PRESIDENCE DE LA REPUBLIQUE

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECRET N° 2021-917 DU 22 DECEMBRE 2021 DEFINISSANT LES PROCEDURES D'AUDIT, DE CONTROLE ET DE CERTIFICATION DES SYSTEMES D'INFORMATION

LE PRESIDENT DE LA REPUBLIQUE,

Sur rapport du Ministre de l'Economie Numérique, des Télécommunications et de l'Innovation,

Vu la Constitution ;

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 l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'ARTCI ;

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 13 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;

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° 2021-176 du 26 mars 2021 portant nomination du Premier Ministre, Chef du Gouvernement ;

Vu le décret n° 2021-181 du 06 avril 2021 portant nomination des Membres du Gouvernement ;

Vu le décret n° 2021-190 du 28 avril 2021 portant attributions des Membres du Gouvernement ;

Vu le décret n°2021-464 du 08 septembre 2021 portant organisation et fonctionnement du Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation ;

LE CONSEIL DES MINISTRES ENTENDU,

DECRETE :

CHAPITRE I : DISPOSITIONS GENERALES

Article 1 : Au sens du présent décret, on entend par :

- **agrément de prestataire,** l'autorisation délivrée par l'ARTCI à une personne morale en vue de réaliser des audits de sécurité conformément aux dispositions du présent décret ;

- **analyse des risques,** le processus systémique consistant à identifier et à estimer les risques auxquels un système d'information est exposé ;

- **audit,** le 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 :** l'organisme responsable de tout ou partie d'un système d'information faisant l'objet d'un audit ;

- **certificat :** l'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 :** le processus de délivrance d'un certificat ;

- **Expert auditeur :** l'auditeur titulaire d'un certificat délivré ou reconnu par l'ARTCI ;

- **prestataire d'Audit de Sécurité des Systèmes d'Information**, en abrégé, **PASSI,** l'organisme agréé par l'ARTCI, qui fournit des prestations d'audits de sécurité des systèmes d'information conformes aux exigences règlementaires ;

- **risque :** la 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, en abrégé SSI,** le processus consistant en la mise en œuvre 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.

Article 2 : Le présent décret a pour objet de définir la procédure d'audit de sécurité, de contrôle et de certification des systèmes d'information.

CHAPITRE II : LES ORGANISMES SOUMIS A L'AUDIT DE SECURITE

Article 3 : Sont soumis à l'audit de sécurité périodique obligatoire :

1. les systèmes d'information de l'Administration et des organismes relevant du secteur public ;

2. les systèmes d'information des organismes et entreprises relevant du secteur privé et se trouvant sur le territoire national, notamment :

- les entreprises de Télécommunications/TIC ;
- les fournisseurs de services de télécommunications et d'Internet ;
- les entreprises dont les systèmes d'information sont connectés à travers des réseaux publics de télécommunications ;
- les entreprises qui procèdent au traitement automatisé des données à caractère personnel de leurs clients dans le cadre de la fourniture de leurs services;
- les entreprises exerçant des activités de transactions électroniques ;
- les prestataires de services agréés par l'Autorité compétente ;
- les prestataires de services d'archivages électroniques ou de conservation.

CHAPITRE III : PROCEDURE D'AUDIT DE SECURITE

Article 4 : L'audit de sécurité des organismes prévus à l'article précédent, en vue de la certification de leur système d'information, a lieu tous les trois ans.

A l'issue de l'audit de sécurité, un certificat de sécurité est délivré à l'audité lorsque l'audit est conforme aux règles de sécurité. Dans le cas contraire, un audit supplémentaire par décision motivée est notifié à l'organisme audité par l'ARTCI.

Dix-huit mois après l'obtention du certificat de sécurité, l'organisme audité procède à un audit de sécurité périodique obligatoire, dans les conditions prévues par le présent décret.

Article 5 : Les missions d'audit de sécurité sont effectuées par l'ARTCI.

Article 6 : L'ARTCI peut confier les missions d'audit de sécurité à des Prestataires d'Audit de Sécurité des Systèmes d'Information.

Les conditions et les procédures d'agrément des PASSI ainsi que de certification des experts auditeurs sont fixées par décision de l'ARTCI.

Article 7 : L'ARTCI établit chaque année, et au plus tard à la fin du troisième trimestre de l'année N, un planning des audits de sécurité de l'année N+1 qu'elle communique aux organismes soumis à l'audit de sécurité.

Le planning en cours d'exécution peut toutefois être modifié par l'ARTCI. La décision de modification doit être motivée et notifiée aux organismes audités.

Article 8 : Les PASSI transmettent leur rapport d'activité d'audit à l'ARTCI au plus tard à la fin du deuxième trimestre de l'année suivante.

Article 9 : L'opération d'audit de sécurité sur site s'appuie notamment sur les éléments suivants :

- l'analyse et l'évaluation des risques qui pourraient résulter de l'exploitation des failles découvertes;
- les aspects organisationnels et le mode de gestion de la fonction sécurité des systèmes d'information, le mode de gestion des procédures de sécurité et la disponibilité des outils de sécurisation du système informatique ainsi que leur mode d'utilisation ;
- les aspects techniques de la sécurité de toutes les composantes du système informatique et la réalisation du test de leur résistance à tous les types de dangers.

Article 10 : Chaque audit de sécurité des systèmes d'information est sanctionné par la délivrance d'un rapport d'audit et d'un procès-verbal de réunion de clôture produits par le PASSI.

Article 11 : Le rapport d'audit contient les éléments suivants :

- un compte rendu résumant les principales conclusions de l'examen des documents et les recommandations ;
- une description et une évaluation complète de la sécurité du système d'information ainsi que les mesures mises en œuvre depuis le dernier audit réalisé et les insuffisances enregistrées dans l'application des recommandations ;
- une description de la démarche méthodologique utilisée ;
- une description complète et détaillée des mesures de sécurité recommandées.

L'audité doit transmettre à l'ARTCI, par lettre recommandée avec accusé de réception, le rapport d'audit signé par le PASSI, dans un délai de dix jours ouvrés à compter de la date de réunion de clôture de l'audit.

Le PASSI transmet à l'ARTCI une copie cosignée par l'audité du procès-verbal de la réunion de clôture et le rapport d'audit, sous les mêmes conditions que celles décrites ci-dessus.

Article 12 : L'ARTCI peut, après analyse du rapport d'audit, demander à l'audité de lui fournir des informations ou des documents complémentaires et entreprendre un contrôle sur site.

Article 13 : L'ARTCI peut rejeter le rapport d'audit dans les cas suivants :

- lorsque l'enquête sur site n'a pas été réalisée conformément aux conditions prévues à l'article 9 ci-dessus;
- lorsque le rapport ne contient pas tous les éléments prévus à l'article 11 ci-dessus ;
- lorsque le contrôle sur site révèle de graves manquements aux obligations réglementaires en matière d'audit de sécurité des systèmes d'information.

Toutefois, en cas de nécessité, l'ARTCI peut faire procéder, aux frais des organismes, à un ou plusieurs audits supplémentaires au cours de la même période.

En cas de rejet du rapport, l'audité est tenu de refaire l'audit de son système d'information par un autre PASSI et de transmettre le nouveau rapport à l'ARTCI, dans un délai de trois mois, à compter de la date de la notification du rejet. L'ARTCI peut désigner un PASSI qui sera chargé de procéder à l'audit susvisé aux frais de l'audité.

Article 14 : Pour assurer la sécurité des systèmes d'information, l'ARTCI élabore un référentiel intitulé 'Référentiel Général de Sécurité des Systèmes d'Information, en abrégé RGSSI, qui fixe les règles et exigences auxquelles les organismes et entreprises visés à l'article 3 doivent se conformer.

Article 15 : En cas de conformité aux exigences du RGSSI, suite à l'audit en vue de la certification des systèmes d'information, l'ARTCI délivre à la structure auditée un certificat de sécurité.

En cas de non-conformité mineure, l'ARTCI délivre à la structure auditée un certificat de sécurité, sous réserve des corrections de la non-conformité mineure, dans un délai de dix-huit mois.

En cas de non-conformité majeure, l'ARTCI instruit la structure auditée de corriger la non-conformité majeure et de refaire auditer son système d'information dans un délai maximum de douze mois.

A l'issue du délai mentionné à l'alinéa précédent, l'ARTCI adresse une mise en demeure à l'organisme audité de se conformer aux mesures de sécurité prévues, sous peine de la sanction prévue à l'article 13.

Article 16 : Tout organisme public ou privé doit informer immédiatement l'ARTCI de toutes attaques, intrusions et autres perturbations susceptibles d'entraver le bon fonctionnement de son système d'information.

Article 17 : L'ARTCI prend toutes mesures pour faire cesser des perturbations constatées.

Article18 : Les PASSI sont soumis au paiement d'une redevance.

Article 19 : Les titulaires de systèmes soumis à l'audit de sécurité qui n'effectuent pas l'audit de sécurité périodique obligatoire, conformément à l'article 6, sont mis en demeure de s'y conformer, dans un délai de trente jours, à partir de la date de la notification.

A l'expiration de ce délai, en cas de non-réalisation de l'audit dans les termes et conditions prescrits, l'ARTCI procède à l'audit de l'organisme défaillant ou désigne un PASSI qui sera chargé de l'audit, aux frais de celui-ci, sans préjudice de toutes sanctions administratives prévues par la réglementation en vigueur et de toutes sanctions pécuniaires prévues par le présent décret.

CHAPITRE IV : SANCTIONS

Article 20 : L'ARTCI peut astreindre financièrement les structures visées à l'article 3 ci-dessus, à exécuter l'audit de sécurité périodique obligatoire.

Lorsqu'un manquement est constaté, il est infligé au contrevenant une sanction pécuniaire dont le montant est proportionnel à la gravité du manquement et aux avantages qui en sont tirés, sans pouvoir excéder la somme de trois cent millions de francs CFA.

En cas de récidive, le montant de la sanction est porté au double.

Article 21 : Les redevances d'audit de sécurité et les pénalités sont recouvrées et perçues par l'ARTCI. En cas de besoin, des quotes-parts de répartition sont définies par le Ministre chargé de l'Economie Numérique.

CHAPITRE V : DISPOSITIONS DIVERSES ET FINALES

Article 22 : Les activités d'audit de sécurité suivantes font l'objet de déclaration :

- la fourniture de service d'audit de sécurité des systèmes d'information de l'Administration et des organismes relevant du secteur public ;

- la fourniture de service d'audit de sécurité des systèmes d'information des organismes et entreprises relevant du secteur privé et se trouvant sur le territoire national.

Toutefois, ne sont pas concernés par la déclaration, les PASSI soumis à agrément de l'ARTCI qui fournissent des prestations d'audit de sécurité des systèmes d'information conformes aux exigences règlementaires.

Article 23 : Les activités d'audit de sécurité des systèmes d'information faisant l'objet de déclaration peuvent être exercées librement sous réserve que leur exploitation ne porte pas atteinte à la sécurité de l'Etat ou à l'ordre public. Toutefois, le fournisseur de service d'audit de sécurité des systèmes d'information doit déposer préalablement, auprès de l'Autorité de régulation des télécommunications/TIC, une déclaration d'intention d'ouverture de ce service.

En cas de cessation d'activité ou de service, il est tenu d'informer l'ARTCI au plus tard trente jours à compter de la date de cessation.

Article 24 : La déclaration d'intention d'ouverture du service d'audit de sécurité des systèmes d'information doit contenir les informations suivantes :

- l'identité et le statut juridique du demandeur ;
- les types d'audit de sécurité des systèmes d'informations ;
- les caractéristiques des logiciels ou équipements utilisés pour les audits de sécurité des Systèmes d'Information ;
- les certifications des experts au sein de son équipe.

Article 25 : Le Ministre de l'Economie Numérique, des Télécommunications et de l'Innovation est chargé de l'exécution du présent décret qui sera publié au Journal Officiel de la République de Côte d'Ivoire.

Fait à Abidjan, le 22 décembre 2021

Alassane OUATTARA

Copie certifiée conforme à l'original
Le Secrétaire Général du Gouvernement

RÉPUBLIQUE DE CÔTE D'IVOIRE
SECRÉTARIAT GÉNÉRAL DU GOUVERNEMENT

Eliane Atté BIMANAGBO
Préfet

N° 2101052