ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE

RÉPUBLIQUE DU BÉNIN

REFERENTIEL DES EXIGENCES

relatives à la qualification des fournisseurs de services de sécurité numérique en République du Bénin

Suivez-nous sur nos canaux digitaux

@asinbenin

TABLE DES MATIERES

SIGLES	DEFINITIONS
ASIN	Agence des Systèmes d'Information et du Numérique
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Networking Professional
CEH	Certified Ethical Hacking
CGEIT	Certified in the Governance of Enterprise IT
CHFI	Computer Hacking Forensic Investigator
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CNSS	Caisse Nationale de Sécurité Sociale
COBIT	Control Objectives for Information and related Technology
CV	Curriculum Vitae
ECIH	EC-Council Certified Incident Handler
FSSN	Fournisseur de Services de Sécurité Numérique
FSSNQ	Fournisseur de Services de Sécurité Numérique Qualifié
GPEN	GIAC Penetration Tester
GWAPT	GIAC Web Application Penetration Tester
ISO 27001 LA	ISO 27001 Lead Auditor
ISO 27001 LI	ISO 27001 Lead Implementer
ISO 27005 RM	ISO 27005 Risk Manager

SIGLES	DEFINITIONS
ISO/IEC 27035	Gestion des incidents de sécurité de l'information
ISSAP	Information Systems Security Architecture Professional
ITIL	Information Technology Infrastructure Library
MCSE	Microsoft Certified Solutions Expert
OCA	Oracle Certified Associate
OIIC	Opérateur d'Infrastructures d'Information Critiques
OCM	Oracle Certified Master
OCP	Oracle Certified Professional
OCPSC	Organe de Contrôle des Prestataires de Services de Confiance
OSCP	Offensive Security Certified Professional
OWASP	Open Web Application Security Project
PPIIC	Politique de Protection des Infrastructures d'Information Critiques
PSSIE	Politique de Sécurité des Systèmes d'Information de l'Etat
RFC	Request for comments
SABSA	Certifications for Security Architects
SSL	Secure Sockets Layer
VPN	Virtual Private Network
WMI	Windows Management Instrumentation

Terminologies	Sens
Commanditaire	C'est la partie qui requiert le service de sécurité numérique. Il s'agit d'une structure du secteur public - administrations publiques : Présidence de la République, Ministères, Institutions de la République, Agences ou structures sous tutelles, y compris les établissements publics et les sociétés d'Etat- ou d'un OIIC sollicitant un service de sécurité de numérique.
Personnel technique	Cadre technique du FSSN participant aux missions de services de sécurité numérique.
Critères d'audit	Ensemble d'exigences utilisées comme référence vis-à-vis de laquelle les preuves objectives sont comparées.
Domaine d'audit ou périmètre d'audit	C'est tout ou partie de l'infrastructure ou du système d'information objet de l'audit de façon spécifique.
Etat de l'art	C'est l'état ou l'évolution des connaissances dans un domaine ou secteur spécifique donné.
Fournisseur de Services de Sécurité Numérique (FSSN)	Cabinet, société ou groupement de cabinets offrant des services de sécurité numérique.

Fournisseur de Services de Sécurité Numérique Qualifié (FSSNQ)	Fournisseur de Services de Sécurité Numérique ayant reçu la qualification de l'OCPSC.
Organe de contrôle des prestataires de services de confiance (OCPSC)	Entité qui délivre la qualification aux fournisseurs de services de sécurité numérique.
Preuves d'audit	Enregistrements, documentation, énoncés de faits ou autres informations pertinentes et vérifiables pour les critères d'audit.
Rapport d'audit	C'est le document qui mentionne le but, les objectifs, la période couverte, la nature et l'étendue de l'audit réalisé. Il identifie l'organisation, les destinataires voulus et toute(s) restriction(s) dans la distribution. Il contient les résultats, conclusions et recommandations ainsi que toute(s) réserve(s) ou qualification(s) de l'auditeur vis-à-vis de l'audit.
Système d'information	Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné (Réf : PSSIE).

PARTIE I

Arrêté année 2023 N°006 / MND / DC / SGM / CTJ / CJ / SA / 006SGG2023 fixant les règles applicables aux fournisseurs de services de sécurité numérique en République du Bénin

MINISTÈRE DU NUMÉRIQUE ET DE LA DIGITALISATION
RÉPUBLIQUE DU BÉNIN

01 BP 120 Cotonou
+229 21312237
menc.contact@gouv.bj
https://numerique.gouv.bj

ARRÊTÉ

ANNÉE 2023 N° 006/MND/DC/SGM/CTJ/CJ/SA/006SGG23
fixant les règles applicables aux fournisseurs de services de sécurité numérique en République du Bénin.

LE MINISTRE DU NUMÉRIQUE ET DE LA DIGITALISATION

Vu la loi n° 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin, telle que modifiée par la loi n° 2019-40 du 07 novembre 2019 ;

vu la loi n° 2007-21 du 16 octobre 2007 portant protection du consommateur en République du Bénin ;

vu la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, telle que modifiée par la loi n° 2020-35 du 06 janvier 2021 ;

vu la décision portant proclamation le 21 avril 2021 par la Cour Constitutionnelle des résultats définitifs de l'élection présidentielle du 11 avril 2021 ;

vu le décret n° 2023-156 du 17 avril 2023 portant composition du Gouvernement ;

vu le décret n° 2021-401 du 28 juillet 2021 fixant la structure-type des ministères, tel que modifié par le décret n°2022-476 du 03 août 2022 ;

vu le décret n° 2021-308 du 09 juin 2021 portant attributions, organisation et fonctionnement du Ministère du Numérique et de la Digitalisation ;

vu le décret n°2020-485 du 07 octobre 2020 portant attributions, organisation et fonctionnement de l'Organe de contrôle des prestataires de services de confiance numérique en République du Bénin ;

vu le décret n° 2021-550 du 27 octobre 2021 portant approbation des règles de politique de sécurité des systèmes d'information de l'État en République du Bénin ;

vu le décret n°2023-060 du 22 février 2023 portant approbation des règles de politique de protection des infrastructures d'information critiques en République du Bénin ;

vu le décret n° 2022-324 du 1er juin 2022 portant création de l'Agence des Systèmes d'Information et du Numérique, par la fusion de l'Agence du Développement du Numérique, de l'Agence des Services et Systèmes d'Information, de l'Agence Nationale de la Sécurité des Systèmes d'Information et de l'Agence béninoise du Service universel des Communications électroniques et de la Poste et approbation de ses statuts ;

Considérant la mission de qualification des prestataires de services de confiance mise en œuvre par l'Organe de contrôle des prestataires de services de confiance ;

Considérant que la qualification des fournisseurs de services de sécurité numérique contribue à l'amélioration de la qualité de services de sécurité numérique offerts aux entités étatiques, et participe à l'essor de l'entrepreneuriat numérique sur le plan national,

ARRÊTE

CHAPITRE PREMIER : DISPOSITIONS GENERALES

Article 1 : Objet

Le présent arrêté a pour objet de fixer les règles applicables aux fournisseurs de services de sécurité numérique en République du Bénin.

Article 2 : Champ d'application

Les dispositions de cet arrêté s'appliquent aux fournisseurs de services de sécurité numérique nationaux ou étrangers désireux d'offrir des services de sécurité numérique aux entités concernées par les règles de la politique de sécurité des systèmes d'information de l'Etat et aux entités concernés par les règles de politique de protection des infrastructures d'information critiques.

Lesdits fournisseurs sont soumis à la fois aux dispositions du présent arrêté et de celles du décret n°2020-485 du 07 octobre 2020 portant attributions, organisation et fonctionnement de l'Organe de contrôle des prestataires de services de confiance numérique en République du Bénin.

Article 3 : Domaines de sécurité numérique soumis à la qualification

La fourniture de services de sécurité numérique dans les domaines suivants, requiert une qualification :

- audit organisationnel et physique ;
- audit de conformité ;
- audit d'architecture ;
- audit de configuration ;
- audit de code source ;
- audit à blanc ;
- audit de vulnérabilités ;
- tests d'intrusion ;
- audit des systèmes industriels ;
- investigation numérique ;
- réponse aux incidents.

Le référentiel annexé au présent arrêté donne les détails des activités relevant de chaque domaine.

CHAPITRE II : REGLES COMMUNES APPLICABLES

Article 4 : Conditions d'éligibilité

Le fournisseur de services de sécurité numérique qui postule à la qualification auprès de l'organe de contrôle des prestataires de services de confiance doit remplir les conditions ci-après :

- être une personne morale et avoir une existence légale ;
- avoir une organisation interne comprenant à minima une direction technique ou équivalent ;
- disposer de personnel dont au moins la moitié sont des permanents, ayant les profils requis pour la réalisation des services de sécurité numérique dans le domaine pour lequel le fournisseur postule ;
- disposer de deux (02) personnes techniques au minimum et par domaine où la qualification est recherchée ; la qualification peut être obtenue dans plusieurs domaines avec le même personnel si le profil de ce dernier est conforme aux exigences des domaines où le fournisseur de services de sécurité numérique le positionne ;
- avoir au moins 30% de nationaux au sein du personnel technique délivrant les services de sécurité numérique ; le fournisseur de services de sécurité numérique disposant d'un effectif total de deux (02) consultants doit présenter à minima une personne de nationalité béninoise;

Article 5 : Composition du dossier de demande

Le dossier de demande de qualification comprend les pièces ci-après :

- copie du registre de commerce ou de l'acte de regroupement (si applicable) ;
- copie des IFU des consultants ;
- copie des CIP (ou équivalent pour les non-nationaux) de chaque consultant présenté pour la qualification ;
- copie de l'organigramme ;
- copie du plan de formation ;
- copie du contrat de travail des consultants présentés pour la qualification ;
- copie des CV des consultants présentés pour la qualification ;
- copie des certifications et diplômes des consultants présentés pour la qualification ;
- copie du code d'éthique signé par chacun des consultants présentés pour la qualification ;
- copie des casiers judiciaires des consultants présentés pour la qualification ;
- formulaires d'engagement à signer (téléchargeables sur le site de l'organe de contrôle des prestataires de services de confiance) ;

- copie de la politique de protection de l'information ;
- plan de situation géographique du cabinet/société ;
- copie des bilans des trois dernières années d'exercices (Non applicable pour les fournisseurs de services de sécurité numérique nouvellement créés) ;
- fournir une attestation CNSS.

CHAPITRE III : REGLES RELATIVES AUX CONSULTANTS DU FOURNISSEUR DE SERVICES DE SECURITE NUMERIQUE

Article 6 : Evaluation des consultants du fournisseur de services de sécurité numérique

Dans le cadre de la qualification, les consultants sont évalués et leurs compétences jouent un rôle primordial dans l'obtention de la qualification.

En cas de démission ou de rupture de contrat, le fournisseur de services de sécurité numérique qualifié informe l'organe de contrôle des prestataires de service de confiance dans un délai de trente (30) jours ouvrés avec ampliation à l'Agence des systèmes d'information et du numérique.

Article 7 : Compétences spécifiques

Des compétences spécifiques sont nécessaires pour chaque domaine de services de sécurité numérique dans lequel le fournisseur de services de sécurité numérique souhaite se faire qualifier. Les exigences relatives à ces compétences spécifiques par domaine sont déclinées en **annexe** du référentiel.

CHAPITRE IV : CYCLE DE QUALIFICATION

Article 8 : Demande de qualification

Le fournisseur de services de sécurité numérique désireux d'obtenir la qualification adresse une demande au Président de l'organe de contrôle des prestataires de services de confiance précisant les types de services de sécurité numérique pour lesquels il souhaite se faire qualifier.

Les pièces à joindre à la demande sont indiquées à l'article 5 ci-dessus.

Article 9 : Frais de qualification

Les frais de qualification sont en fonction du chiffre d'affaires annuel du fournisseur de services de sécurité numérique et du nombre de domaine de qualification. Ils sont définis comme suit :

N° d'ordre	Tranches de chiffre d'affaires en FCFA	Frais de qualification par domaine (FCFA)
1	CA inférieur ou égal à 30.000.000	150.000
2	CA compris entre 30.000.000 et 100.000.000	300.000
3	CA compris entre 100.000.000 et 250.000.000	750.000
4	CA supérieur à 250.000.000	1.500.000
5	Entreprises disposant du label "Startup" du Bénin	75.000

Article 10 : Demande d'extension du nombre de domaine de qualification

Le fournisseur de services de sécurité numérique qualifié qui désire avoir de nouvelle(s) qualification(s) introduit auprès de l'organe de contrôle des prestataires de services de confiance, le dossier complémentaire, suivant les exigences du nouveau domaine de qualification.

Il y joint un mémoire décrivant les motifs de sa demande.

Le dossier du fournisseur de services de sécurité numérique qualifié est étudié et son statut mis à jour au terme du processus de qualification et conformément à la décision de l'organe de contrôle des prestataires de services de confiance.

Article 11 : Demande de réduction du nombre de domaine de qualification

Le fournisseur de services de sécurité numérique qui désire réduire le nombre de domaines de qualification, en informe l'organe de contrôle des prestataires de services de confiance. Ce dernier en prend acte, rend dans les mêmes formes que la qualification la décision subséquente, la notifie au demandeur et procède à la mise à jour de son dossier.

Article 12 : Demande de modification de l'équipe technique

Le fournisseur de service de sécurité numérique désireux de modifier son équipe technique informe l'organe de contrôle des prestataires de services de confiance contenant le motif du remplacement, le personnel à remplacer et le dossier du remplaçant.

L'organe de contrôle des prestataires de services de confiance procède à l'étude de la demande et prend une décision qu'il notifie au fournisseur de services de sécurité numérique par écrit dans un délai ne dépassant pas dix (10) jours ouvrés à compter de la date de la demande et son dossier est mis à jour.

Article 13 : Renouvellement de la qualification

Le renouvellement de la qualification dans un domaine intervient au terme de la période de validité.

Le processus se déroule dans les mêmes conditions que la qualification initiale.

Article 14 : Durée de la qualification

La qualification est délivrée pour une durée de trois (03) ans renouvelable dans les mêmes conditions sauf si les différents audits diligentés révèlent des manquements graves aux exigences liées à la qualification.

Article 15 : Perte de la qualification

Le fournisseur de service de sécurité numérique qualifié perd sa qualification dans les conditions énumérées ci-après :

- défaut de remplacement d'un personnel technique démissionnaire ou en cas de rupture du contrat de ce dernier ;
- inexistence d'au moins deux (02) personnes pour la prestation de service dans un domaine donné ;
- usurpation de domaine de qualification ;
- défaut de notification à l'organe de contrôle des prestataires de services de confiance et à l'Agence des systèmes d'information et du numérique dans les trente (30) jours, de tous les changements dans les conditions ayant déterminé l'obtention de la qualification ;
- défaut de transmission du rapport d'activités à l'organe de contrôle des prestataires de services de confiance et à l'Agence des systèmes d'information et du numérique dans les délais requis ;
- obstruction aux missions d'audit diligentées par l'organe de contrôle des prestataires de services de confiance et à l'Agence des systèmes d'information et du numérique ;
- fourniture de services de sécurité numérique avec du personnel non qualifié ;
- tout autre manquement grave aux exigences de la qualification.

Article 16 : Délai de traitement des demandes de qualification

L'organe de contrôle des prestataires de services de confiance dispose d'un délai de quarante-cinq (45) jours ouvrés à compter de la date de soumission du dossier pour rendre sa décision.

CHAPITRE : DISPOSITIONS TRANSITOIRES ET FINALES

Article 17 : Délai de mise en conformité

Les fournisseurs de services de sécurité numérique disposent d'un délai de trois (03) mois à compter de l'entrée en vigueur du présent arrêté pour leur mise en conformité.

Article 18 : Modalités de mise en conformité

La mise en conformité est faite dans les mêmes conditions que la demande de qualification initiale.

Article 19 : Application

L'organe de contrôle des prestataires de services de confiance et l'Agence des systèmes d'information et du numérique sont chargés, chacun en ce qui le concerne de l'application du présent arrêté.

Article 20 : Entrée en vigueur

Le présent arrêté, qui prend effet à compter de la date de sa signature, abroge toutes dispositions antérieures contraires.

Il sera publié au Journal officiel.

Fait à Cotonou, le 24 JUIL. 2023

Aurelie I. ADAM SOULE ZOUMAROU

Ampliations : PR 1 (ATCR) ; SGG 1 ; MND 2 ; AN 1 ; CS 1 ; CC 1 ; COUR DES COMPTES 1 ; CES 1 ; HAAC 1 ; HCJ 1 ; AUTRES MINISTERES 21 ; ASIN 1 ; BAI 1 ; IGF 1 ; DGB 1 ; DCF 1 ; DGTCP 1 ; DGI 1 ; ARCHIVES 1 ; ORIGINAL 1 ; JORB 1.

PARTIE II

Référentiel des exigences relatives à la qualification des fournisseurs de services de sécurité numérique en République du Bénin

I.Types de services de sécurité numérique

A Audit organisationnel et physique

L'audit organisationnel et physique permet de réaliser un état des lieux exhaustif du niveau de sécurité de l'ensemble du système d'information du commanditaire sur les volets organisationnels, procéduraux et technologiques. Cet audit peut comprendre l'organisation générale de la sécurité, la sécurité physique des locaux, l'exploitation et l'administration.

B Audit de conformité

L'audit organisationnel et physique permet de réaliser un état des lieux exhaustif du niveau de sécurité de l'ensemble du système d'information du commanditaire sur les volets organisationnels, procéduraux et technologiques. Cet audit peut comprendre l'organisation générale de la sécurité, la sécurité physique des locaux, l'exploitation et l'administration.

C Audit d'architecture

L'audit d'architecture consiste à contrôler la conformité du choix, du déploiement et de la mise en œuvre d'un système d'information avec les normes et standards reconnus ou sectoriellement imposés au commanditaire de l'audit.
Idéalement, l'audit d'architecture est conduit pendant la phase de conception du système d'information et veille toujours à s'assurer que l'architecture auditée est en phase avec les fondamentaux de la sécurité de l'information à savoir la confidentialité, l'intégrité et la disponibilité, mais il peut également être fait après la mise en œuvre du système d'information.

D Audit de configuration

L'audit de configuration consiste à vérifier la conformité des éléments de paramétrage d'une solution informatique ou d'un équipement par rapport à la documentation officielle du fabricant ou de l'éditeur, ou des référentiels ou des standards internationaux (règlementation nationale, RFC, SANS (SysAdmin, Audit, Network, Security), du CIS (Center for Internet Security), et les contraintes métiers spécifiques de l'audité normes ISO, ...).

E Audit de code source

L'audit de code source, également appelé revue de code source, est le processus d'examination du code source d'un logiciel ou d'une application permettant de vérifier que les contrôles de sécurité appropriés sont présents, qu'ils fonctionnent comme prévu et qu'ils ont été invoqués aux bons endroits. La revue de code source est également un moyen de s'assurer que l'application a été développée pour s'auto-défendre dans un environnement donné et quelle ne présente de failles évidentes.

F Audit à blanc

L'audit à blanc encore appelé audit de pré-qualification est réalisé en amont du processus de certification d'un système d'information. Il permet d'évaluer le gap entre le système et les procédures existantes par rapport à une norme de certification donnée.

G Audit de vulnérabilités

Les audits de vulnérabilités permettent d'identifier les failles matérielles et logicielles de tout ou partie d'un système d'information (réseaux, applications, cloud, etc.). Ils peuvent être effectués en ayant une connaissance complète du système d'information audité (boite blanche), ou une connaissance partielle (boite grise). Lorsque les audits de vulnérabilités sont effectués sans connaissance aucune du système d'information audité (boite noire), il s'agit d'un test d'intrusion, décrit au point suivant.

H Tests d'intrusion

Les tests d'intrusion permettent aux entreprises d'évaluer la sécurité globale de leur infrastructure informatique du point de vue d'un acteur malveillant. Ainsi, un test d'intrusion interne simule une tierce personne malveillante et interne à l'organisation tandis qu'un test d'intrusion externe reproduit les comportements d'un pirate externe à l'organisation.

I

Audit des systèmes industriels

L'audit des systèmes industriels est une spécialisation des audits de vulnérabilités qui évalue et traite les questions de sécurité relatives aux systèmes industriels. Ces systèmes deviennent de plus en plus intelligents et connectés et font donc face aux menaces informatiques, en particulier provenant d'acteurs étatiques. La connaissance des technologies spécifiques à la production industrielle est souvent primordiale dans ce type d'audit.

J

Investigation numérique

L'investigation numérique consiste en l'analyse de l'information dans les systèmes informatiques en recherchant des preuves numériques qui peuvent être utilisées dans le cadre de procédures judiciaires, ou encore pour découvrir la cause d'un incident. Il s'agit du processus par lequel on extrait des données et des informations des systèmes informatiques dans le cadre d'enquêtes judiciaires notamment lorsque des supports numériques sont impliqués dans un crime. On note les principaux types d'investigations numériques suivants : investigation numérique judiciaire et investigation numérique en réponse à un incident.

K

Réponse aux incidents

La réponse aux incidents est l'ensemble des processus visant à se préparer, détecter, rendre compte, évaluer, réagir, prendre en charge et à tirer les enseignements des incidents de cybersécurité. Elle est souvent assurée par des équipes spécialisées communément appelées CSIRT (Computer Security Incident Response Team).

EXIGENCES RELATIVES À LA QUALIFICATION D'UN FOURNISSEUR DE SERVICES DE SÉCURITÉ NUMÉRIQUE

A Code d'éthique

Le fournisseur de services de sécurité numérique doit disposer d'un code d'éthique connu et signé par tout le personnel technique. Une copie dudit code est jointe au dossier de demande de qualification.
Le code d'éthique doit au minimum comporter les points suivants :

i. Indépendance, objectivité et impartialité

Le personnel technique doit s'efforcer non seulement d'être indépendant vis-à-vis des entités contrôlées, mais aussi d'être objectifs dans le traitement des questions et des sujets examinés. L'indépendance et l'impartialité de celui-ci doit se traduire non seulement dans les faits mais aussi en apparence. L'indépendance peut être compromise, par exemple, par :

- des pressions ou une influence externe sur le personnel technique;
- les préjugés des cadres techniques sur des personnes, des entités auditées par exemple, des projets ou des programmes ;
- un emploi antérieur récent au sein de l'entité contrôlée (moins de 02 ans) ;
- des transactions personnelles ou financières susceptibles de provoquer des conflits d'intérêts.

ii. Neutralité politique

Il est important que le personnel technique maintienne publiquement une neutralité politique afin de s'acquitter de leurs missions de manière impartiale.

iii. Secret professionnel

Le personnel technique doit absolument préserver la confidentialité des informations obtenues dans le cadre de leurs activités sauf si la divulgation est requise par une autorité judiciaire ou si l'assentiment du commanditaire est donné par écrit. Ces informations ne doivent pas être utilisées à des fins personnelles, ni communiquées à des parties inappropriées que ce soit oralement, par écrit ou à travers les médias de toute nature.

iv. Professionnalisme

Le personnel technique est tenu de se limiter aux outils, méthodes et techniques validées par le commanditaire. Il est tenu d'informer le commanditaire des résultats des travaux effectués à travers un rapport détaillé, y compris la divulgation de tous les faits importants dont il a connaissance, et qui, s'ils ne sont pas divulgués, peuvent fausser l'appréciation finale de leur rapport. Il doit réaliser et apporter les preuves d'une évaluation des risques préalables pouvant découler des services de sécurité à offrir.

B Exigences relatives à la protection de l'information

Le fournisseur de services de sécurité numérique doit tout mettre en œuvre pour protéger les informations collectées dans le cadre des services de sécurité numérique offerts. Ces informations comprennent les informations fournies par le commanditaire et celles collectées par d'autres moyens techniques et qui sont contenues dans le périmètre de ces services. Le fournisseur de services de sécurité numérique devra donc s'engager à :

- mettre en place un environnement dédié à chaque mission où sont collectées, stockées et traitées les informations recueillies ;
- détruire en présence du commanditaire toutes les données collectées et stockées dans cet environnement à la fin de la mission ;
- s'assurer que l'information relative à une mission donnée ne soit stockée dans d'autres espaces que l'environnement dédié ;
- s'assurer que le personnel technique se connecte de façon sécurisée à l'environnement dédié pour accéder à l'information relative à la mission ;
- garantir que l'information relative à une mission ne se retrouve sur des espaces privés des cadres techniques du fournisseur de services de sécurité numériques (ordinateurs, messagerie électronique, etc..) sans être chiffrée ;
- s'assurer que la transmission des documents relative à la mission se fasse à travers des canaux sécurisés.

C Exigences relatives à la protection de l'information

Le fournisseur de services de sécurité numérique doit tout mettre en œuvre pour protéger les informations collectées dans le cadre des services de sécurité numérique offerts. Ces informations comprennent les informations fournies par le commanditaire et celles collectées par d'autres moyens techniques et qui sont contenues dans le périmètre de ces services. Le fournisseur de services de sécurité numérique devra donc s'engager à :

i. Vérification du curriculum vitæ et de l'éthique

Le fournisseur de services de sécurité numérique est responsable au même titre que le personnel technique qu'il emploie, de la véracité des informations incluses dans le CV de ce dernier. En particulier, il incombe au fournisseur de services

de sécurité numérique de s'assurer que le personnel technique n'a jamais été condamné pour des crimes informatiques.
Tout personnel technique recruté doit signer la charte d'éthique du fournisseur de services de sécurité numérique lors de son engagement. Il doit bénéficier au moins une fois par an d'une formation sur le code d'éthique. Le fournisseur de services de sécurité numérique doit veiller au respect de la charte d'éthique par son personnel technique.

ii. Mise à jour des compétences

Il incombe au fournisseur de services de sécurité numérique de mettre en place un processus de mise à jour continue des compétences du personnel technique en particulier dans les domaines où il détient une qualification.
Ce processus est validé à travers un plan de formation que le fournisseur de services de sécurité numérique soumet à l'organe de contrôle des prestataires de services de confiance uniquement lors de la qualification initiale.

iii. Compétences du personnel technique

Le fournisseur de services de sécurité numérique doit s'assurer que tout le personnel technique désigné pour une mission de services de sécurité numérique a les compétences requises pour effectuer correctement les activités relatives à cette mission. Il est de la responsabilité du fournisseur de services de sécurité numérique de composer son équipe en adéquation avec les services de sécurité numérique à offrir. Le fournisseur de services de sécurité numérique doit veiller à disposer de personnel technique ayant les compétences requises pour chaque domaine où il est qualifié.

iv. Effectif du personnel technique

Le fournisseur de services de sécurité numérique doit s'assurer de confier chaque mission de services de sécurité numérique à une équipe d'au moins deux (02) cadres techniques dont un chef d'équipe.
Dès que le nombre de cadres techniques pour un service de sécurité numérique donné est inférieur à deux (02) pour un fournisseur de services de sécurité numérique, ce dernier perd automatiquement la qualification sur ce type de service.

D Exigences spécifiques relatives aux personnels du fournisseur de services de sécurité numérique

Dans le cadre de la qualification, le personnel technique est évalué et leurs compétences jouent un rôle primordial dans la qualification.
En cas de démission ou de rupture de contrat, le fournisseur de service de sécurité numérique doit informer par courrier l'organe de contrôle des prestataires de services de confiance et l'Agence des systèmes d'information et du numérique dans **un délai de trente (30) jours ouvrés.**
Le personnel technique du fournisseur de services de sécurité numérique présentés pour la qualification doit remplir les conditions ci-après :

i. Prérequis généraux

Le personnel technique impliqué dans les missions de services de sécurité numérique doit posséder les qualités personnelles ci-après :

- avoir une grande capacité d'analyse et un bon esprit critique ;
- être un bon communicateur ;
- avoir le sens du secret professionnel ;
- être loyal et de bonne foi ;
- avoir des connaissances spécifiques au secteur et au service pour lequel le candidat souhaite se faire qualifier ;
- avoir le sens de l'observation et d'écoute ;
- être autonome dans l'exécution des missions ;
- avoir l'esprit de synthèse ;
- être perspicace ;
- être rigoureux avec un grand sens de responsabilités ;
- agir avec objectivité, diligence et professionnalisme en conformité avec les standards professionnels et les meilleures pratiques ;
- maîtriser la législation et la réglementation en vigueur au Bénin en particulier dans le domaine du numérique notamment la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin et la loi n° 2020-35 du 06 janvier 2021 qui l'a modifié;

- avoir une bonne connaissance des exigences de la PSSIE et de la PPIIC ;
- avoir une bonne qualité rédactionnelle et savoir s'exprimer en français à l'oral de façon claire et compréhensible ;
- s'inscrire dans une démarche d'amélioration continue.

ii. Education et parcours

Tout le personnel technique doit avoir un diplôme de niveau BAC+3 minimum en sécurité des systèmes d'information ou équivalent avec une année d'expérience professionnelle, ou à défaut, avoir obtenu un diplôme de niveau BAC+3 minimum en informatique avec trois (03) années d'expérience dans le domaine de la sécurité des systèmes d'information.

iii. Engagement

Le personnel technique du fournisseur de services de sécurité numérique doit avoir un contrat de travail valide avec celui-ci. Il doit avoir signé la charte d'éthique élaborée par ce dernier et s'engager à respecter ses clauses.

iv. Compétences spécifiques

Des compétences spécifiques sont nécessaires par rapport à chaque domaine de services de sécurité numérique dans lequel le fournisseur de services de sécurité numérique souhaite se faire qualifier. Les exigences relatives à ces compétences spécifiques par domaine sont déclinées en annexe.

ANNEXE : COMPÉTENCES SPÉCIFIQUES PAR DOMAINE DE QUALIFICATION

Le personnel technique présenté par les fournisseurs de services de sécurité numérique doit disposer des compétences ci-dessous selon le domaine de qualification. Ces compétences sont vérifiées par l'étude du CV pour les postes occupés et les expériences accumulées, les certifications et diplômes soumis, ainsi que les différents engagements pris par les cadres techniques du forunisseur. L'analyse de ces documents peut être complétée au besoin par un entretien.

A Audit organisationnel et physique

L'auditeur en sécurité organisationnelle et physique doit disposer de compétences approfondies dans les domaines suivants :

a. Cadre normatif

- normes ISO 27001, ISO 27002, ISO 27005 ;
- textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes.

b. Organisation de la sécurité des systèmes d'information

- connaissance de la gouvernance, des normes et des standards : maîtrise des méthodologies d'audits ;
- connaissance du système d'information et des principes d'architecture ;
- maîtrise des fondamentaux dans les principaux domaines de la SSI ;
- connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO (2700X), normes sectorielles (PCI-DSS…) ;
- bonne connaissance de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) ;
- bonne connaissance de la Politique de Protection des Infrastructures d'information Critiques (PPIIC) du Bénin ;
- sécurité liée aux ressources humaines ;
- tests d'intrusion physique.

c. Maîtrise des pratiques liées à l'audit

- conduite d'entretien ;
- visite sur site ;
- analyse documentaire ;
- analyse des politiques et procédures.

Au moins une des certifications professionnelles ci-après est requise : CISA, CISM, CISSP, ISO 27001 LA, ISO 27001 LI, ISO 27005 RM, COBIT, ITIL, ou autres certifications en relation avec ce domaine.

B Audit de conformité

Les spécialistes en audit de conformité doivent disposer des compétences spécifiques ci-dessous :

a. Cadre normatif

- reporting des résultats de recherche ;
- objectivité.

c. Maîtrise des pratiques liées à l'audit

- conduite d'entretien ;
- visite sur site ;
- analyse documentaire.

Au moins une des certifications professionnelles ci-après est requise : CISA, CISSP, CISM, ISO 27001 LA, ISO 27001 LI, ISO 27005 RM, ITIL, ou autres certifications en relation avec ce domaine.

C Audit d'architecture

L'auditeur d'architecture doit disposer de compétences approfondies dans les domaines suivants :

a. Réseaux et protocoles

- Protocoles réseau et infrastructures ;
- Protocoles applicatifs courants et service d'infrastructure ;
- Configuration et sécurisation des principaux équipements réseau du marché ;
- Réseaux de télécommunication ;
- Technologie sans fil ;
- Téléphonie IP.

b. Equipements et logiciels de sécurité

- Pare-feu ;
- Système de sauvegarde ;
- Système de stockage mutualisé ;
- Dispositifs de chiffrement des communications ;
- Serveurs d'authentification ;
- Serveurs mandataires ;
- Solutions de gestion de la journalisation ;
- Équipements de détection et prévention d'intrusion.

c. Techniques et outils pour établir

- des cartographies fonctionnelles, techniques et applicatives ;
- Schémas d'architecture ;
- Architectures hautement disponibles et redondantes ;
- Mécanismes de défense en profondeur.

Au moins une des certifications professionnelles ci-après est requise : CISSP, ISSAP, GDSA, CCNP, CCIE, MSCA, MCSE, OCA, ou autres certifications en relation avec ce domaine ;

D Audit de configuration

L'auditeur de configuration doit disposer des compétences approfondies dans les domaines suivants :

a. Equipements réseau et protocoles

- Protocoles réseau et infrastructures ;
- Protocoles applicatifs courants et service d'infrastructure ;
- Configuration et sécurisation des principaux équipements réseau du marché ;
- Réseaux de télécommunications ;
- Technologies sans fil ;
- Téléphonie IP.

b. Equipements de sécurité

- Pare-feu ;
- Système de sauvegarde ;
- Système de stockage mutualisé ;
- Logiciels de sécurité côté poste client.

c. Systèmes d'exploitation

- Architectures Microsoft ;
- Systèmes UNIX/Linux ;
- Solution de virtualisation ;

d. Couche applicative

- Guides et principes de développement sécurisé ;
- Applications de type Web ou client/serveur ;
- Mécanismes cryptographiques (SSL, VPN, etc.) ;
- Socle applicatif ;
- Serveurs web ;
- Serveurs d'application ;
- Systèmes de gestion de base de données ;
- Environnements de virtualisation ;

Au moins une des certifications professionnelles ci-après est requise : CCNP, CCIE, CISA, MCSA, MCSE, CISSP ou autres certifications en relation avec ce domaine.

E Audit de code source

L'auditeur de code source doit disposer de compétences approfondies dans les domaines techniques suivants :

a. Couche applicative

- Guides et principes de développement sécurisé ;
- Architectures applicatives (client/serveur, n-tiers, etc.) ;
- Langages de programmation ;
- Mécanismes cryptographiques ;
- Mécanismes de communication (internes au système et par le réseau) et protocoles
- associés ;

b. Socle applicatif

- serveurs web ;
- serveurs d'application ;
- systèmes de gestion de bases de données ;
- progiciels ;
- méthodologies d'attaque ;
- principes et méthodes d'intrusion applicatives ;
- contournement des mesures de sécurité logicielles ;
- techniques d'exploitation de vulnérabilités et d'élévation de privilèges.

F Audit des systèmes d'information Industriels

L'auditeur des systèmes industriels doit disposer, en plus des compétences concernant les architectures et les configurations des systèmes d'information conventionnels ou de gestion, de compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base d'automates programmables (PLC) ;
- réseaux et protocoles industriels :
- topologie des réseaux industriels ;
- cloisonnement des réseaux industriels vis-à-vis des autres systèmes d'information ;
- protocoles de transmission et de communication utilisés par les automates
- programmables et équipements industriels ;

- technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la couche 802.15.4).
- configuration et sécurisation des principaux automates et équipements industriels du marché.

Au moins une des certifications professionnelles est requise : CSSA, GICSP, CISA, CISSP, CEH, ou autres certifications en relation avec ce domaine .

G Audit à blanc

Pour réaliser l'audit à blanc, l'auditeur doit disposer de compétences approfondies dans les domaines suivants :

a. Cadre normatif

- loi portant Code du numérique en République du Bénin ;
- normes ISO 27001 et ISO 27002 ;
- textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes.

a. Cadre normatif

- loi portant Code du numérique en République du Bénin ;
- normes ISO 27001 et ISO 27002 ;
- textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes.

b. Maîtrise des pratiques liées à l'audit

- conduite d'entretien ;
- visite sur site ;
- analyse documentaire.

Au moins une des certifications professionnelles ci-après est requise : CISA, ISO 27001 LA, ISO 27001 LI, ISO 27005 RM, COBIT, ITIL, ou autres certifications en relation avec ce domaine.
En plus des certifications ci-dessus citées, l'auditeur devra avoir des certifications spécifiques au domaine audité.

H Audits de vulnérabilités

La réalisation d'audits de vulnérabilités nécessite les compétences techniques dans les domaines suivants :

a. Réseau et protocoles

- protocoles réseau et infrastructures ;
- protocoles applicatifs courants et service d'infrastructure ;
- technologie sans fil ;

b. Equipements de sécurité

- pare-feu ;
- dispositif de chiffrement des communications ;
- serveur d'authentification ;
- solution de gestion de la journalisation ;
- équipement de détection et prévention d'intrusion ;
- logiciels de sécurité côté poste client ;

d. Couche applicative

- applications de type Web ou client/serveur ;
- langages de programmation utilisés pour la configuration;
- mécanismes cryptographiques (SSL, VPN, etc.) ;
- serveurs web ;
- serveurs d'application ;
- systèmes de gestion de base de données ;

Au moins une des certifications professionnelles ci-après est requise : CEH, OSCP, ECSA, CPENT, OSWE ou autres certifications en relation avec ce domaine.

I. Tests d'intrusion

L'auditeur en tests d'intrusion doit disposer des compétences approfondies dans les domaines techniques suivants :

a. Réseau et protocoles

- protocoles réseau et infrastructures ;
- protocoles applicatifs courants et service d'infrastructure ;
- technologie sans fil ;

b. Equipements de sécurité

- pare-feu ;
- dispositif de chiffrement des communications ;
- serveur d'authentification ;
- solution de gestion de la journalisation ;
- équipement de détection et prévention d'intrusion ;
- logiciels de sécurité côté poste client ;

c. Systèmes d'exploitation

- systèmes Microsoft ;
- systèmes UNIX/Linux ;
- solutions de virtualisation ;

d. Couche applicative

- applications de type Web ou client/serveur ;
- langages de programmation utilisés pour la configuration;
- mécanismes cryptographiques (SSL, VPN, etc.) ;
- serveurs web ;
- serveurs d'application ;
- systèmes de gestion de base de données ;

Au moins une des certifications professionnelles ci-après est requise : CEH, , CISSP, OSCP, ECSA, CPENT, OSWE, OSEP ou autres certifications en relation avec ce domaine

J Investigation numérique

L'investigateur numérique doit maîtriser les exigences relatives à la recherche et la collecte des preuves numériques suivant les standards nationaux et internationaux y relatifs. Il doit avoir la maîtrise des techniques des données et des informations des systèmes informatiques dans le cadre d'enquêtes judiciaires impliquant des supports numériques. De façon plus spécifique, l'investigateur doit détenir des connaissances techniques dans les principaux domaines ci-dessous :

a. Investigation réseau

- enregistrement et surveillance réseau;
- connaître les différents types de données;
- acquisition des preuves et sondes;
- connaissances de bases du réseau;
- savoir identifier une exfiltration de données.

b. Forensique Windows

- analyse des systèmes de fichiers ;
- analyse base de registre ;
- analyse VSC (Volume Shadow Copies) ;
- collecte d'artefacts applicatifs ;

c. Forensique Linux

- analyse de la mémoire vive ;
- analyse des logs systèmes et applications : historique, logins et droits

d. Investigation Web

- analyse de logs (déclinaison top 10 OWASP)
- analyse base de données
- dump mémoire
- analyse des logs, base de données et navigateurs
- acquisition logique ;
- acquisition physique ;
- analyse des différents artefacts IOS.

Au moins une des certifications professionnelles ci-après est requise : CHFI, CEH, CISSP, ISO 27037, ISO 27041 et ISO 27042 et ISO 27043 ou autres certifications en relation avec ce domaine.

K La réponse aux incidents

La réponse aux incidents est une activité majeure en ce qui concerne la protection des systèmes d'information et l'assurance de la continuité de services. Le spécialiste de la réponse aux incidents de sécurité numérique doit disposer des compétences ci-après :

- avoir une grande capacité d'analyse et un bon esprit critique ;
- être un bon communicateur ;
- avoir le sens du secret professionnel ;
- être loyal et de bonne foi ;
- avoir des connaissances spécifiques au secteur et au service pour lequel le candidat souhaite se faire qualifier ;
- avoir le sens de l'observation et d'écoute ;
- être autonome dans l'exécution des missions ;
- avoir l'esprit de synthèse ;

- être perspicace ;
- être rigoureux avec un grand sens de responsabilités ;
- agir avec objectivité, diligence et professionnalisme en conformité avec les standards professionnels et les meilleures pratiques ;
- maîtriser la législation et la réglementation en vigueur au Bénin en particulier dans le domaine du numérique notamment la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin et la loi n° 2020-35 du 06 janvier 2021 qui l'a modifié;
- avoir une bonne connaissance des exigences de la PSSIE et de la PPIIC ;
- avoir une bonne qualité rédactionnelle et savoir s'exprimer en français à l'oral de façon claire et compréhensible ;
- s'inscrire dans une démarche d'amélioration continue.

Au moins une des certifications professionnelles est requise : ECIH, CHFI, CEH, CISSP, ISO/CEI 27043, ISO/CEI 27035 ou autres certifications en relation avec ce domaine.

@asinbenin

Visiter notre site Web

https://asin.bj/