République du Sénégal
Un Peuple - Un But - Une Foi

PRESIDENCE DE LA REPUBLIQUE

SECRETARIAT GENERAL

Commission Nationale de Cryptologie

Direction générale du Chiffre et de la Sécurité des Systèmes d'Information

N° 1257 /PR/SG/CNC/DCSSI/DIE/DPSSAN

ACCREDITATION DES PRESTATAIRES D'AUDIT DES SYSTEMES D'INFORMATION - (PASI)

Dakar le 30 octobre 2023

INFORMATIONS

REDACTEURS

Rédigé par	Version	Date
DCSSI/DIE/DPSSAN	1.0	03 juillet 2023

VALIDATION

Valider par	Version	Date
Commission nationale de Cryptologie	1.0	26 septembre 2023

EVOLUTION DU DOCUMENT

Version	Date	Nature des modifications

CIBLES

Les départements ministèriels
Les prestataires d'audit des systèmes d'information
Les auditeurs
Les organismes d'évaluateurs
Le secteur privé

POUR TOUTE REMARQUE

Contact	Email
DCSSI	contact.dcssi@stcc-ssi.sn

SOMMAIRE

I. CONTEXTE ET OBJECTIFS

Conformément à la Circulaire Présidentielle n° 098/PR du 01 juillet 2021 relative au renforcement de la gouvernance de la sécurité des systèmes d'information de l'Etat et aux recommandations de la Commission Nationale de Cryptologie (CNC), la Direction générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI), en application de l'article 2 du décret n° 2021-35 portant création et fixant les règles de son organisation et de son fonctionnement, a la mission périodique de conduire l'audit des systèmes d'information des départements ministériels suivant les normes en la matière auprès des organismes publics et des autorités de certification.

Ces audits sont menés par des cabinets accrédités par l'Autorité Nationale de Cybersécurité (DCSSI) qui est l'organisme d'accréditation, pour garantir la qualité, la compétence et l'intégrité des prestataires de services et la crédibilité des rapports d'audit produits à l'issue des opérations.

L'objectif principal de l'accréditation est de renforcer la confiance des départements ministériels, dans le choix des cabinets d'audit, en regroupant l'ensemble des exigences et des critères techniques à respecter par les prestataires pour être qualifiés par la DCSSI.

Ce procédé de qualification constitue un gage de confiance pour confier des missions d'audit à des prestataires qualifiés. Il s'appuie sur la vérification d'un certain nombre de critères attestant, entre autres :

- des références des prestataires dans le domaine de l'audit des systèmes d'information ;
- de la qualification de leurs ressources humaines ;
- de l'efficacité et de l'adéquation des méthodes et outils audits utilisés ;
- de l'organisation du travail et du respect des règles déontologiques et de sécurité ;
- du respect des délais arrêtés pour le dépôt des rapports après l'audit ;
- du respect des procédures de passation des marchés publics.

II. NATURES DES AUDITS CONCERNEES PAR LA QUALIFICATION

Sont concernés par la qualification, six (06) natures d'audit tels que définis dans le référentiel n° 1055PR/SG/CNC/DCSSI de juillet 2021, et qui sont :

1. Audit de l'infrastructure physique ;
2. Audit organisationnel et logique ;
3. Audit communicationnel ;
4. Audit de la sécurité des systèmes d'information ;
5. Audit des projets et des marchés liés aux systèmes d'information ;
6. Audit de la conformité et la réglementation.

III. PROCEDURE DE QUALIFICATION DES PRESTATAIRES D'AUDIT DES SYSTEMES D'INFORMATION

Le processus de qualification se déroule ainsi qu'il suit :

1. CANDIDATURE :

Le prestataire d'audit soumet une demande à l'organisme d'accréditation compétent (DCSSI). La demande devra comporter :

- **a.** des informations détaillées sur la structure de l'entreprise ;
- **b.** des qualifications du personnel d'audit ;
- **c.** des politiques et des procédures internes ;
- **d.** des preuves de conformité aux critères d'accréditation ;
- **e.** des références et des expériences passées dans le domaine des systèmes d'information.

2. ÉVALUATION INITIALE :

L'organisme d'accréditation (DCSSI) effectue une évaluation initiale de la demande pour déterminer si le prestataire d'audit répond aux critères préliminaires d'accréditation. Cela peut inclure l'examen des documents soumis, des entretiens avec le personnel d'audit et des visites sur site.

3. ÉVALUATION APPROFONDIE :

Si la demande initiale est acceptée, une évaluation approfondie est réalisée. Cela implique un examen détaillé des politiques et procédures internes, des échantillons d'audits précédents, ainsi que des entretiens supplémentaires avec le personnel d'audit. L'objectif est de vérifier la conformité du prestataire d'audit aux critères d'accréditation décrits ci-après.

4. AUDIT DE CONFORMITE :

Dans certains cas, un audit de conformité peut être réalisé pour évaluer la conformité du prestataire d'audit aux normes d'audit internationalement reconnues. Cet audit peut être effectué par des auditeurs externes ou des évaluateurs désignés par l'organisme d'accréditation (DCSSI), pour des examens techniques approfondis, des évaluations des contrôles de sécurité mis en place, ainsi que des vérifications de la conformité aux exigences réglementaires.

5. DECISION D'ACCREDITATION :

Une fois que toutes les évaluations sont terminées, la DCSSI, sur proposition d'un comité prévu à cet effet piloté par la Direction Ingénierie Expertise (DIE), prend une décision concernant l'accréditation des prestataires d'audit répondant à toutes les exigences. Une accréditation est accordée pour une période déterminée, à fixer par décision (ou autre) signée par le Ministre Secrétaire Général de la Présidence de la République (MSGPR).

6. SUIVI ET EVALUATION :

Pendant la période d'accréditation, le prestataire d'audit est soumis à un suivi régulier pour assurer le maintien de la conformité aux critères d'accréditation. Des évaluations périodiques et inopinées peuvent également être effectuées pour renouveler l'accréditation.

IV. CRITERES DE QUALIFICATION DES PRESTATAIRES D'AUDIT

La qualification des prestataires d'audit des systèmes d'information obéit aux critères ci-après :

- être constitué sous forme de société de droit sénégalaise avec un statut juridique reconnu et approuvé et avoir plus de 50% plus de son capital détenu par des personnes de nationalité sénégalaise ;

- être en règle avec l'Administration du Sénégal ou celle de son pays en matière de fiscalité (si elle est basée à l'étranger) ;
- jouir d'une bonne moralité (enquêtes de sécurité et de moralité par les services compétents de l'État) ;
- être en règle avec l'Administration du Sénégal ou du pays où elle est immatriculée en matière de sécurité sociale (Inspection du Travail, Caisse de sécurité sociale et Institut de Prévoyance Retraite du Sénégal ou IPRES) ;
- avoir une expertise avérée dans l'audit des systèmes d'information (fournir des résultats d'audit effectués) ;
- remplir les conditions figurant dans le référentiel d'audit n° 1055PR/SG/CNC/DCSSI de juillet 2021 ;
- être qualifié au minimum dans deux (02) natures d'audit parmi ceux précédemment citées et disposer d'un auditeur au minimum dans chaque domaine de qualification demandé ;
- prouver une expertise technique solide dans le domaine de la sécurité des systèmes d'information, en fournissant des certifications professionnelles reconnues de son personnel, telles que :
    - CISA (Certified Information Systems Auditor), pour les auditeurs des systèmes d'information ;
    - CISSP : (Certified Information Systems Security Professional), pour les auditeurs en sécurité systèmes d'information ;
    - CISM (Certified Information Security Manager), pour les auditeurs en gestion de la sécurité de l'information, les principes de gouvernance, de gestion des risques et de conformité ;
    - ISO 27001 Lead Auditor/Lead Implementor, pour les auditeurs principauxs ayant une compréhension approfondie de la norme du système de gestion de la sécurité de l'information (SMSI) ;

- ISO 27034, pour les auditeurs en sécurité des applications ;
- ITIL (Information Technology Infrastructure Library), pour la gestion des services informatiques ;
- OSCP (Offensive Security Certified Professional), pour les compétences et les connaissances nécessaires pour faire des tests d'intrusion, Pentester ;
- COBIT (Control Objectives for Information and Related Technology), pour une meilleure approche en matière d'audit informatique, de gouvernance et de bonnes pratiques liées à la gestion des systèmes d'information et des technologie ;
- CEH (Certified Ethical Hacker - hackeur éthique certifié), pour des connaissances requises pour déployer les outils et méthodes des pirates afin de déceler des éventuelles failles dans un système et de proposer des recommandations essentielles pour mettre en œuvre une défense adéquate (Certified Ethical Hacker) ;
- ISO 22301, pour un Système de Management de la Continuité d'Activité (savoir comment maintenir les activités d'un organisme en cas de crises) ;
- PMP (Project Management Professional), pour assurer la compétence, l'efficacité et le professionnalisme en gestion de projet ;
- Ingénieurs électrotechniciens, spécialistes confirmés pour la gestion de l'énergie.

– être indépendants et impartiaux, a fin d'éviter les conflits d'intérêts qui pourraient compromettre l'objectivité de l'évaluation des systèmes d'information ;
– avoir une méthodologie claire et bien définie pour mener des audits des systèmes d'information. Cela peut inclure des étapes telles que la collecte d'informations, l'analyse des risques, l'évaluation des contrôles de sécurité, la documentation des résultats et la formulation de recommandations ;
– respecter les politiques et les procédures d'audit mise en place pour garantir la confidentialité et la protection des informations sensibles auxquelles ils peuvent avoir accès pendant l'audit ;
– s'engager à maintenir à jour leurs compétences en suivant des programmes de formation continue dans le domaine de la sécurité des systèmes d'information. Ils doivent

également être tenus informés des évolutions technologiques et des nouvelles menaces de sécurité ;

- être en mesure de produire des rapports d'audit complets, précis, pertinents, et dans les délais raisonnables mettant en évidence les faiblesses de sécurité identifiées et formulant des recommandations claires pour améliorer la sécurité des systèmes d'information.

V. DEMANDE DE QUALIFICATION DES PRESTATAIRES D'AUDIT

Le dossier de demande de qualification des prestataires d'audit comprend les documents suivants:

- copie des statuts de la structure ;
- attestation d'inscription au registre de commerce ;
- liste des noms des associés et leurs nationalités ;
- copies légalisées des pièces d'identité des dirigeants de la société et ses organes d'administration ainsi que des auditeurs proposés ;
- note indiquant les moyens humains et techniques de la structure ;
- copies des casiers judiciaires des auditeurs proposés ;
- curriculums vitae des auditeurs proposés et le cas échéant les copies de leurs diplômes et certificats de formation ;
- copies des contrats de travail conclus avec les auditeurs proposés ;
- copies des attestations délivrées par les maîtres d'ouvrages au profit desquels ont été exécutées des prestations d'audit des systèmes d'information, et devant préciser notamment la nature de la prestation fournie et la date de sa réalisation ;
- document décrivant la méthodologie appliquée pour conduire la prestation d'audit, objet de la demande de qualification.

Ce dossier est déposé par le prestataire lui-même avec la mention ***« DEMANDE D'ACCREDITATION POUR L'AUDIT DES SYSTEMES D'INFORMATION »*** au Secrétariat général de la Présidence de la République en trois (03) exemplaires à l'adresse ci-dessous :

A Monsieur le Ministre, Secrétaire général de la Présidence de la République
Secrétariat général de la Présidence de la République.

(Direction générale du Chiffre et de la Sécurité des Systèmes d'Information – DCSSI)

Avenue Léopold Sedar Senghor,

BP 4026 Dakar

E-mail : contact.dcssi@stcc-ssi.sn

Tel : (+221)338808369

Dakar, Sénégal

Le prestataire est tenu d'informer la DCSSI de toute modification de l'un des éléments figurant dans la demande de qualification.

VI. INSTRUCTION DE LA DEMANDE EN VUE DE LA QUALIFICATION DES PRESTATAIRES D'AUDIT

Après avoir reçu le dossier de demande d'accréditation comprenant tous les documents et informations requis, la DCSSI procède à l'instruction des dossiers de demande de prestations d'audit, par un comité, présidé par le Directeur général de la DCSSI et piloté par la Direction Ingénierie Expertise.

Ce comité est composé :

- du Directeur général du Chiffre et de la Sécurité des Systèmes d'Information ou son représentant ;
- du Directeur de l'Ingénieur Expertise (DIE) ou son représentant ;
- du Directeur de l'Administration, des Affaires juridiques et des Relations extérieures ou son représentant ;
- du Directeur du Centre National Opérationnel de Cybersécurité (CNOC) ou son représentant ;
- du Chef de la Division Produits et Services de sécurité, Audit et Normalisation (DPSSAN) ;
- du Chef de la Division Expertise et Assistance (DEA) ;
- du Chef de la Division Ingénierie cryptologique (DIC) ;
- du Chef du Centre de Formation Cryptologique et à la Sécurité des Systèmes d'Information (CFC-SSI) ;

Le comité peut s'adjoindre à toute personne dont les compétences sont jugées utiles à l'instruction des dossiers de demande d'accréditation.

L'évaluation précitée s'effectue conformément aux critères de qualification et au référentiel n° 1055PR/SG/CNC/DCSSI de juillet 2021. Ledit référentiel précise les exigences relatives aux auditeurs.

A l'issue des résultats de l'évaluation, la DCSSI prend la décision de qualification qui précise notamment :

- la dénomination et l'adresse du siège social du prestataire d'audit ;
- les natures d'audit, objet de la qualification;
- la durée de validité de la qualification qui ne dépasse pas trois (03) ans ;
- la liste des auditeurs par nature d'audit en indiquant leurs niveaux de qualification.

En cas de réponse défavorable, la DCSSI notifie sa décision au demandeur de la qualification.

VII. RENOUVELLEMENT DE LA QUALIFICATION DES PRESTATAIRES D'AUDIT

Le renouvellement de la qualification du prestataire d'audit se fait dans les mêmes conditions exigées pour son obtention. Cependant une nouvelle demande de renouvèlement devra être déposée, au moins, dans les soixante (60) jours, avant la date d'expiration de la décision de qualification en cours.

Le prestataire d'audit des systèmes d'information devra informer, sans délai, la DCSSI de toute modification intervenue dans l'un des éléments sur la base desquels la qualification avait été délivrée.

VIII. RETRAIT DE LA QUALIFICATION DES PRESTATAIRES D'AUDIT

En cas de nos respect des critères sur la base desquels la qualification était délivrée, la DCSSI adresse une mise en demeure de se conformer aux prescriptions y afférentes dans un délai qu'elle fixe selon l'importance de ses prescriptions.

Si le prestataire d'audit ne défère pas à la mise en demeure, la DCSSI suspend sa qualification, jusqu'à ce qu'il se conforme auxdites prescriptions, à défaut, la qualification est retirée.

IX. PUBLICATION DE LA QUALIFICATION DES PRESTAIRES D'AUDIT

La liste des prestataires d'audit des systèmes d'information qualifiés est publiée au journal Officiel et sur le site web de la DCSSI.

ANNEXE 1

FORMULAIRE DE LA DEMANDE DE QUALIFICATION DES PRESTATAIRES D'AUDIT DES SYSTEMES D'INFORMATION

I. NATURE DE LA DEMANDE

- ☐ Première qualification
- ☐ Renouvellement de la qualification *(03 ans après la première qualification)*

II. SYSTEMES D'INFORMATION CIBLES *(voir annexe 2)*

- ☐ CLASSE A
- ☐ CLASSE B
- ☐ CLASSE C
- ☐ CLASSE D

III. INFORMATIONS GENERALES SUR LE PRESTATAIRE D'AUDIT

Raison sociale	
Inscription au registre de commerce (RCCM)	N°.....Ville.....
Adresse	
Téléphone	
Fax	
Site Web	

IV. INFORMATIONS SUR LE REPRESENTANT LEGAL

Prénoms et Nom	
Qualité	
Nationalité	
Pièce d'identité	Nature ..... N°.....
Adresse	
Téléphone	
Fax	
Email	

V. INFORMATIONS SUR LE CAPITAL ET LES ASSOCIES

Prénoms et Nom de l'associé	Personne physique ou morale	Nationalité	Part du capital	Nombre des actions ou de parts sociales

VI. NATURES D'AUDIT OBJET DE LA DEMANDE DE QUALIFICATION

- ☐ Audit de l'infrastructure physique
- ☐ Audit organisationnel et logique
- ☐ Audit communicationnel
- ☐ Audit de la sécurité des systèmes d'information
- ☐ Audit des projets et des marchés liés aux systèmes d'information
- ☐ Audit de la conformité et la réglementation

VII. AUDITEURS PROPOSES

Prénoms et Nom	Email	Nationalité	Domaines d'audit	Séniorité (Senior ou Junior)	Années d'expérience	Nombre de jours d'audit des SI/ Nombre de missions
			Audit de l'infrastructure physique			
			Audit organisationnel et logique			
			Audit communicationnel			
			Audit de la sécurité des systèmes d'information			
			Audit des projets et des marchés liés aux systèmes d'information			
			Audit de la conformité et la réglementation			
			Audit de l'infrastructure physique			
			Audit organisationnel et logique			
			Audit communicationnel			
			Audit de la sécurité des systèmes d'information			
			Audit des projets et des marchés liés aux systèmes d'information			
			Audit de la conformité et la réglementation			
			Audit de l'infrastructure physique			
			Audit organisationnel et logique			
			Audit communicationnel			
			Audit de la sécurité des systèmes d'information			

				Audit des projets et des marchés liés aux systèmes d'information			
				Audit de la conformité et la réglementation			
				Audit de l'infrastructure physique			
				Audit organisationnel et logique			
				Audit communicationnel			
				Audit de la sécurité des systèmes d'information			
				Audit des projets et des marchés liés aux systèmes d'information			
				Audit de la conformité et la réglementation			
				Audit de l'infrastructure physique			
				Audit organisationnel et logique			
				Audit communicationnel			
				Audit de la sécurité des systèmes d'information			
				Audit des projets et des marchés liés aux systèmes d'information			
				Audit de la conformité et la réglementation			
				Audit de l'infrastructure physique			
				Audit organisationnel et logique			
				Audit communicationnel			
				Audit de la sécurité des systèmes d'information			
				Audit des projets et des marchés liés aux systèmes d'information			

				Audit de la conformité et la réglementation			

VIII. AUDITS DES SYSTEMES D'INFORMATION EFFECTUES

Organisme	Mission réalisée	Période

IX. METHODOLOGIES D'AUDIT ADOPTEES

NATURE D'AUDIT	REFERENTIELS	OUTILS
Audit de l'infrastructure physique		
Audit organisationnel et logique		
Audit communicationnel		
Audit de la sécurité des systèmes d'information		
Audit des projets et des marchés liés aux systèmes d'information		
Audit de la conformité et la réglementation		

Je déclare, sur l'honneur, l'exactitude des renseignements fournis dans cette demande.

Fait à ..... le .....

Signature et cachet

ANNEXE 2

CLASSIFICATION DES ACTIFS DES SYSTEMES D'INFORMATION

Les vulnérabilités des systèmes d'information sont classifiées sur la base d'une analyse des impacts des incidents susceptibles de porter atteinte à la confidentialité, à la disponibilité ou à l'intégrité des actifs, en passant par le matériel, le logiciel, la donnée ou la procédure, qui composent lesdits systèmes d'information.

Le niveau d'impact des incidents précités doit refléter l'importance des conséquences pouvant se traduire par l'incapacité de la structure à:

- accomplir ses missions ;
- préserver la vie, la santé ou le bien-être des personnes ;
- se conformer aux lois, aux règlements et aux obligations contractuelles ;
- préserver l'image de l'Etat ;
- maintenir et renforcer la confiance des citoyens et des partenaires à l'égard des services offerts, ou par la capacité de ladite structure à affecter le fonctionnement d'entités tierces, tributaires de ses services.

L'analyse des impacts doit se faire selon l'échelle suivante :

1- Impact très grave : Si un incident informatique portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif pourrait :

- nuire au maintien des capacités de sécurité et de défense de l'Etat ;
- porter préjudice aux intérêts stratégiques de l'Etat ;
- porter atteinte à la santé et à la sécurité de la population ;
- perturber ou nuire au fonctionnement de l'économie nationale ;
- engendrer une incapacité partielle ou totale de plusieurs infrastructures d'importance vitale à assurer leurs fonctions essentielles.

2- Impact grave : Si un incident informatique portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif pourrait engendrer :

- une incapacité partielle ou totale d'une infrastructure d'importance vitale à assurer ses fonctions essentielles ;
- une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures d'importance vitale à assurer leurs fonctions critiques ;
- des pertes financières importantes pour une ou plusieurs entités ou infrastructures d'importance vitale.

3- Impact modéré : Si un incident informatique portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif pourrait engendrer :

- une gêne ou perturbation mineure dans les fonctions d'une infrastructure d'importance vitale ;
- une incapacité partielle d'une ou de plusieurs entités non considérées comme infrastructures d'importance vitale, à assurer leurs fonctions ;
- des pertes financières modérées ;
- ou toute autre conséquence de nature analogue.

4- Impact limité : Si un incident informatique portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif pourrait, causer :

- une gêne ou perturbation dans les fonctions de l'entité non considérée comme infrastructure d'importance vitale ;
- des pertes financières limitées ;
- ou toute autre conséquence de nature analogue.

Un système d'information est classifié sur la base de l'échelle de l'analyse des impacts ci-dessus et ce, selon les niveaux suivants :

« **CLASSE A** », si au minimum un incident informatique, portant sur la confidentialité, la disponibilité ou l'intégrité d'un des actifs qui compose le système d'information, a un impact très grave ;

« **CLASSE B** », si tous les incidents informatiques portant sur la confidentialité, la disponibilité ou l'intégrité, des actifs qui composent le système, ont au maximum un impact grave ;

« **CLASSE C** », si tous les incidents informatiques portant sur la confidentialité, la disponibilité ou l'intégrité, des actifs qui composent le système, ont au maximum un impact modéré ;

« **CLASSE D** », si tous les incidents informatiques portant sur la confidentialité, la disponibilité ou l'intégrité, des actifs informationnels qui composent le système, ont un impact limité.