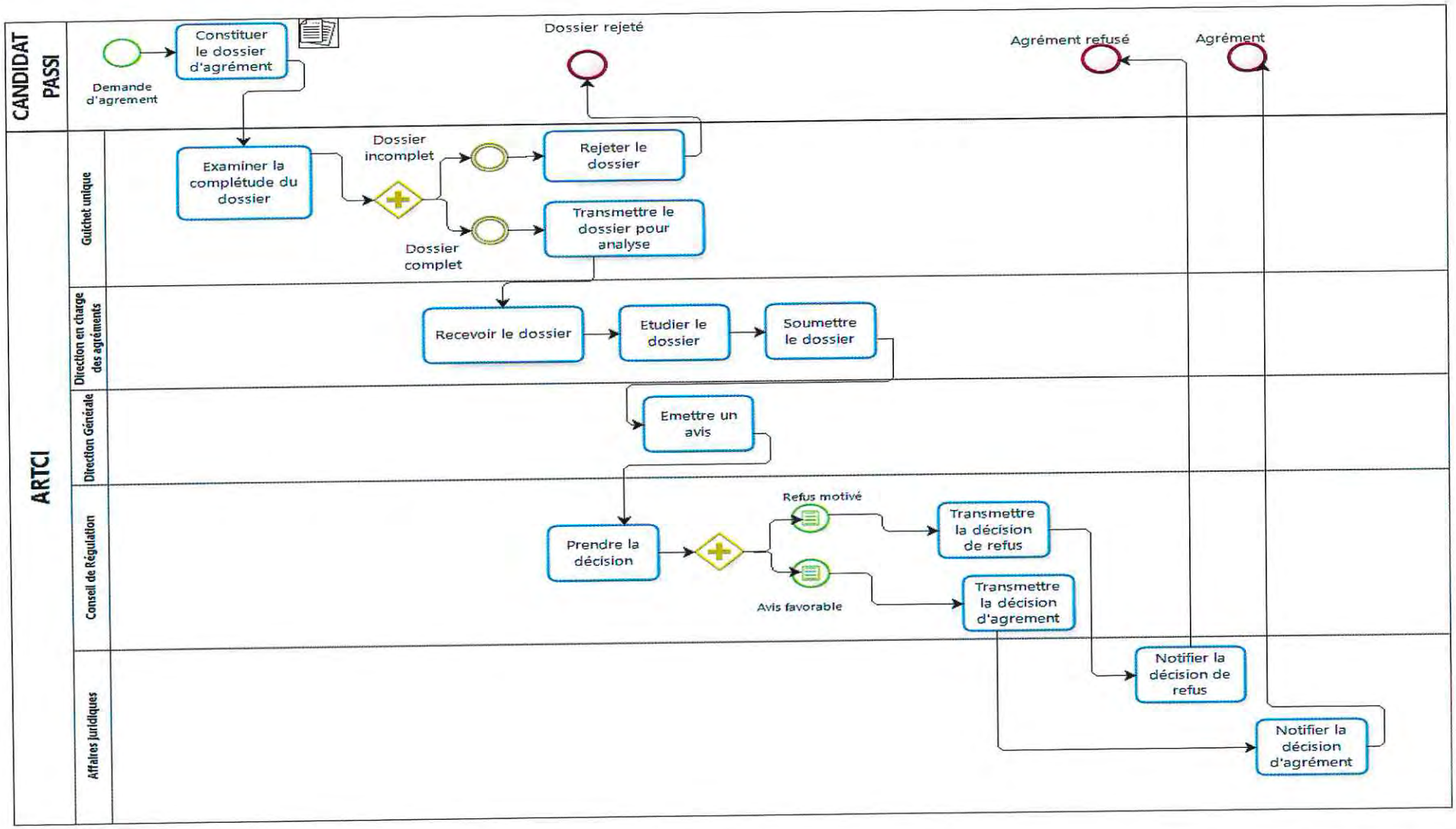
Le cahier des charges des PASSI est annexé à l'agrément. En cas de non-respect des dispositions qui y sont mentionnées, l'ARTCI peut procéder à la suspension ou au retrait de l'agrément du PASSI en fonction de la nature et de la gravité des manquements.

2.3.2.4 Publication de la liste des PASSI agréés

L'ARTCI met à la disposition du public via son site Internet, une liste des PASSI agréés contenant leurs coordonnées, le type d'agrément et sa durée de validité.

2.4 Procédure de renouvellement d'agrément

2.4.1 Schéma



2.4.2 Descriptif

2.4.2.1 Dépôt de la demande de renouvellement d'agrément

L'agrément est valable trois (3) ans. Le PASSI, peut au terme de la validité de son agrément, demander un renouvellement trois (3) mois avant sa date d'expiration par dépôt physique auprès des services du Guichet Unique de l'ARTCI contre accusé de réception.

L'accusé de réception du dossier de demande d'agrément ne vaut pas acceptation du renouvellement de l'agrément.

Les frais d'étude du dossier de demande de renouvellement d'agrément s'élèvent à deux cent mille francs CFA (200 000 FCFA) par type.

La demande de renouvellement d'agrément des PASSI doit obligatoirement impliquer un audit organisationnel et physique, et un audit de tests d'intrusion.

Toutefois nous aurons des agréments d'audit optionnel :

- Agrément en audit de code source ;
- Agrément en audit d'architecture ;
- Agrément en audit de configuration.

Le dossier de demande de renouvellement doit obligatoirement, comprendre les documents suivants :

- Une demande de renouvellement d'agrément, établie par l'ARTCI, dûment remplie, et signée par le représentant légal du demandeur de l'agrément ;
- Une attestation de régularité fiscale ;
- Une copie certifiée conforme des certificats en audit de sécurité de l'expert auditeur ;
- Le justificatif du paiement des frais d'étude de dossier ;
- Les justificatifs de paiement de la redevance pour l'audit, le contrôle des systèmes d'information et la certification électronique ;
- Le justificatif du paiement complet antérieur des frais d'agrément des PASSI ;
- La politique de la sécurité des systèmes d'information du PASSI ;
- Le code déontologique du PASSI dûment signé ;
- La demande de mise en conformité ou attestation de mise en conformité des DCP.

En cas de changement ou de modification, fournir les documents suivants :

- Une copie de la carte d'identité nationale du représentant légal de la personne morale ;
- Une copie du Registre de Commerce et du Crédit Mobilier (RCCM) ;
- Un extrait de casier judiciaire du représentant légal de la demanderesse datant de moins de trois (3) mois ;
- Une copie certifiée conforme des statuts juridiques.

2.4.2.2 Etude et examen de la demande de renouvellement

Le délai de traitement de la demande de renouvellement d'agrément est de deux mois maximum à compter de la date de réception du dossier complet.

Le dossier de candidature est soumis à la direction en charge des audits de sécurité qui doit se prononcer sur les demandes d'obtention d'agrément des Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI).

La Direction en charge des audits procède à un contrôle auprès du candidat PASSI afin de vérifier le respect des obligations du Référentiel d'exigences des PASSI et le cahier des charges des PASSI et la loi DCP.
Après examen du dossier, la direction en charge des audits de sécurité soumet un rapport de traitement à la Direction Générale de l'ARTCI, qui émet un avis pour décision du Conseil de Régulation.

2.4.2.3 Décision

Le Conseil de Régulation de l'ARTCI, sur avis de la Direction Générale octroie ou refuse le renouvellement d'agrément par décision qui sera notifiée au demandeur.
Les demandes de renouvellement d'agrément peuvent être refusées si le PASSI ne respecte pas ses obligations au titre du cahier des charges pendant la période d'agrément. Ce refus ne donne droit à aucune indemnisation.
Si un agrément n'est pas renouvelé à la date d'échéance, il sera considéré « retiré » à compter du lendemain de cette date.

La Décision d'agrément est notifiée à l'organisme demandeur par la direction en charge des affaires juridiques de l'ARTCI. Il précise les domaines pour lesquels l'organisme est agréé. La date de validité de l'agrément est de trois (03) ans à compter de sa date de signature.

L'agrément de Prestataire d'Audit de Sécurité des Systèmes d'Information, délivré par l'ARTCI est strictement personnel à l'exploitant. Cet agrément ne peut être ni cédé, ni mis en gage, ni transmis à un tiers.

2.4.2.4 Mise à jour de la liste publiée des PASSI agréés

L'ARTCI, à travers sa direction en charge des audits, met à jour la liste des PASSI agréés sur son site Internet.

3. Formulaires et supports liés

A. Demande d'agrément de Prestataire d'Audit de Sécurité du Système d'Information (PASSI) : Premier agrément ou renouvellement d'agrément.
B. Attestation d'Agrément.

Demande d'agrément de PASSI

1. Nature de la demande

☐ Premier agrément ☐ Renouvellement d'agrément

2. Spécialité d'agrément demandé

	Agrément en audit organisationnel et physique (A1)
	Agrément en audit de code sources (A2)
	Agrément en audit d'architecture (A3)
	Agrément en audit de configuration (A4)
	Agrément de tests d'intrusion (A5)

Cochez la spécialité ou les spécialités d'audit relatives à la demande d'agrément.

3. Identification du demandeur

3.1 Identité de la société

Dénomination sociale	
Secteur d'activité	
Identifiant fiscal	
Date de création	
Journal Officiel	N°_____du__/__/_____
N° RCCM	
Nombre du personnel	

3.2 Identité du représentant légal

Nom et prénom :_____Nationalité : _____

Fonction :_____Date et lieu de naissance : _____

Carte d'identité n° :_____délivrée le __/__/_____à_____

Téléphone fixe :_____Tél. Portable : _____

Email : _____

3.3 Coordonnées de la société

Adresse postale	
Téléphone	
Fax	
Site Web	
Email	

Je déclare, sur l'honneur, que les renseignements fournis dans ce présent dossier de candidature[1] sont exacts.

Date, Signature et Cachet

[1] *Toute fausse déclaration sera considérée comme une enfreinte grave aux règles déontologiques et entraînera la prise des sanctions appropriées.*

ARTCI

AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

Enregistré sous le numéro : _____

Date de fin de validité : __/__/_____

Le Directeur Général de l'Autorité de Régulation des Télécommunications de Cote d'Ivoire, atteste que *[Indiquer la dénomination sociale du PASSI]* sis au *[Indiquer l'adresse complète]*, représenté par, Mr/Mme *[Nom et prénom du représentant légal]*, inscrit au Registre de Commerce et du Crédit Mobilier sous le numéro [_____] *et dont le matricule fiscal est [_____]*, est agrée en tant que **Prestataire d'Audit de Sécurité du Système d'Information** spécialisé dans [_____*Indiquer la ou les spécialité (s) d'audit*].

Le Directeur Général de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire

Date d'émission

REFERENTIEL D'AUDIT ET DE CERTIFICATION DES SYSTEMES D'INFORMATION

Sommaire

1. Introduction 4
2. Objectif du référentiel 5
3. Audit de la Sécurité des Systèmes d'Information 7
4. Les phases de la mission d'audit de la sécurité des systèmes d'information 10
   4.1 Définition de la charte d'audit 11
   4.2 Préparation de l'audit 11
   4.3 Réunion d'ouverture 11
   4.4 Audit Organisationnel et Physique 11
   4.5 Audit Technique de sécurité 13
      4.5.1 Audit d'architecture du système 13
      4.5.2 Audit de configuration 14
      4.5.3 Audit des vulnérabilités infrastructure et système 14
      4.5.4 Audit applicatif et code source 14
      4.5.5 Tests d'intrusions internes et externes 14
   4.6 Synthèse, plan d'action et recommandations 15
   4.7 Sensibilisation post-audit (optionnelle) 16
   4.8 Clôture de l'audit 16
   4.9 Revue des rapports et approbation par l'ARTCI 17
   4.10 Assistance et suivi Post-audit 17
5. Annexes : 18
   5.1 Annexe 1 : Exemplaire plan d'audit 18
   5.2 Annexe 2 : Revue de la documentation du SMSI 18
   5.3 Annexe 3 : Règlement de certification 18
   5.1 Annexe 1 : Exemplaire plan d'audit 19
   5.2 Annexe 2 : Revue de la documentation du SMSI 22
   5.3 Annexe 3 : Règlement de certification 23

Références

Descriptif du Document	
Titre du document :	**ARTCI – Référentiel d'audit et de certification des systèmes d'information**
Version du document :	**1.1**
Statut du document :	**En cours** / Revu / Validé
Auteur :	Autorité de Régulation des Télécommunications de Côte d'Ivoire

Mise à jour		
Version	Date	Motif et nature de la modification
1.0	01 JUIN 2024	Création

1. Introduction

Les attaques informatiques contre les infrastructures critiques de notre pays, sont de plus en plus nombreuses et hautement sophistiqués au point de mettre en danger la sécurité nationale. Cependant, l'altération du système d'information n'est pas toujours le fait de malveillances.

Elle peut être également due aux pannes, accidents ou erreurs humaines qui affectent la disponibilité, la confidentialité, l'intégrité ou la traçabilité de l'information et entrave le bon fonctionnement des systèmes d'information. Une évaluation systématique de la sécurité du système d'information s'impose donc afin de permettre le développement et la mise en œuvre de pratiques de sécurité efficaces.

L'audit de sécurité des systèmes d'information est un moyen d'éprouver et d'évaluer le niveau de sécurité d'un système d'information. Il permet de mettre en évidence les forces, mais surtout les faiblesses du système d'information. Ses conclusions permettent d'identifier des axes d'amélioration, de proposer des recommandations et de contribuer ainsi à l'élévation de son niveau de sécurité en vue notamment de son homologation.

Il devient donc impératif que les personnes morales mettent à jour leur système d'information en procédant à la réalisation d'audits de sécurité SI.

Dans ce contexte, l'ARTCI décrit les mesures de sécurité qui doivent être appliquées par les personnes morales. Ces derniers seront amenés à réaliser un audit de sécurité de leur système d'information afin d'évaluer son niveau de maturité et d'identifier les projets à mettre en œuvre pour se conformer aux réglementations.

Pour l'ARTCI il s'agit d'un enjeu de souveraineté nationale. En effet, elle a la responsabilité de garantir la sécurité de ses propres systèmes d'information critiques, la continuité d'activité des institutions et des infrastructures vitales pour le bon fonctionnement des activités socio-économiques de notre pays, la protection des entreprises et des citoyens.

De leur côté, les entreprises doivent protéger de la concurrence et de la malveillance leur système d'information qui supporte l'ensemble de leur patrimoine (propriété intellectuelle et savoir-faire) et porte leur stratégie de développement.

L'ARTCI décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les administrations publiques et privées ainsi que les infrastructures d'importance vitale.

L'ARTCI a élaboré ce référentiel pour traiter la démarche à mener afin de réaliser un audit de sécurité des systèmes d'information, et adopter une démarche cohérente et homogène pour la mise en conformité de la sécurité des systèmes d'information avec les règles de sécurité.

Ce référentiel (ou guide) d'audit et de certification des systèmes d'information définit les règles, les procédures et la démarche pour l'audit de sécurité en vue de la certification.

2. Objectif du référentiel

2.1 Objectif global

L'objectif de ce document est double. D'une part, permettre aux organismes de bien définir leurs besoins en termes d'audit afin de rédiger d'éventuels appels d'offres. D'autres part, lister les exigences relatives aux prestataires d'audit permettant de garantir à l'organisme audité la compétence des auditeurs et la pertinence de leurs recommandations, ainsi que la qualité des audits effectués.

Une mission d'audit de sécurité ne permet que de trouver les vulnérabilités liées au Système d'Information et de proposer des actions correctives à travers un ensemble de vérifications et de contrôles. A l'issue de la mission, le prestataire d'audit livre un rapport détaillé pour mettre en évidence les écarts et les non-conformités trouvés. Un plan d'action contenant les mesures à mettre en œuvre par priorité est établi, partagé et validé avec l'organisme audité.

Il faut faire une distinction entre l'audit et l'analyse de risques. Cette dernière permet d'apprécier les risques identifiés liés à la sécurité afin de les traiter (accepter, transférer, éviter, réduire, etc.). Le risque est un concept dynamique qui dépend de la menace, de la vulnérabilité, de l'impact (sur la disponibilité, confidentialité, intégrité) et de la probabilité d'occurrence.

L'objectif de ce document est d'expliquer la norme ivoirienne en matière de sécurité des systèmes d'information et comment assurer l'application du référentiel général de sécurité des systèmes d'information (RGSSI).

Pour la certification de leurs systèmes d'information, les entreprises doivent, se conformer à la norme ivoirienne en matière de sécurité des systèmes d'information et appliquer le RGSSI.

Ce référentiel comprend les contrôles de sécurité nécessaires pour la certification d'un système de gestion de la sécurité et que l'auditeur est appelé à vérifier lors de la mission d'audit. Il détaille les critères par rapport auxquels l'audit est réalisé conformément aux exigences des lois et ses décrets applicatifs.

Le présent document est un document de référence pour :

- L'ARTCI, garant de la qualité des missions d'audit, pour la validation des rapports d'audit et la certification des systèmes d'information,
- Les auditeurs qui réalisent les missions d'audit pour les accompagner à conduire la mission conformément aux exigences du présent référentiel ;
- Les audités, bénéficiaires de la mission d'audit, pour assurer un meilleur suivi de ladite mission ;

Le référentiel d'audit et de certification des systèmes d'information (RACSI) constitue un des composants du cadre normatif pour la sécurité des systèmes d'information en Côte d'Ivoire.

Le schéma général du cadre normatif, ci-dessous, présente la structure dudit cadre à trois piliers et ses implications sur les différents intervenants : ARTCI, organismes audités, prestataires d'audit en sécurité des systèmes d'information et auditeurs en sécurité des systèmes d'information.

2.2 Procédure d'audit

La figure ci-dessous présente la procédure liée aux activités types pour l'audit de sécurité conduite par l'ARTCI, sur la base des recommandations de la norme internationale ISO 19011.

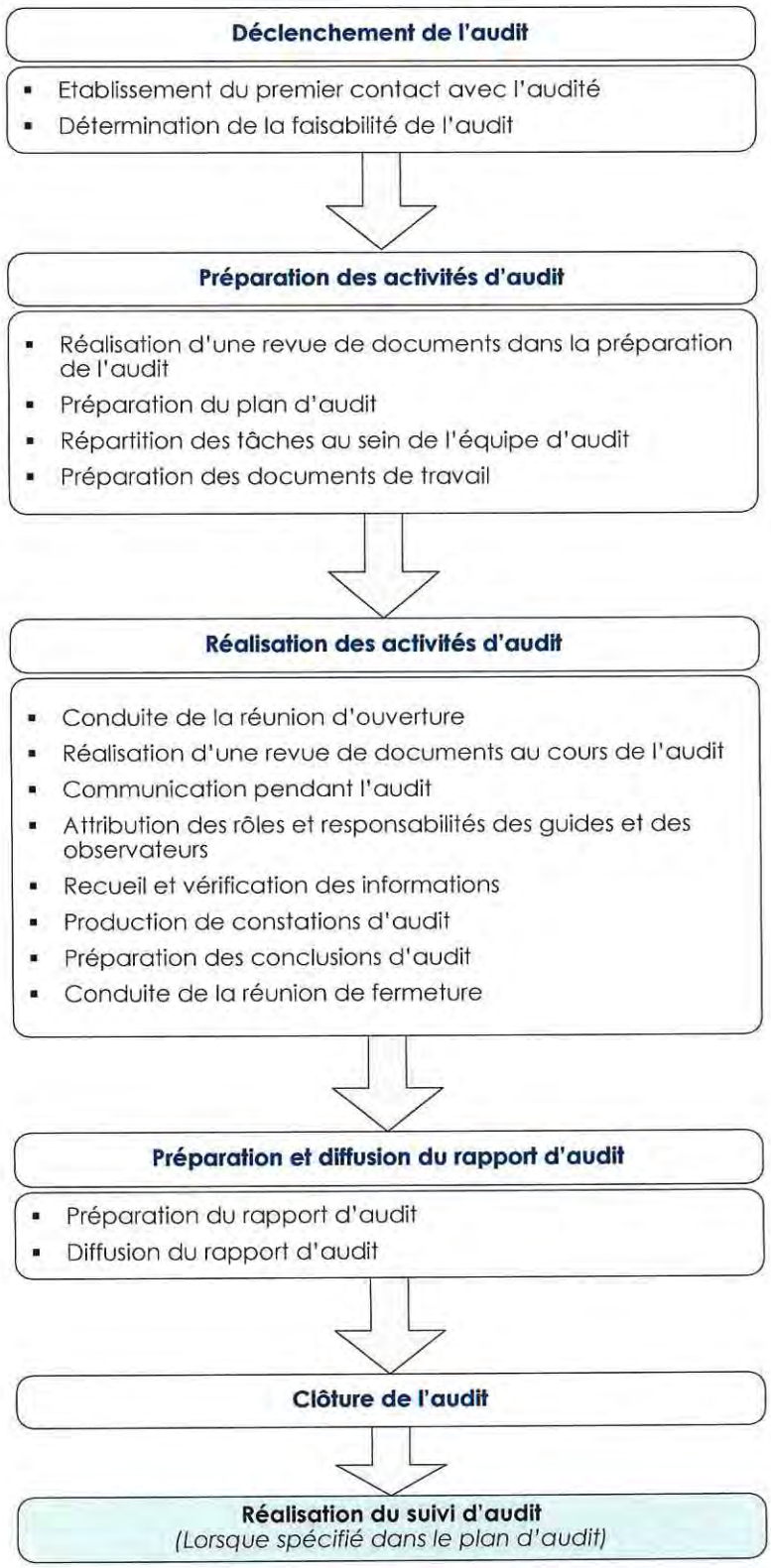


Figure 1 : Activités typiques au cours d'un audit SSI (source : norme ISO 19011)

3. *Audit de la Sécurité des Systèmes d'Information*

3.1 Introduction

On appelle sécurité de l'information, l'ensemble des moyens techniques, organisationnels, juridiques, et humains mis en place pour faire face aux risques identifiés, afin d'assurer la confidentialité, l'intégrité, la disponibilité, et la traçabilité de l'information traitée :

- **Confidentialité** : l'information ne doit pas être divulguée à toute personne, entité ou processus non autorisé. En clair, cela signifie que l'information n'est consultable que par ceux qui ont le droit d'y accéder (on dit aussi « besoin d'en connaître »).
- **Intégrité** : le caractère correct et complet des actifs doit être préservé. En clair, cela signifie que l'information ne peut être modifiée que par ceux qui en ont le droit.
- **Disponibilité** : l'information doit être rendue accessible et utilisable sur demande par une entité autorisée. Cela veut dire que l'information doit être disponible dans des conditions convenues à l'avance (soit 24h/24, soit aux heures ouvrables, etc.).
- **Traçabilité** (ou « *Preuve* ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

3.2 Concepts généraux relatifs aux audits de Sécurité SI

L'audit selon la norme ISO 19011 _ 2011 est « un processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits ». En ce qui concerne le domaine de la sécurité des systèmes d'information (SSI), l'audit permet de mettre en évidence les faiblesses et les vulnérabilités organisationnelles et/ou techniques du système d'information et de déterminer des axes d'amélioration visant à augmenter le niveau de sécurité.

Pour mener un programme d'audit, il convient de bien définir les besoins, le périmètre, ainsi que l'implication des différents acteurs concernés.

3.3 Objectifs des audits de sécurité SI

Un audit de sécurité SI peut être réalisé pour répondre à des besoins différents, notamment :

- Evaluer le niveau de maturité du SI en termes de sécurité pour donner suite à la demande du commanditaire d'audit;
- Vérifier l'efficacité de la politique de sécurité du SI mise en place ;
- Tester l'installation d'un nouvel élément dans le SI;
- Analyser et réagir à la suite d'une attaque;
- Tester la résistance du SI par la simulation des attaques dans des conditions réelles ;
- Se certifier (par exemple ISO 27001);

Une mission d'audit de sécurité SI ne permet que de trouver les vulnérabilités liées au SI et de proposer des actions correctives à travers un ensemble de vérifications et de contrôles. A l'issue de la mission, le prestataire d'audit livre un rapport détaillé pour mettre en évidence les écarts et les non-conformités

trouvés. Un plan d'action contenant les mesures à mettre en œuvre par priorité est établi, partagé et validé avec l'organisme audité.

Il faut faire la distinction entre l'audit et l'analyse de risques. Cette dernière permet d'apprécier les risques identifiés liés à la sécurité afin de les traiter (accepter, transférer, éviter, réduire, etc.). Le risque est un concept dynamique qui dépend de la menace, de la vulnérabilité, de l'impact (sur la disponibilité, confidentialité, intégrité) et de la probabilité d'occurrence.

3.4 Classification des audits

Les audits peuvent être classifiés en trois catégories :

- **Les audits internes** (appelés aussi audits de 1ère partie) sont réalisés pour les organismes souhaitant que leur système d'information soit examiné par rapport à des exigences de sécurité de système d'information. Ces audits sont établis par des auditeurs internes ou externes à l'organisme.

- **Les audits externes** (appelés aussi audits de 2ème partie) sont commandités par des entités ayant un intérêt à l'égard de l'organisme audité, dans le but d'évaluer le niveau de sécurité du système d'information de ce dernier. Ces audits sont établis par des organismes d'audit externes.

- **Les audits de certification** (appelés aussi audits de tierce partie) sont réalisés pour les organismes qui souhaitent faire reconnaître que la sécurité de leur système d'information est conforme aux exigences comme celles de l'ISO/CEI 27001. Ces audits sont établis par des organismes externes généralement accrédités.

3.5 Référentiels relatifs à la sécurité des Systèmes d'Information

Les référentiels de la sécurité des systèmes d'information constituent l'ensemble des normes, des méthodes et de bonnes pratiques permettant de fournir un moyen d'assurance d'une démarche sécuritaire cohérente. Parmi ces référentiels et méthodes, on peut citer :

- **Référentiel général de sécurité des systèmes d'information (RGSSI) :** élaboré par l'ARTCI, il décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les administrations publiques et privées ainsi que les infrastructures d'importance vitale. Ce référentiel, constitue aujourd'hui la première référence nationale qui fixe les objectifs et les règles de la sécurité des systèmes d'information.
- **La suite ISO/CEI 27000** : La suite ISO/CEI 27000 (connue sous le nom de Famille des standards SMSI ou ISO27k) comprend les normes de sécurité de l'information publiées par l'organisation internationale de normalisation (ISO) et la Commission Electrotechnique Internationale (CEI).

- **L'ISO/IEC 27001** : Intitulée « Systèmes de gestion de sécurité de l'information – Exigences », elle a été publiée en octobre 2005 et révisée en 2022. Cette norme spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information (SMSI) au sein d'une organisation.

- **L'ISO/IEC 27002** : Intitulée « Code de bonnes pratiques pour la gestion de la sécurité de l'information », elle a été publiée en 2005 et révisée en 2022. L'ISO/CEI 27002 est un ensemble de mesures dites de bonnes pratiques, destinées à être utilisées par tous les responsables de la mise en place ou du maintien d'un SMSI.

- **L'ISO/IEC 27005** : Publiée en 2008 et révisée en 2022, L'ISO/CEI 27005 est une norme de gestion des risques de la Sécurité des Systèmes d'Information.

- **L'ISO 27006** : Cette norme a été remise à jour en 2011. Elle a pour objectif de fournir les exigences pour les organismes procédant à l'audit et à la certification des SMSI.

- **CobiT (Control Objectives for Information and Related Technology)** : Le référentiel CobiT a été développé par l'ISACA. Il fournit des indicateurs, des processus et des bonnes pratiques pour aider les gestionnaires, les auditeurs et les utilisateurs à aligner le système d'information sur les besoins et la stratégie de l'organisme et à élaborer la gouvernance et le contrôle.

- **ITIL (Information Technology Infrastructure Library)** : La bibliothèque ITIL est un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information. C'est un référentiel très large qui aborde des sujets différents tel que l'organisation, l'amélioration et l'augmentation de la qualité de service.

- **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)** : Créée par l'Agence Française de la Sécurité des Systèmes d'Information (ANSSI), cette méthode permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information conformément à la norme ISO : IEC 27005. Elle permet également de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'organisme et des vulnérabilités liées à son SI.

- **MEHARI (Méthode Harmonisée d'Analyse de Risques)** : Développée et proposée par CLUSIF (Club de la Sécurité de l'Information Français), est une méthode d'évaluation et de management des risques liés aux systèmes d'in- formation. Elle est conforme aux exigences de la norme ISO/IEC 27005.

- **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation) : Produite par l'Institut d'ingénierie logiciel de l'université Carnegie Mellon de Pittsburgh aux USA en 1999. C'est une méthode qui permet d'identifier et d'évaluer les risques de sécurité associés aux systèmes d'information.

4. Les phases de la mission d'audit de la sécurité des systèmes d'information

L'audit de la sécurité du système d'information représente une activité complexe qui couvre l'ensemble des composants du système d'information. Il consiste à évaluer le niveau de sécurité et à proposer les moyens de correction adaptés. Cette évaluation concerne les domaines suivants :

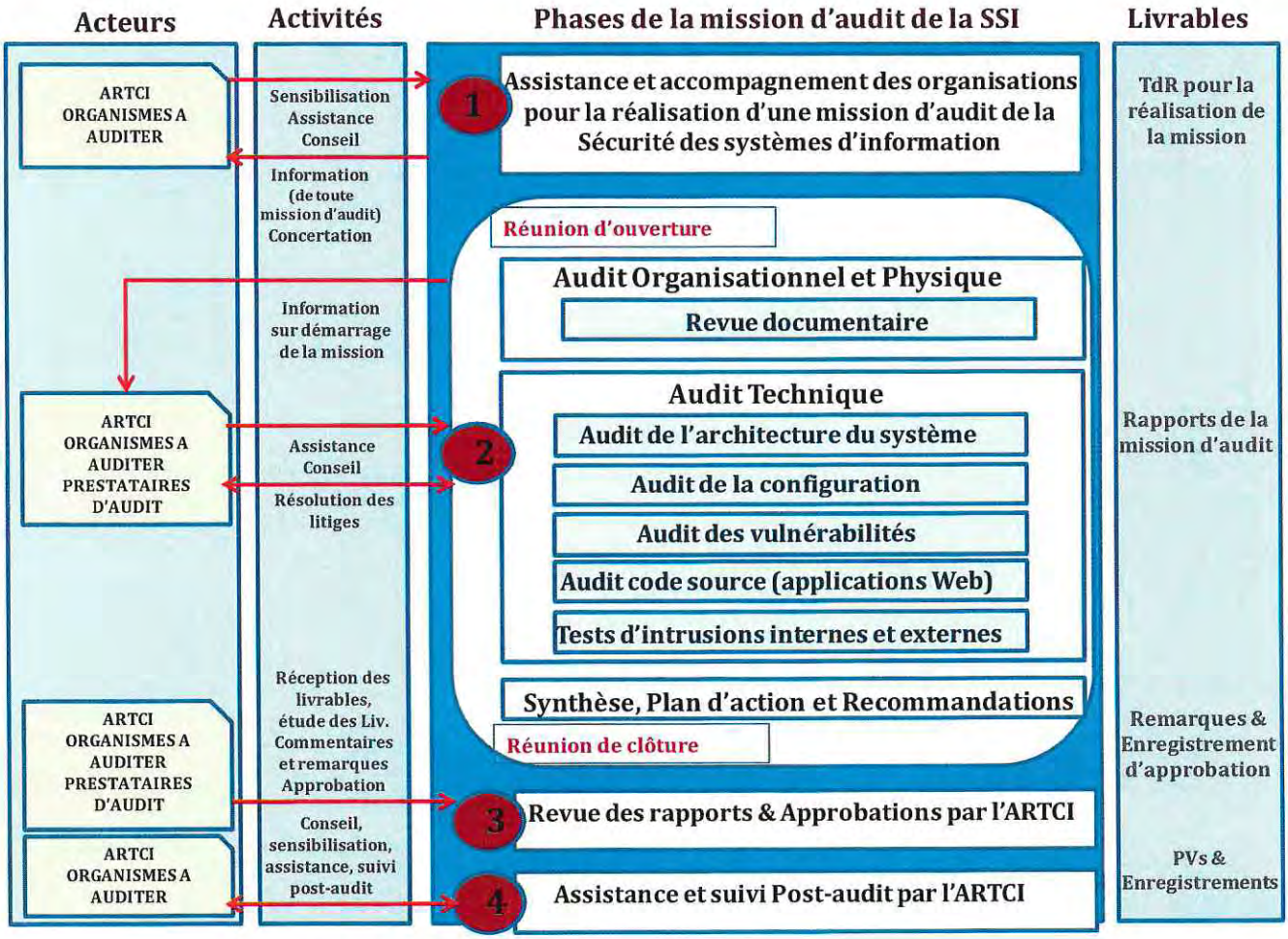


Figure 2 : Schéma général (synthétique) de la mission d'audit SSI

4.1 Définition de la charte d'audit

Avant de procéder à une mission audit, une charte d'audit doit être réalisée, elle a pour objet de définir la fonction de l'audit, les limites et modalités de son interventions, ses responsabilités ainsi que les principes régissant les relations entre les auditeurs et les audités. Elle fixe également les qualités professionnelles et morales requises des auditeurs.

4.2 Préparation de l'audit

Cette phase est aussi appelée phase de pré audit. Elle constitue une phase importante pour la réalisation de l'audit sur terrain. En effet, c'est au cours de cette phase que se dessinent les grands axes qui devront être suivis lors de l'audit sur terrain.

Elle se manifeste par des rencontres entre auditeurs et responsables de l'organisme à auditer. Au cours de ces entretiens, les attentes des responsables vis-à-vis de l'audit devront être exprimées. Aussi, le planning de réalisation de la mission de l'audit doit être fixé.

Les personnes qui seront amenées à répondre au questionnaire concernant l'audit organisationnel doivent être également identifiées. L'auditeur (ou les auditeurs) pourrait également solliciter les résultats des précédents audits. Cette phase sera suivie par l'audit organisationnel et physique.

4.3 Réunion d'ouverture

L'exécution de l'audit commence par une réunion d'ouverture tenue entre les deux acteurs (l'organisme audité et le prestataire). Toute fois l'ARTCI pourrait y assister. Le but de cette réunion est de valider le plan d'audit préétablit, exposer le planning prévisionnel de l'audit, présenter les activités d'audit qui seront menées, confirmer les circuits de communication, et fournir des clarifications sur les éventuelles ambiguïtés existantes. A la suite de cette réunion, un compte rendu doit être rédigé.

Les livrables de cette phase :

- Plan d'assurance qualité;
- Note de cadrage;
- Planning prévisionnel.

4.4 Audit Organisationnel et Physique

L'audit organisationnel et physique permet de faire un état des lieux complet de la sécurité du système d'information et d'en identifier les dysfonctionnements et les risques. Il permet ainsi de couvrir l'ensemble du système d'information de l'organisme et de détecter les carences liées aux différents processus de gestion et d'organisation de la sécurité.

Durant cet audit, les éléments suivants peuvent être abordés :

- ***Politiques de sécurité de l'information :***

Cette section met l'accent sur la nécessité de la mise en place, et révision régulière d'une politique de sécurité de l'information.

- ***Organisation de la sécurité de l'information :***

Cette section définit un cadre de gestion et d'approbation de la politique de sécurité, et traite les aspects contractuels liés à la sécurisation des accès au système d'information par les tiers.

- ***Sécurité des ressources humaines :***

Cette section donne des recommandations pour réduire le risque d'erreur ou de fraude favorisant la formation et la sensibilisation des utilisateurs sur les menaces affectant la sécurité de l'information, ainsi que les comportements à adopter pour protéger l'information.

- ***Gestion des actifs :***

Cette section décrit la nécessité d'inventorier et de classifier les actifs informationnels de l'organisme, dans le but d'identifier les besoins et le niveau de protection adapté à ces actifs.

- ***Contrôle d'accès :***

Cette section définit les mesures pour gérer et contrôler les accès à l'information afin d'assurer la protection des systèmes en réseau. Elle couvre également la sécurité de l'information lors de l'utilisation d'appareils mobiles.

- ***Cryptographie :***

Cette section traite les mesures visant à protéger la confidentialité et l'intégrité de l'information par des moyens cryptographiques.

- ***Sécurité physique et environnementale :***

Cette section définit les mesures pour protéger les lieux et les locaux de l'organisme contre les accès non autorisés, et pour minimiser les dommages causés par les menaces environnementales. Elle traite également la sécurité des matériels afin de réduire les menaces liées aux risques de vol, et de fuites d'information.

- ***Sécurité liée à l'exploitation :***

Cette section définit les mesures permettant d'assurer une exploitation correcte et sécurisée des moyens de traitement de l'information (protection contre les logiciels malveillants, maitrise des logiciels en exploitation, et gestion des vulnérabilités techniques).

- ***Sécurité des communications :***

Cette section définit les mesures d'une part, pour assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient, et d'autre part, pour maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.

- ***Acquisition, développement et maintenance des systèmes d'information :***

Cette section traite les spécifications requises pour assurer la sécurité des systèmes d'information tout au long de leur cycle de vie.

- ***Relations avec les fournisseurs :***

Cette section définit les mesures permettant de gérer les prestations de service assurées par des tiers.

- ***Gestion des incidents liés à la sécurité de l'information :***

Cette section met l'accent sur la nécessité de la mise en place des procédures pour la détection et le traitement des incidents de sécurité.

- ***Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité :***

Cette section décrit les mesures pour mettre en œuvre un plan de continuité de l'activité qui vise à minimiser les impacts causés par les catastrophes naturelles et les pannes matérielles sur l'organisme, afin d'assurer une reprise dans les meilleurs délais.

- ***Conformité :***

Cette section traite le respect des réglementations et des obligations légales, ainsi que la conformité des procédures et des mesures de sécurité mises en place avec la politique et les normes de sécurité.

L'audit organisationnel et physique permet de procéder à la vérification de la conformité et de la pertinence des mesures déployées par rapport à la politique de sécurité de l'organisme, à un référentiel, à une norme ou à des procédures. D'une manière générale, il convient de définir les référentiels de

sécurité à respecter lors de l'audit en tenant compte des exigences et des attentes des responsables de l'organisme audité.

Cependant, les administrations publiques et privées et les infrastructures d'importance vitale doivent s'assurer à minima de la conformité de leur système d'information avec le RGSSI.

Pour mener à bien cette phase, une analyse de risques doit être menée. Il convient de choisir la méthode la plus adaptée au contexte selon les besoins de l'organisme ou suivre une démarche personnalisée et simplifiée.

L'audit organisationnel et physique est considéré comme étant un audit de premier niveau, il ne s'agit pas d'une analyse technique profonde, mais plutôt d'un exercice de questions/réponses.

En effet, cette phase repose sur l'utilisation de questionnaires adaptés au contexte de l'organisme audité, des interviews, ainsi que sur l'analyse des ressources et des documents fournis.

4.5 Audit Technique de sécurité

L'audit technique de sécurité est une évaluation permettant d'analyser en profondeur le système d'information (systèmes, applications, composants et équipements actifs de l'infrastructure réseau, réseaux d'accès interne, réseaux d'interconnexion, etc.) pour identifier les vulnérabilités techniques éventuelles.

4.5.1 Audit d'architecture du système

Cette activité d'audit a pour vocation d'analyser l'architecture du système existant afin de déterminer les éléments pouvant nuire à la sécurité. Elle consiste à étudier la topologie du réseau, ainsi que les hôtes et les équipements d'interconnexion. L'audit d'architecture repose sur l'analyse de la documentation du réseau et la réalisation des sondages en utilisant des outils de traçage et de découverte. L'objectif étant de s'assurer du respect des bonnes pratiques et des recommandations en matière de sécurité quant à l'emplacement des actifs réseaux et sécurité pare-feu, pare-feu applicatif, sondes, proxy, relais anti-virus, relais messagerie, etc.), le cloisonnement, l'échange des flux, les réseaux sans fil, etc.

- L'audit d'architecture peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

- L'audit d'architecture ne peut pas être dissocié de l'audit de configuration car il permet de traiter les points névralgiques de l'architecture du système d'information.

4.5.2 Audit de configuration

L'audit de configuration repose sur une évaluation technique de la configuration des composants du système d'information afin de s'assurer que les mesures de sécurité déployées respectent les bonnes pratiques en matière de sécurité. Les audits de configuration peuvent s'effectuer sur tout type d'élément informatique (équipements réseaux, systèmes d'exploitation, logiciels, applications, bases de données, etc.) en utilisant des outils appropriés d'analyse de configuration.

4.5.3 Audit des vulnérabilités infrastructure et système

L'objectif de l'audit des vulnérabilités infrastructure et système est de réaliser les tests permettant de ressortir les faiblesses et les failles techniques sur les systèmes, les applications et les équipements réseaux. Il permet ainsi de proposer un plan de remédiation avec des actions correctives. L'audit des vulnérabilités se déroule en deux phases :

- Phase de découverte des vulnérabilités : cette phase consiste à effectuer des tests automatisés à l'aide d'outils spécifiques qui s'appuient en général sur une base de failles connues (scanners des vulnérabilités systèmes, scanners des vulnérabilités applicatives et web, etc.) pour détecter les éventuelles vulnérabilités du système d'information.
- Phase d'analyse des vulnérabilités : cette phase consiste à analyser les vulnérabilités identifiées lors de la première phase afin de proposer les actions de remédiation en cohérence avec les pratiques et les exigences de sécurité adoptées au sein de l'organisme audité.

4.5.4 Audit applicatif et code source

L'audit applicatif permet d'évaluer le niveau de sécurité des applications déployées au niveau du système d'information de l'organisme audité. Cet audit peut se faire selon plusieurs approches dont l'audit du code applicatif qui consiste à examiner les vulnérabilités liées au code source d'une application. Cette activité exige l'implication d'un auditeur expert du langage de programmation utilisé dans le développement de l'application.

4.5.5 Tests d'intrusions internes et externes

Le concept des tests d'intrusion repose sur l'exploitation des failles identifiées afin de mesurer l'impact réel sur la sécurité du système d'information de l'organisme audité. Ces tests simulent des scénarios d'attaques préparés à l'avance dans des conditions réelles. L'objectif est de tester la résistance du système d'information aux attaques informatiques provenant de l'intérieur ou de l'extérieur du réseau de l'organisme (ex : réseau internet).

- **Les tests d'intrusion externes :** permettent d'évaluer la capacité d'un attaquant externe à pénétrer le réseau interne de l'organisme audité ;
- **Les tests d'intrusion internes :** permettent d'évaluer l'impact d'un acte malveillant mené de l'intérieur du réseau de l'organisme audité.

ARTCI

AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

REFERENTIEL D'EXIGENCES RELATIF À L'AGREMENT DES PRESTATAIRES D'AUDIT DE LA SECURITE DES SYSTEMES D'INFORMATION

Sommaire

1. Introduction 3
2. Définitions 4
3. Activités visées par le référentiel 5
3.1 Audit Organisationnel et Physique 5
3.2 Audit Technique de sécurité 5
3.2.1 Audit d'architecture du système 5
3.2.2 Audit de configuration 5
3.2.3 Audit de code source 6
3.2.4 Tests d'intrusion 6
4. Les exigences relatives aux prestataires d'audit 6
4.1 Exigences générales 6
4.2 Charte d'éthique 7
4.3 Exigences relatives à la gestion des ressources et des compétences 7
4.4 Protection de l'information 8
5. Les exigences relatives aux auditeurs du prestataire d'audit 8
5.1 Exigences d'ordre général : Aptitudes et engagements 8
5.2 Formation et expérience 9
6. Les exigences relatives au déroulement de la prestationd'audit 9
6.1 Etablissement de la convention 9
6.1.1 Méthodes de la prestation 10
6.1.2 Organisation 10
6.1.3 Responsabilités 11
6.1.4 Confidentialité 11
6.1.5 Lois et réglementations 12
6.1.6 Livrables 12
6.1.7 Agrément 12
6.2 Préparation et déclenchement de la prestation 12
6.3 Exécution de la prestation 13
6.4 Restitution 14
6.4.1 Synthèse, plan d'action et recommandations 14
6.4.2 Sensibilisation post-audit (optionnelle) 15
6.5 Elaboration du rapport et clôture d'audit 15
Annexe : Code déontologique des PASSI 17

Références

Descriptif du Document	
Titre du document :	**ARTCI – Référentiel d'exigences des PASSI**
Version du document :	**1.0**
Statut du document :	**En cours** / Revu / Validé
Auteur :	Autorité de Régulation des Télécommunications de Côte d'Ivoire

Mise à jour		
Version	Date	Motif et nature de la modification
1.0	01 JUIN 2024	Création

1. Introduction

1.1 Objet du document

Selon les dispositions du décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information, les organismes relevant du secteur public ainsi que les entreprises du secteur privé se trouvant sur le territoire national, doivent faire auditer régulièrement leurs systèmes d'information par des prestataires de services d'audit agréés par l'Autorité de Régulation des télécommunications de Côte d'Ivoire (ARTCI).

Ce document constitue donc un référentiel d'exigences applicables à un prestataire d'audit de la sécurité des systèmes d'information (PASSI) délivrant des prestations d'audit organisationnel et physique, d'audit de code source, d'audit de l'architecture, d'audit de configuration et de tests d'intrusion, ci-après dénommé «le prestataire ».

Ce document peut être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Il a vocation à permettre le contrôle et l'agrément des PASSI.

Ce système d'agrément est un gage de confiance dans la délégation des missions d'audit à des prestataires agréés. Il repose sur la vérification d'un certain nombre de critères de preuve, notamment :

- les références de prestataires dans le domaine ;
- la qualification de ses ressources humaines ;
- l'efficacité et l'adéquation des méthodes et outils utilisés ;
- l'organisation du travail et le respect des règles d'éthique et de sécurité.

Il n'exclut ni l'application de la législation et de la réglementation nationale, ni l'application des règles générales (le Référentiel Général de Sécurité des Systèmes d'Information, le Référentiel d'Application du Référentiel Général de Sécurité des Systèmes d'Information et le Référentiel d'Audit et de Certification des Systèmes d'Information) imposées aux prestataires en leur qualité de professionnels et notamment leur devoir de conseil vis-à-vis des audités.

1.2 Structure du document

Le titre (1) correspond à l'introduction du présent référentiel.

Le titre (2) décrit les définitions mentionnées par le présent

référentiel.

Le titre (3) décrit les activités visées par le présent référentiel.

Le titre (4) présente les exigences relatives aux prestataires.

Le titre (5) présente les exigences relatives aux auditeurs du prestataire.

Le titre (6) présente les exigences relatives au déroulement de la prestation d'audit.

L'Annexe présente le code déontologique des prestataires d'audit de sécurité des systèmes d'information.

2. Définitions

Les définitions ci-dessous s'appuient sur la norme ISO19011 et le décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information.

Agrément des prestataires – autorisation délivrée par l'ARTCI à une personne morale en vue de réaliser des missions d'audit de sécurité.

Analyse des risques – processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque.

Audit– processus périodique, méthodique, indépendant et documenté permettant d'évaluer le niveau de conformité d'un système d'information avec les exigences du référentiel général de sécurité des systèmes d'information.

Audité– organisme(s) responsable(s) de tout ou partie du système d'information audité et faisant appel au service d'audit de la sécurité des systèmes d'information.

Auditeur– auditeur titulaire d'une certification en cybersécurité reconnu par l'ARTCI.

Certificat– attestation formelle, délivrée par l'Autorité compétente prouvant qu'une personne physique ou morale remplit les conditions fixées par le référentiel général de sécurité.

Certification– processus de délivrance d'un certificat.

Constats d'audit– résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

Convention de service– accord écrit entre un audité et un prestataire pour la réalisation de l'activité d'audit de la sécurité des systèmes d'information. Dans le cas où le prestataire d'audit est un organisme privé, la convention d'audit est le contrat.

Critères d'audit– ensemble des référentiels, guides, procédures ou exigences applicables à la sécurité du

système d'information audité.

Périmètre d'audit– environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel l'audit est effectué.

Prestataire d'audit de sécurité des systèmes d'information– en abrégé PASSI, organisme agréé par l'ARTCI qui fournit des prestations d'audits de sécurité des systèmes d'informations conformes aux exigences règlementaires.

Preuves d'audit– enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et sont vérifiables.

Rapport d'audit– document de synthèse élaboré par l'équipe d'audit et remis à l'ARTCI et à l'audité à l'issue de l'audit de sécurité. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

Référentiel– le présent document.

Responsable d'équipe d'audit– personne responsable de l'audit et de la constitution de l'équipe d'audit, en particulier de la complémentarité de leurs compétences.

Risques– probabilité qu'une menace donnée exploite une vulnérabilité occasionnant un impact dommageable sur la disponibilité, l'intégrité et la confidentialité d'un système d'information.

Sécurité des systèmes d'information– processus constituant en la mise en valeur de mesures techniques et organisationnelles visant à assurer qu'un système d'information est capable de résister à des évènements volontaires ou non, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données

stockées ou transmises.

Système d'information– ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

Vulnérabilité– faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces.

3. Activités visées par le référentiel

Ce chapitre présente les différentes activités d'audit traitées dans le présent document et dont les exigences spécifiques associées sont décrites dans le Référentiel d'Audit et de Certification des Systèmes d'Information (RACSI).

Chaque activité d'audit est, par principe, associée à la fourniture d'un rapport d'audit regroupant des recommandations et dont la forme et le contenu sont décrits par le Référentiel d'Audit et de Certification des Systèmes d'Information (RACSI).

3.1 Audit Organisationnel et Physique

L'audit organisationnel et physique permet de faire un état des lieux complet de la sécurité du système d'information et d'en identifier les dysfonctionnements et les risques. Il permet ainsi de couvrir l'ensemble du système d'information de l'organisme et de détecter les carences liées aux différents processus de gestion et d'organisation de la sécurité.

Cet audit vise à s'assurer que :

- Les politiques et procédures de sécurité définies par l'audité pour assurer le maintien en conditions opérationnelles et de sécurité d'une application ou de tout ou partie du système d'information, sont conformes aux besoins de sécurité de l'organisme audité, aux normes en vigueur ;
- Elles complètent correctement les mesures techniques mises en place ;
- Elles sont efficacement mises en pratique ;
- Les aspects physiques de la sécurité de l'application ou du système d'information sont correctement couverts.

3.2 Audit Technique de sécurité

3.2.1 Audit d'architecture du système

L'audit d'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information aux normes en vigueur et aux exigences et règles internes de l'audité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, notamment Internet.

3.2.2 Audit de configuration

L'audit de configuration repose sur une évaluation technique de la configuration des composants du système d'information afin de s'assurer que les mesures de sécurité déployées, respectent les bonnes pratiques en matière de sécurité. Les audits de configuration peuvent s'effectuer sur tout type d'élément informatique (équipements réseaux, systèmes d'exploitation, logiciels, applications, bases de données, etc.)

en utilisant des outils appropriés d'analyse de configuration.

3.2.3 Audit de code source

L'audit de code source consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une application dans le but d'y découvrir des vulnérabilités liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

3.2.4 Tests d'intrusion

Le principe du test d'intrusion est de découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel. Les vulnérabilités testées peuvent également avoir été identifiées au cours d'autres activités d'audit définies dans ce chapitre.

Cette activité d'audit peut être réalisée soit depuis l'extérieur du système d'information audité (notamment depuis internet ou le réseau interconnecté d'un tiers), soit depuis l'intérieur.

Un test d'intrusion seul n'a pas vocation à être exhaustif. Il s'agit d'une activité qui doit être effectuée en complément d'autres activités d'audit afin d'en améliorer l'efficacité ou de démontrer la faisabilité de l'exploitation des vulnérabilités découvertes à des fins de sensibilisation.

Les tests de vulnérabilité, notamment automatisés, ne représentent pas à eux seuls une activité d'audit au sens du référentiel.

4. Les exigences relatives aux prestataires d'audit

4.1 Exigences générales

1) Le prestataire doit être une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation.
2) Le prestataire s'engage à respecter les lois et règlements en vigueur en Côte d'Ivoire.
3) Le prestataire doit décrire l'organisation de son activité d'audit auprès de l'audité.
4) En sa qualité de professionnel, le prestataire a un devoir de conseil envers l'audité.
5) Le prestataire réalise ses audits dans le cadre d'une convention d'audit de sécurité des Systèmes d'Information, préalablement cosignée par les deux parties.
6) Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte de l'audité dans le cadre de la prestation, notamment de tout dommage causé à l'audité.
7) Le prestataire doit protéger au mieux, les informations sensibles relatives à la prestation, notamment les preuves, les constats et les rapports.
8) Le prestataire doit pouvoir apporter la preuve qu'il a évalué les risques résultant de ses activités

d'audit et qu'il a pris les dispositions appropriées pour couvrir les risques résultant de ses prestations d'audit. Il met à disposition de l'audité ces éléments de preuve.

9) Il est, à ce titre, recommandé que le prestataire s'engage à souscrire à une assurance couvrant les dommages éventuellement causés aux systèmes d'information des audités.

10) Le prestataire doit s'assurer du consentement de l'audité, avant toute communication d'informations obtenues ou produites dans le cadre de la prestation.

11) Le prestataire doit garantir que les informations qu'il fournit, ne sont ni fausses ni trompeuses.

12) Le prestataire doit apporter une preuve suffisante que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de ses prestations, ou à donner lieu à des conflits d'intérêts.

13) Le prestataire doit fournir le service de manière impartiale, en toute bonne foi et dans le respect de l'audité, de son personnel et de son infrastructure.

14) Le prestataire doit demander à l'audité de lui communiquer les éventuelles obligations légales et réglementaires spécifiques auxquelles il est soumis, notamment celles relatives à son secteur d'activité.

15) Le prestataire doit informer l'audité que ce dernier est tenu de déclarer tout incident de sécurité au CI-CERT et doit l'accompagner dans cette démarche si ce dernier le lui demande.

16) Le prestataire doit exécuter sa prestation dans le cadre d'une convention formellement approuvée à l'écrit par l'audité, et conforme aux exigences du référentiel d'audit et de certification des systèmes d'information (RACSI).

17) Le prestataire doit être suffisamment indépendant et neutre des éditeurs et des intégrateurs informatiques.

18) Le prestataire doit obligatoirement être conforme au traitement des données à caractère personnel.

4.2 Charte d'éthique

1) Le prestataire doit disposer d'une charte d'éthique prévoyant notamment que :
   - Les prestations sont réalisées avec loyauté, discrétion et impartialité ;
   - Les auditeurs ne recourent qu'aux méthodes, outils et techniques validés par le prestataire ;
   - Les auditeurs s'engagent à ne divulguer aucune information à un tiers, même anonymisée et décontextualisée, obtenue dans le cadre de leurs activités, sauf autorisation de l'audité ;
   - Les auditeurs signalent à l'audité tout contenu manifestement illicite découvert lors la prestation ;
   - Les auditeurs s'engagent à respecter la législation et la réglementation nationale en vigueur ainsi que les bonnes pratiques relatives à leurs activités d'audit.

2) Le prestataire doit faire signer et appliquer la charte d'éthique par ses auditeurs.

4.3 Exigences relatives à la gestion des ressources et des compétences

1) Le prestataire doit employer, à plein temps, au moins un auditeur, pour assurer totalement les activités d'audit pour lesquels il demande d'être agréé ;

2) Le prestataire veille à ce que les compétences des auditeurs soient actualisées dans les types d'audits pour lesquels ils ont obtenu une certification. Pour cela, le prestataire doit disposer d'un

processus de formation continue et permettre à ses auditeurs d'assurer une veille technologique.

3) Le prestataire doit vérifier, en matière de recrutement, les formations, compétences et références professionnelles des auditeurs candidats et la véracité de leur curriculum vitae.
4) Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisées par ses auditeurs et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration, etc.) pour la réalisation de la prestation. Pour cela, le prestataire doit assurer une veille technologique sur leur mise à jour et leur pertinence (efficacité et confiance).
5) Le prestataire doit disposer, éventuellement, des licences valides des outils (logiciels ou matériels) utilisés pour l'exécution de la prestation.
6) Le prestataire justifie, par l'intermédiaire des auditeurs évalués au titre de l'agrément du prestataire, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit et couvrant les domaines détaillés par le Référentiel Général de la Sécurité des Systèmes d'Information (RGSSI).
7) Le prestataire doit s'assurer que les auditeurs ne font pas l'objet d'une inscription au bulletin n°3 du casier judiciaire.
8) Un processus disciplinaire doit être élaboré par le prestataire à l'intention des auditeurs ayant enfreint les règles de sécurité ou la charte d'éthique.

4.4 Protection de l'information

1) Le prestataire doit protéger au mieux les informations sensibles relatives à la prestation, notamment les preuves, les constats et les rapports.
2) Le prestataire doit respecter les règles établies par l'ARTCI relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles.
3) Le prestataire doit appliquer les bonnes pratiques de sécurité de l'information sur son système d'information, dans le cadre du traitement des informations sensibles relatives à la prestation.

5. Les exigences relatives aux auditeurs du prestataire d'audit

5.1 Exigences d'ordre général : Aptitudes et engagements

Chaque auditeur du prestataire doit :

1) Maitriser la réglementation applicable aux activités d'audit qu'il met en œuvre (maitrise de la réglementation spécifique aux types d'audits, au secteur d'activité de l'audité).
2) Maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme ISO19011 représentant la base des exigences du Référentiel d'audit de sécurité et de certification des systèmes d'information (RACSI) de l'ARTCI.
3) Assurer les missions selon son profil et ses compétences : auditeur d'architecture, auditeur de configuration, auditeur de code source, auditeur en tests d'intrusion, auditeur en sécurité organisationnelle et physique.
4) Disposer de qualités rédactionnelles et de synthèse, et savoir s'exprimer à l'oral de façon claire et compréhensible, en français.
5) Actualiser régulièrement ses compétences par une veille active sur la méthodologie, les techniques

ou les outils utilisés lors des activités d'audit.

6) Disposer des compétences de gestion d'équipe nécessaires à la constitution adéquate de l'équipe d'audit par rapport aux objectifs visés dans la convention d'audit.

7) Avoir signé la charte d'éthique élaborée par le prestataire.

8) S'engager à subir une évaluation personnelle de ses compétences au titre de la procédure d'agrément du prestataire dont il dépend.

9) Il est recommandé que l'auditeur soit sensibilisé à l'ensemble des autres activités d'audit pour lesquelles le prestataire demande l'agrément.

5.2 Formation et expérience

1) L'auditeur doit être titulaire d'au moins une licence en informatique ou en télécommunications ou d'un diplôme équivalent.

2) l'auditeur doit disposer :
   - au moins deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
   - au moins une année d'expérience dans le domaine de l'audit ou détenir une certification dans le domaine de l'audit des systèmes d'information

6. *Les exigences relatives au déroulement de la prestation d'audit*

1) La définition du périmètre de la prestation et la description de la prestation attendue, formulées généralement dans un appel d'offres, sont du ressort de l'audité.

2) Le prestataire s'assure que l'audité lui fournit un environnement de travail adapté à ses missions.

3) Le prestataire vérifie que l'audité a correctement identifié le système audité ainsi que ses dépendances externes.

4) Le prestataire s'assure que la prestation est adaptée au contexte et aux objectifs souhaités par l'audité. A défaut, le prestataire en informe l'audité préalablement à la prestation.

5) L'audité doit pouvoir refuser un expert auditeur qui ne disposerait pas des compétences attendues.

6) D'une manière générale, le déroulement de l'audit doit respecter les dispositions du RGSSI et les prescriptions du Référentiel d'Audit de sécurité et de Certification des Systèmes d'Information (RACSI).

6.1 Etablissement de la convention

1) Le prestataire doit établir une convention de service avec l'audité avant l'exécution de la prestation.

2) La convention doit être signée par le représentant légal de l'audité et du prestataire.

6.1.1 Méthodes de la prestation

La convention de service doit :

1) Décrire le périmètre de la prestation, la démarche générale d'audit de sécurité des systèmes d'information, les activités et les modalités de la prestation (objectifs, champs et critères de l'audit, jalons, livrables attendus en entrée, prérequis, etc.) ;
2) Préciser les livrables attendus en sortie, les réunions d'ouverture et de clôture, les publics cibles, leur niveau de sensibilité ou de classification et les modalités associées ;
3) Décrire les moyens techniques (matériel et outils) et organisationnels mis en œuvre par le prestataire dans le cadre de sa prestation ;
4) Décrire les méthodes de communication qui seront employées lors de la prestation entre le prestataire et l'audité ;
5) Prévoir les moyens logistiques devant être mis à disposition du prestataire par l'audité (moyens matériels, humains, techniques, etc.) ;
6) Définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les outils développés spécifiquement par le prestataire dans le cadre de la prestation, les indicateurs de compromission ou le rapport d'audit.
7) Préciser les actions qui ne peuvent être menées sur le système d'information ou sur les informations collectées sans autorisation expresse de l'audité. Le cas échéant, l'accord ou la présence de l'audité, ainsi que les modalités associées (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensibles et des actions autorisées, etc.) doivent également être effectives.
8) Définir les moyens assurant la traçabilité entre l'audité, le prestataire des informations et les supports matériels soumis pour analyse.

6.1.2 Organisation

La convention de service doit :

1) Préciser le nom du correspondant d'audit en charge chez l'audité, et mettre en relationle prestataire avec les différents correspondants impliqués ;
2) Préciser les noms, rôles, responsabilités ainsi que les droits des personnes désignées par le prestataire et l'audité. Cette exigence est d'autant plus importante si l'existence d'un incident de sécurité ne doit pas être divulguée ;
3) Stipuler que le prestataire ne fait pas intervenir d'auditeurs n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique, ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire.

6.1.3 Responsabilités

La convention de service doit stipuler que :

1) Le prestataire ne réalisera la prestation qu'après une autorisation formelle et écrite de l'audité ;
2) Le prestataire informe l'audité en cas de manquement à la convention ;
3) Le prestataire s'engage à ce que les actions réalisées dans le cadre de la prestation restent strictement conforme aux objectifs de la prestation ;
4) l'audité garantit qu'il dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.). l'audité garantit également d'avoir recueilli l'accord des éventuels tiers, notamment de ses prestataires ou de ses partenaires, dont les systèmes d'information entreraient dans le périmètre ;
5) L'audité et le prestataire remplissent toutes les obligations légales et réglementaires nécessaires aux activités d'audit ;
6) L'audité autorise provisoirement (pendant la durée de la mission) le prestataire aux seules fins de réaliser la prestation, à accéder et à maintenir dans tout ou partie du périmètre et d'effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données ;
7) l'audité autorise provisoirement le prestataire à reproduire, collecter et analyser, aux seules fins de l'exécution de la prestation, des données appartenant au périmètre d'audit ;
8) Il est recommandé de définir les responsabilités et les précautions d'usage à respecter par l'ensemble des parties concernant les risques liés à la prestation, en matière de confidentialité des informations collectées et analysées ainsi qu'en matière de disponibilité (déni de service lors du scan de vulnérabilités d'une machine ou d'un serveur par exemple) et d'intégrité du système d'information ciblé ;
9) Si le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés lors de l'exécution des activités d'audit, le cas échéant, préciser la couverture de celle- ci et inclure l'attestation d'assurance.

6.1.4 Confidentialité

La convention de service doit :

1) Prévoir la non-divulgation à un tiers, par le prestataire et par les auditeurs, de toute information relative à l'audit et à l'audité, sauf autorisation écrite ;
2) Stipuler que le prestataire puisse, sauf refus formel et écrit de l'audité, conserver certains types d'informations liées à la prestation une fois celle-ci réalisée. Le prestataire devra identifier ces types d'informations dans la convention (ex : livrables, informations, documents, etc.) ;
3) Stipuler que le prestataire anonymise et décontextualise (suppression de toute information identifiant l'audité, de toute information à caractère personnel, etc.) l'ensemble des informations que l'audité l'autorise à conserver ;
4) Stipuler que le prestataire détruit l'ensemble des informations relatives à l'audité à l'issue de la prestation, à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part de l'audité ;
5) Préciser les modalités (contenu, forme, portée, etc.) de rédaction des recommandations.

6.1.5 Lois et réglementations

La convention de service doit :

1) Être rédigée au moins en français ;
2) Stipuler que seule la version française fait foi, notamment dans le cadre d'un litige ;
3) Stipuler que la législation applicable à la convention de service est la législation ivoirienne ;
4) Préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour se conformer à la législation ivoirienne applicable, notamment celle concernant la protection des données à caractères personnel ;
5) Préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis l'audité, notamment celles liées à son secteur d'activité ;
6) Définir la durée de conservation des informations liées à la prestation, notamment les évènements collectés et les failles de sécurité détectées. Si besoin, une distinction de la durée de

conservation peut être faite en fonction du type d'information. La durée minimale de conservation est de douze mois après la restitution du rapport d'audit, sous réserve de la législation et de la réglementation en vigueur.

Cette conservation s'effectue pour des besoins de contrôle de l'ARTCI.

6.1.6 Livrables

1) La convention doit préciser que tous les livrables produits par le prestataire au titre de la prestation sont fournis en langue française sauf cas contraire sous demande formelle et écrite par l'audité.

6.1.7 Agrément

La convention de service doit :

1) Indiquer que la prestation réalisée est une prestation agréée et inclure l'attestation d'agrément du prestataire ;
2) Indiquer que les auditeurs disposent d'une attestation individuelle de compétence pour les activités d'audit et inclure ces attestations.

6.2 Préparation et déclenchement de la prestation

1) Le prestataire doit désigner un responsable d'équipe d'audit pour tout audit qu'il effectue.

2) Le responsable d'équipe d'audit doit constituer une équipe d'auditeurs ayant les compétences adéquates à la nature de l'audit. Le responsable d'équipe d'audit peut, s'il dispose des compétences suffisantes dans les domaines requis, réaliser l'audit lui-même.

3) Le responsable d'équipe d'audit doit, dès le début de la préparation de l'audit, établir un contact avec l'audité. Ce contact formel, a pour objectif de mettre en place les circuits de communication, de décision et de préciser les modalités d'exécution de la prestation. Le responsable d'équipe d'audit doit également obtenir du correspondant d'audit la liste des points de contact nécessaires à la réalisation de la prestation.

4) Le responsable d'équipe d'audit élabore un plan d'audit. Ce plan d'audit couvre en particulier les points suivants : les objectifs, champs et critères de l'audit, le périmètre technique et organisationnel de la

prestation, les dates et lieux où seront menées les activités d'audit, les informations générales sur les réunions de démarrage et de clôture de la prestation, les auditeurs qui constituent l'équipe d'audit, la confidentialité des données récupérées et l'anonymisation des constats et des résultats.

5) Les objectifs, le champ, les critères et le calendrier de l'audit doivent être définis entre le prestataire et l'audité, en considération des contraintes d'exploitation du système d'information de l'audité. Ces éléments doivent figurer dans la convention d'audit et dans le plan d'audit.

6) En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, au préalable, toute la documentation existante de l'audité (politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, etc.), relative à la cible auditée dans l'objectif d'en faire une revue.

7) L'audit ne doit débuter qu'après une réunion formelle d'ouverture au cours de laquelle les représentants habilités du prestataire et ceux de l'audité confirment leur accord sur l'ensemble des modalités de la prestation. Son but est de :

   i. valider le plan de charge d'audit préétablit,
   ii. exposer le planning prévisionnel de l'audit,
   iii. présenter les activités d'audit qui seront menées,
   iv. confirmer les circuits de communication,
   v. fournir des clarifications sur les éventuelles ambiguïtés existantes.
   vi. Suite à cette réunion, un compte rendu doit être rédigé et signé par les deux parties.

8) Le prestataire doit sensibiliser avant l'audit, l'audité sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées.

9) Au préalable, et dans le cas spécifique des tests d'intrusion, une fiche d'autorisation doit être signée par l'audité et d'éventuelles tierces parties. Elle précise en particulier :
   a. la liste des cibles auditées (adresses IP, noms de domaine, etc.) ;
   b. la liste des adresses IP de provenance des tests ;
   c. la date et les heures exclusives des tests ;
   d. la durée de l'autorisation.

10) Les livrables de cette phase :
   a. le plan d'assurance qualité ;
   b. la note de cadrage ;
   c. le planning prévisionnel.

6.3 Exécution de la prestation

1) Le responsable d'équipe d'audit doit tenir informé l'audité des vulnérabilités critiques découvertes au cours de l'audit. Il doit rendre compte immédiatement à l'audité de tout élément constaté présentant un risque immédiat et significatif, et dans la mesure du possible, lui proposer des mesures permettant de lever ce risque.

2) L'audit doit être réalisé dans le respect du personnel et des infrastructures physiques et logiques de l'audité.

3) Les constatations et observations effectuées par les auditeurs doivent être factuelles et basées sur la preuve.

4) Les auditeurs doivent rendre compte des constats d'audit au responsable d'équipe d'audit, lequel peut en avertir sur-le-champ sa hiérarchie et l'audité, dans le respect des clauses de confidentialité mentionnées dans la convention d'audit.

5) Toute modification effectuée sur le système d'information audité, durant l'audit, doit être tracée, et en fin d'audit, le système d'information concerné doit retrouver un état dont la sécurité n'est pas dégradée par rapport à l'état initial.

6) Les constats d'audit doivent être documentés, tracés, et conservés, par le prestataire, durant toute la durée de l'audit.

7) Le prestataire et les auditeurs doivent prendre toutes les précautions utiles pour préserver la confidentialité des documents et informations relatives à l'audité.

8) Les actions et résultats des auditeurs du prestataire sur le système d'information audité, ainsi que leurs dates de réalisation, devraient être tracés. Ces traces peuvent par exemple servir à identifier les causes d'un incident technique survenu lors de l'audit.

9) Lorsqu'elles sont demandées par l'audité, les activités d'audit réalisées par le prestataire doivent être conformes aux exigences précisées par le référentiel d'audit et de certification des systèmes d'information (RACSI).

6.4 Restitution

1) Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, le responsable d'équipe d'audit doit informer l'audité des constats et des premières conclusions de l'audit.

2) Le cas échéant, ceux-ci présentent les vulnérabilités majeures et critiques qui nécessiteraient une action rapide et décrivent les recommandations associées.

6.4.1 Synthèse, plan d'action et recommandations

1) Les documents résultant de la phase d'exécution doivent être soigneusement archivés. Ces documents se déclinent comme suit :
   - Les comptes rendus validés et signés par les interlocuteurs de l'organisme audité ;
   - Les fiches de constat dûment remplies. Une fiche de constat comporte essentiellement :
     - les constats des auditeurs ;
     - les recommandations ;
     - les engagements et/ou actions proposés par l'organisme audité ;
     - les commentaires des auditeurs relatifs au point précédent.
   - Une grille d'évaluation des niveaux de maturité par rapport aux objectifs de sécurité initialement définis doit être remplie ;
   - Les relevés techniques, à savoir :
     - les fichiers contenant les résultats des scans de sécurité ;
     - le rapport d'analyse des vulnérabilités ;
     - les échantillons du trafic capturé.
   - Les résultats des tests techniques d'audit sont composés principalement de :
     - la liste des vulnérabilités (réseaux, systèmes, applicatives, etc.) ;
     - la liste des anomalies de configuration des équipements (configuration des firewalls et des équipements réseaux).
2) Les enregistrements de la phase d'exécution de l'audit doivent être évalués, analysés et consolidés

par l'équipe d'audit. Cette consolidation est réalisée à travers les actions suivantes :

- présentation des constats fiables et pertinents, formulés clairement, de manière synthétique ;
- validation des conclusions d'audit ;
- préparation des recommandations ;
- définition des modalités de suivi d'audit.

3) Le prestataire d'audit est invité à rédiger un rapport de synthèse sur sa mission d'audit. Cette synthèse doit être révélatrice des défaillances constatées. Autant est-il important de déceler une faille, autant il est également important d'y proposer des solutions. Ainsi, l'auditeur est également invité à donner ses recommandations, pour pallier les défauts qu'il aura constaté.
4) Ces recommandations doivent tenir compte de l'audit organisationnel et physique, ainsi que de celui technique et intrusif.

6.4.2 Sensibilisation post-audit (optionnelle)

1) Le prestataire d'audit est invité à proposer [nombre de sessions] sessions de sensibilisation post-audit, destinées aux responsables et/ou aux acteurs du système d'information.
2) Les sessions post-audit auront pour objectif, une sensibilisation aux failles décelées et aux risques cachés encourus et l'octroi de la collaboration des utilisateurs, pour ce qui concerne la mise en œuvre de la politique de sécurité proposée en spécifiant l'objectif de cette politique et les bienfaits attendus.
3) A la fin de cette opération un procès-verbal sera dressé et signé conjointement par le titulaire et le maitre d'ouvrage et des fiches d'évaluation de ces sessions seront remplies par les participants. Des copies de ce procès-verbal et de ces fiches seront jointes au rapport d'audit.

6.5 Elaboration du rapport et clôture d'audit

1) Le prestataire d'audit doit rédiger le rapport d'audit et doit être responsable de son contenu. Une réunion de clôture de l'audit est prévue pour présenter le rapport d'audit à la Direction de l'organisme audité, pour répondre aux éventuelles questions qui peuvent se poser.
2) Les constats et les conclusions d'audit présentés doivent être bien compris et acceptés par l'audité.
3) Le rapport d'audit doit être émis dans les délais prédéterminés. En cas de retard, il est recommandé de communiquer à l'audité, les raisons du retard et de fixer une date d'émission.

   Le rapport d'audit doit être validé et signé par les deux parties puis transmis à l'ARTCI dans un délai de deux semaines. Il doit également rester confidentiel.
4) La mission d'audit est achevée suite à la réalisation de l'ensemble des actions définies dans le plan de charge d'audit et suite à la réunion de clôture.
5) Livrables de la phase de clôture :
   - Le rapport d'audit de sécurité qui englobe :
     - ✓ Les résultats des différentes activités réalisées
     - ✓ Le plan de recommandations global et les prés requis pour leur mise en œuvre.
     - ✓ Une copie de la convention co-signée
6) Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenus par le prestataire, doivent être restitués à l'audité ou sur sa demande,

détruits conformément au cahier des charges. Le cas échéant, le responsable d'audit produit un procès-verbal de destruction de ces données qu'il remet à l'audité en précisant les données détruites et leur mode de destruction.

Annexe : Code déontologique des PASSI

Préambule

- Article 50 de la loi N°2013-456 du 30 juillet 2013 relative aux transactions électroniques.
- Article 6 du décret N°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information.
- Le Prestataire d'audit de sécurité des systèmes d'information agréé par l'ARTCI (désigné par PASSI) s'engage à respecter les principes et les règles définis dans le présent code déontologique. Le non-respect du présent code peut entraîner à son encontre des mesures qui peuvent aller jusqu'au retrait définitif de l'agrément.

Déontologie générale

a. Le PASSI doit réaliser l'audit de manière loyale, indépendante et impartiale, avec la diligence nécessaire, conformément aux normes professionnelles et dans le respect de l'audité, de son personnel et de ses infrastructures.
b. Le PASSI doit garantir la confidentialité des informations liées aux missions d'audit, à moins qu'une communication ne soit requise par une autorité judiciaire ou une divulgation exigée par l'ARTCI. Ces informations ne doivent pas être utilisées pour en tirer un bénéfice personnel ni communiquées à des tiers non autorisés.
c. Le PASSI assume la responsabilité de l'audit qu'il réalise pour le compte de l'audité, en particulier des dommages éventuellement causés au cours de l'audit.
d. Les auditeurs du PASSI ne recourent qu'aux méthodes, outils et techniques validés.
e. Les auditeurs du PASSI signalent à l'audité tout contenu manifestement illicite découvert durant la prestation.
f. Le PASSI doit prendre en considération les dispositions appropriées pour couvrir les risques résultant de ses prestations d'audit.
g. Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés au mieux. Le traitement de ces données doit être conforme aux normes et standards relatifs à leur classification, sauvegarde et archivage.
h. Le PASSI doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.
i. Un processus disciplinaire doit être élaboré par le prestataire d'audit à l'intention des salariés ayant enfreint les règles de sécurité ou la charte d'éthique.
j. Le PASSI doit informer l'ARTCI de tout changement au niveau de l'état sur lequel il a été agréé (Nombre d'auditeurs, départ, recrutement, etc.).
k. Le PASSI doit veiller au respect de ses confrères et éviter de toucher à leur réputation.
l. Le PASSI est tenu de respecter la législation et la réglementation en vigueur, notamment en matière de traitements de données à caractère personnel, de propriété intellectuelle et de fraude informatique.

Je soussigné_____, le représentant légal du [Dénomination sociale du PASSI__], dont le registre de commerce_____, m'engage à respecter les dispositions du présent code déontologique, et j'assume mes responsabilités face à toute infraction.

Lu et Approuvé, le___/___/_____