RÉFÉRENTIEL D'EXIGENCES CONCERNANT LA QUALIFICATION DES PRESTATAIRES D'AUDIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (PASSI) PRIS AU TITRE DU PARAGRAPHE C) DE L'ARTICLE 3 DE L'ORDONNANCE SOUVERAINE N° 5.664 DU 23 DÉCEMBRE 2015 CRÉANT L'AGENCE MONÉGASQUE DE SÉCURITÉ NUMÉRIQUE, MODIFIÉE.

Annexe à l'Arrêté Ministériel n° 2017-625
du 16 août 2017

ANNEXE AU « JOURNAL DE MONACO » N° 8.344

DU 25 AOÛT 2017

SOMMAIRE

I. Introduction 3

I.1. Présentation générale 3

I.1.1. Objet du document 3

I.1.2. Structure du document 3

I.2. Définitions et acronymes 3

I.2.1. Acronymes 3

I.2.2. Définitions 3

II. Activités d'audit visées par le référentiel 4

II.1. Audit d'architecture 4

II.2. Audit de configuration 5

II.3. Audit de code source 5

II.4. Tests d'intrusion 5

II.5. Audit organisationnel et physique 5

III. Qualification des prestataires d'audit 5

III.1. Modalités de la qualification 5

III.2. Portée de la qualification 6

IV. Exigences relatives au prestataire d'audit 6

IV.1. Exigences générales 6

IV.2. Charte d'éthique 7

IV.3. Gestion des ressources et des compétences 7

IV.4. Protection de l'information 8

V. Exigences relatives aux auditeurs 8

V.1. Aptitudes générales 8

V.2. Expérience 8

V.3. Aptitudes et connaissances spécifiques aux activités d'audit 9

V.4. Engagements 9

VI. Exigences relatives au déroulement d'une prestation d'audit 9

VI.1. Étape 1 - Établissement de la convention 9

VI.2. Étape 2 - Préparation et déclenchement de la prestation 12

VI.3. Étape 3 - Exécution de la prestation 13

VI.4. Exigences relatives au prestataire 13

VI.5. Étape 4 - Restitution 15

VI.6. Étape 5 - Élaboration du rapport d'audit 15

VI.7. Étape 6 - Clôture de la prestation 16

VII. Référentiel d'exigences applicables aux prestataires d'audit de la sécurité des systèmes d'information pour les besoins de la sécurité nationale 16

Appendice 1 : Documents cités en référence 17

Appendice 2 : Missions et compétences attendues du personnel du prestataire 17

Appendice 3 : Recommandations à l'intention des commanditaires d'audits 24

Appendice 4 : Échelle de classification des vulnérabilités 24

Appendice 5 : Protection des systèmes d'information des prestataires d'audit de la sécurité des systèmes d'information (PASSI) 26

I. Introduction

I.1. Présentation générale

I.1.1. Objet du document

Le présent référentiel a vocation à permettre la qualification des prestataires d'audit de la sécurité des systèmes d'information, ci-après dénommés « prestataires d'audit », selon les modalités décrites au chapitre III.

Il permet à l'entité auditée de disposer de garanties sur la compétence du prestataire d'audit et de ses auditeurs, sur la qualité des audits qu'ils effectuent, sur la capacité du prestataire d'audit à lui apporter un conseil pertinent et adapté à son contexte et sur la confiance qu'elle peut leur accorder, notamment en matière de confidentialité, avant de lui donner accès à son système et aux informations qu'il contient.

Les prestataires d'audit doivent respecter les règles générales qui leur sont imposées en leur qualité de professionnel, notamment celles concernant leur devoir de conseil vis-à-vis de leurs clients.

Le présent document liste les règles et recommandations que les « prestataires d'audit de la sécurité des systèmes d'information » (PASSI) qualifiés délivrant des prestations d'audit d'architecture, d'audit de configuration, d'audit de code source, de tests d'intrusion, d'audit organisationnel et physique et d'audit des systèmes industriels, doivent respecter.

I.1.2. Structure du document

Le chapitre II décrit les activités d'audit visées par le présent référentiel.

Le chapitre III présente les modalités de la qualification, qui atteste de la conformité du prestataire d'audit aux exigences qui lui sont applicables.

Le chapitre IV présente les exigences relatives aux prestataires d'audit.

Le chapitre V présente les exigences relatives aux auditeurs.

Le chapitre VI présente les exigences relatives au déroulement d'une prestation d'audit de la sécurité des systèmes d'information.

Le chapitre VII présente le référentiel d'exigences applicables aux prestataires d'audit pour les besoins de la sécurité nationale.

L'Appendice 1 présente les documents cités en référence.

L'Appendice 2 présente les missions et compétences attendues des auditeurs du PASSI.

L'Appendice 3 donne des recommandations à l'intention des commanditaires d'audit dans le but de les aider à exprimer leurs besoins en termes d'audit et à rédiger d'éventuels appels d'offres.

L'Appendice 4 propose une échelle de classification des vulnérabilités.

L'Appendice 5 donne des recommandations pour la protection des systèmes d'information des prestataires d'audit de la sécurité des systèmes d'information.

I.2. Définitions et acronymes

I.2.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

AMSN	Agence Monégasque de Sécurité Numérique ;
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information, française ;
COFRAC	Comité français d'accréditation ;
CA	Correspondant audit ;
PASSI	Prestataire d'audit de la sécurité des systèmes d'information ;
PSSI	**Politique de Sécurité des Systèmes d'Information ;**
RGS	Référentiel Général de Sécurité ;
RSSI	Responsable de la Sécurité des Systèmes d'Information.

I.2.2. Définitions

« **Audit** » - 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. Pour les besoins du Référentiel, un audit est constitué d'un sous-ensemble des activités d'audit de la sécurité d'un système d'information décrites au chapitre II et des recommandations assorties.

« **Audité** » - organisme(s) responsable(s) de tout ou partie du système d'information audité[1]. Le commanditaire de l'audit peut être l'audité.

[1] Exemples : prestataires d'hébergement, d'infogérance, d'exploitation et d'administration du système d'information, de tierce maintenance applicative, etc.

« **Auditeur** » - personne réalisant un audit pour le compte d'un prestataire d'audit.

« **Commanditaire de l'audit** » - organisme ou personne pour le compte duquel l'audit est mené.

« **Constats d'audit** » - résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

« **Convention d'audit** » - accord écrit entre un commanditaire d'audit et un prestataire d'audit pour la réalisation d'un audit. 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.

« **État de l'art** » - ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

« **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** » - organisme réalisant des prestations d'audit de la sécurité des systèmes d'information.

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

« **Rapport d'audit** » - document de synthèse élaboré par l'équipe d'audit et remis au commanditaire de l'audit à l'issue de l'audit. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

« **Référentiel PASSI** » - 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 des auditeurs et de leurs compétences.

« **Sécurité d'un système d'information** » - ensemble des moyens techniques et non-techniques de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

« **Services de l'État** » - sont considérés comme services de l'État : les services exécutifs de l'État, les services judiciaires, les établissements publics, les services du Palais Princier, les services municipaux, les autres organismes chargés de la gestion d'un service public administratif.

« **Système d'information** » - est qualifié de système d'information, tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

II. Activités d'audit 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 au chapitre VI.

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 est décrit au chapitre VI du présent référentiel.

L'Appendice 2 fournit des recommandations sur les types d'audit à réaliser, le périmètre de l'audit, et les compétences attendues des auditeurs.

II.1. Audit d'architecture

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 à l'état de l'art et aux exigences et règles internes de l'audité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

II.2. Audit de configuration

L'audit de configuration a pour vocation de vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de l'audité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information. Ces dispositifs peuvent notamment être des équipements réseau, des systèmes d'exploitation (serveur ou poste de travail), des applications ou des produits de sécurité.

II.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.

II.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 failles et 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.

II.5. Audit organisationnel et physique

L'audit de l'organisation de la sécurité logique et physique 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 au besoin de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur ;
- complètent correctement les mesures techniques mises en place ;
- sont efficacement mises en pratique ;
- couvrent les aspects physiques de la sécurité de l'application ou du système d'information.

II.6. Audit de systèmes industriels

L'audit de systèmes industriels consiste en l'évaluation du niveau de sécurité d'un système industriel et des dispositifs de contrôle associés. Il se compose d'un audit d'architecture, d'un audit de la configuration des éléments composant l'architecture ainsi que d'un audit organisationnel et physique.

III. Qualification des prestataires d'audit

III.1. Modalités de la qualification

Le présent référentiel contient les exigences et les recommandations à destination des prestataires d'audit. Les exigences doivent être respectées par les prestataires d'audit dans le but d'obtenir la qualification. Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet d'une quelconque vérification en vue de la qualification.

La qualification des prestataires d'audit est réalisée par le Directeur de l'Agence Monégasque de Sécurité Numérique conformément à l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée, et selon le processus suivant qui permet d'attester de la conformité du prestataire aux exigences du référentiel.

a) Le respect des exigences du référentiel par les prestataires d'audit est vérifié par un organisme de certification accrédité par le comité français d'accréditation (COFRAC) et habilité par l'Agence Monégasque de Sécurité Numérique. La liste des organismes de certification est disponible sur le site de l'Agence Monégasque de Sécurité Numérique https://amsn.gouv.mc/.

b) Aux fins de vérification du respect des exigences prescrites, l'organisme de certification :

   a. audite l'établissement[2] du prestataire d'audit en Principauté ;

   b. évalue les auditeurs du prestataire d'audit à l'aide d'examens écrits et oraux ;

[2] L'établissement correspond au lieu de travail habituel des auditeurs en Principauté. Il peut s'agir du siège social ou d'établissements secondaires.

c. observe le prestataire d'audit mener un ou plusieurs audits.

c) La qualification est attribuée, pour une durée maximale de trois ans, aux prestataires d'audit par l'Agence Monégasque de Sécurité Numérique :

a. sur avis de l'organisme de certification ;

b. après examen oral de vérification de connaissance des textes législatifs et règlementaires du prestataire d'audit candidat.

d) Un audit de surveillance est réalisé par un organisme de certification dix-huit mois après la décision de qualification.

Les prestataires d'audit candidats peuvent se procurer le règlement de qualification auprès de l'organisme de qualification.

Pour les PASSI qualifiés en France par l'ANSSI, l'Agence Monégasque de Sécurité Numérique peut prononcer leur qualification en Principauté dans la mesure où les exigences du présent référentiel sont remplies par le prestataire.

III.2. Portée de la qualification

Le prestataire d'audit peut demander la qualification pour tout ou partie des activités d'audit décrites au chapitre II. Toutefois, la qualification d'un prestataire d'audit ne portant que sur l'activité de tests d'intrusion ou que sur l'activité d'audit organisationnel et physique n'est pas autorisée, de telles activités étant jugées insuffisantes si elles sont menées seules.

La qualification est notamment accordée au regard de la compétence des auditeurs qui réaliseront les prestations qualifiées. Les auditeurs seront reconnus compétents pour tout ou partie des activités pour lequel le prestataire d'audit a demandé la qualification, à l'issue d'un processus d'évaluation par rapport à l'état de l'art. Les auditeurs ainsi que les activités d'audit pour lesquelles ils ont été reconnus compétents sont inscrits dans un registre tenu à jour par l'AMSN.

Est considérée comme une prestation qualifiée au sens du présent Référentiel, une activité d'audit telle que décrite au chapitre II réalisée par un ou plusieurs auditeurs reconnus compétents pour cette activité d'audit et travaillant pour un prestataire d'audit qualifié pour cette même activité d'audit. Une prestation d'audit qualifiée est associée à la fourniture, au commanditaire de l'audit, de recommandations destinées à élever le niveau de sécurité du système d'information de l'audité.

Les prestataires d'audit qualifiés gardent la faculté de réaliser des prestations de services en dehors du périmètre pour lequel ils sont qualifiés, mais ne peuvent, dans ce cas, se prévaloir de la qualification sur ces prestations.

Une prestation qualifiée peut être associée à d'autres prestations complémentaires (développement, intégration de produits de sécurité, etc.) sans perdre le bénéfice de la qualification.

Pour être qualifié dans le cadre de l'application de l'article 28 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, un prestataire d'audit doit, en plus des exigences du chapitre IV, répondre aux exigences supplémentaires définies au chapitre VII.

IV. Exigences relatives au prestataire d'audit

IV.1. Exigences générales

Le prestataire doit :

a) être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation ;

b) avoir au minimum deux auditeurs dont un responsable d'équipe ;

c) respecter la législation et la réglementation en vigueur sur le territoire de la Principauté ;

d) décrire l'organisation de son activité d'audit auprès du commanditaire ;

e) en sa qualité de professionnel, exercer son devoir de conseil vis-à-vis du commanditaire ;

f) assumer la responsabilité des activités qu'il réalise pour le compte du commanditaire dans le cadre de la prestation et en particulier les éventuels dommages causés au commanditaire ;

g) souscrire une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de la prestation ;

h) s'assurer du consentement du commanditaire avant toute communication d'informations obtenues ou produites dans le cadre de la prestation ;

i) garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses ;

j) 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 à l'égard du commanditaire ou de provoquer des conflits d'intérêts ;

k) réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect du commanditaire, de son personnel et de son infrastructure ;

l) disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;

m) demander au commanditaire de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité ;

n) informer le commanditaire lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale et doit l'accompagner dans cette démarche si ce dernier en fait la demande ;

o) réaliser sa prestation dans le cadre d'une convention approuvée formellement et par écrit par le commanditaire, et conforme aux exigences du chapitre VI.1.

IV.2. Charte d'éthique

Le prestataire doit disposer d'une charte d'éthique, qu'il fait appliquer aux auditeurs, 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 pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de leurs activités, sauf autorisation du commanditaire ;
- ✓ les auditeurs signalent au commanditaire tout contenu manifestement illicite découvert durant la prestation ;
- ✓ les auditeurs s'engagent à respecter la législation et la réglementation nationale en vigueur ainsi que les bonnes pratiques liées à leurs activités d'audit.

IV.3. Gestion des ressources et des compétences

Le prestataire doit :

a) employer un nombre suffisant d'auditeurs, de responsables d'équipe d'audit et éventuellement recourir à des sous-traitants pour assurer totalement et dans tous leurs aspects les activités d'audit pour lesquels il a établi des conventions de service ou marchés avec des commanditaires. Le prestataire doit s'assurer, pour chaque prestation, que les auditeurs désignés ont les qualités et les compétences requises ;

b) s'assurer du maintien à jour des compétences des auditeurs dans les types d'audits pour lesquelles ils ont obtenu une attestation individuelle de compétence. Pour cela, le prestataire dispose d'un processus de formation continue et permet à ses auditeurs d'assurer une veille technologique ;

c) en matière de recrutement, procéder à une vérification des formations, compétences et références professionnelles des auditeurs candidats et de la véracité de leur curriculum vitae. Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisés 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 assure une veille technologique sur leur mise à jour et leur pertinence (efficacité et confiance) ;

d) disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;

e) justifier, au travers des auditeurs évalués au titre de la qualification, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit citées aux chapitres II.1 à II.4, couvrant les domaines détaillés en Appendice 2 ;

f) justifier, au travers des auditeurs évalués au titre de la qualification, qu'il dispose des compétences organisationnelles, théoriques et pratiques, afférentes aux activités d'audit citées au chapitre II.5, couvrant les domaines détaillés en Appendice 2 ;

g) justifier, au travers des auditeurs évalués au titre de la qualification, qu'il maîtrise la réglementation afférente à son activité contenue au sein des lois n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, n° 1.435 du 8 novembre 2016, relative à la lutte contre la criminalité technologique et de l'arrêté ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016, modifié, portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié, ainsi que l'arrêté ministériel, à paraître ultérieurement, portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré (Référentiel Général de Sécurité et ses Annexes) et les référentiels et guides relatifs à la sécurité des systèmes d'information de l'Agence Monégasque de Sécurité Numérique (voir Appendice 1) ;

h) mettre en place un processus de sensibilisation des auditeurs à la législation en vigueur sur le territoire de la Principauté applicable à leurs missions ;

i) s'assurer que les auditeurs ne font pas l'objet d'une inscription au bulletin n° 3 du casier judiciaire ;

j) élaborer un processus disciplinaire à l'intention des auditeurs ayant enfreint les règles de sécurité ou la charte d'éthique.

IV.4. Protection de l'information

Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés en portant une mention particulière (voir Appendice 2 de l'Annexe à l'Arrêté Ministériel n° 2016-723 du 12 décembre 2016, modifié, précité).

Le système d'information que le prestataire d'audit utilise pour le traitement de ces informations doit respecter les règles relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles (voir Appendice 5).

V. Exigences relatives aux auditeurs

V.1. Aptitudes générales

a) Le responsable d'équipe d'audit doit :

- ✓ posséder les qualités personnelles identifiées au chapitre 7.2.3.4 de la norme ISO 19011 ;
- ✓ maîtriser la législation en vigueur et applicable à ses missions ainsi qu'à celles des auditeurs.

b) L'auditeur doit :

- ✓ disposer des qualités personnelles décrites au chapitre 7.2.2 de la norme ISO 19011 ;
- ✓ être sensibilisé à la législation en vigueur sur le territoire de la Principauté et applicable à ses missions ;
- ✓ disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible, en langue française ;
- ✓ régulièrement mettre à jour ses compétences conformément aux processus de formation et de veille du prestataire (voir chapitre IV.3, paragraphe b), par une veille active sur la méthodologie, les techniques et les outils utilisés dans le cadre de ses missions.

Il est recommandé que l'auditeur contribue à l'évolution de l'état de l'art par une participation à des évènements professionnels de son domaine de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Expérience

a) L'auditeur doit avoir reçu une formation en technologies des systèmes d'information.

b) Il est recommandé que l'auditeur justifie :

- ✓ d'au moins deux années d'expérience dans le domaine des systèmes d'information ;
- ✓ d'au moins une année d'expérience dans le domaine de la sécurité des systèmes d'information ;
- ✓ d'au moins une année d'expérience dans le domaine de l'audit de sécurité des systèmes d'information ;
- ✓ d'au moins deux années d'expérience dans le domaine des systèmes industriels, pour réaliser l'activité d'audit de la sécurité des systèmes industriels.

Ces recommandations ne sont pas cumulatives.

V.3. Aptitudes et connaissances spécifiques aux activités d'audit

a) L'auditeur doit :

- ✓ maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme [ISO19011] ;
- ✓ réaliser la prestation conformément aux exigences du chapitre VI ;
- ✓ assurer les missions selon son profil, telles que définies dans l'Appendice 2.

L'auditeur doit disposer des compétences requises par son profil, telles que définies dans l'Appendice 2.

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

V.4. Engagements

L'auditeur doit :

a) avoir un contrat avec le prestataire ;

b) avoir signé la charte d'éthique élaborée par le prestataire (voir chapitre IV.2).

VI. Exigences relatives au déroulement d'une prestation d'audit

La définition du périmètre de la prestation et la description de la prestation attendue, formulées généralement dans un appel d'offres, sont du ressort du commanditaire. L'Appendice 3 du référentiel fournit des recommandations à cet effet.

Bien que le prestataire ne puisse qu'adapter et moduler sa proposition de service à la demande, il doit informer, dans la mesure du possible, et à titre de conseil, le commanditaire des recommandations issues de l'Appendice 3.

Le prestataire :

- ✓ s'assure que le commanditaire lui fournit un environnement de travail adapté à ses missions ;
- ✓ vérifie que le commanditaire a identifié correctement le système audité ainsi que ses dépendances externes ;
- ✓ s'assure que la prestation est adaptée au contexte et aux objectifs souhaités par le commanditaire ;
- ✓ à défaut, en informe le commanditaire préalablement à la prestation.

Dans la suite de ce chapitre, les exigences, auxquelles doivent se conformer les prestataires, sont regroupées dans les différentes étapes du déroulement d'un audit, à savoir :

- ✓ étape 1 : établissement d'une convention ;
- ✓ étape 2 : préparation et déclenchement de la prestation ;
- ✓ étape 3 : exécution de la prestation ;
- ✓ étape 4 : restitution ;
- ✓ étape 5 : élaboration du rapport d'audit ;
- ✓ étape 6 : clôture de la prestation.

D'une manière générale, le déroulement de l'audit doit respecter les dispositions de la norme ISO 19011.

VI.1. Étape 1 - Établissement de la convention

Le prestataire doit établir une convention de service avec le commanditaire avant l'exécution de la prestation.

La convention doit être signée par un représentant légal du commanditaire et du prestataire.

VI.1.1. Modalités de la prestation

La convention de service ou marché doit :

a) 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.) ;

b) préciser si la prestation est qualifiée ;

c) préciser les livrables attendus en sortie, les réunions d'ouverture et de clôture, les publics destinataires, leur niveau de sensibilité ou de classification et les modalités associées ;

d) décrire les moyens techniques (matériel et outils) et organisationnels mis en œuvre par le prestataire dans le cadre de sa prestation ;

e) décrire les méthodes de communication qui seront employées lors de la prestation entre le prestataire, le commanditaire et l'audité ;

f) prévoir les moyens logistiques devant être mis à disposition du prestataire par le commanditaire et l'audité (moyens matériels, humains, techniques, etc.) ;

g) 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 ;

h) préciser les actions qui ne peuvent être menées sur le système d'information ou sur les informations collectées sans autorisation expresse du commanditaire et éventuellement accord ou présence du commanditaire, ainsi que les modalités associées (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensibles et des actions autorisées, etc.) ;

i) définir les moyens assurant la traçabilité entre l'audité et le prestataire des informations et supports matériels remis pour analyse.

VI.1.2. Organisation

La convention de service doit :

a) préciser le nom du correspondant audit (CA) en charge, chez l'audité si différent du commanditaire, de mettre en relation le prestataire avec les différents correspondants impliqués ;

b) préciser les noms, rôles, responsabilités ainsi que les droits et besoins d'en connaître des personnes désignées par le prestataire, le commanditaire et l'audité. Cette exigence est d'autant plus importante si l'existence d'un incident de sécurité ne doit pas être divulguée ;

c) stipuler que le prestataire doit, le cas échéant, collaborer avec des prestataires tiers qui travaillent pour le compte de l'audité et qui auront été spécifiquement désignés par le commanditaire et distinguer clairement les responsabilités du prestataire tiers. Cette exigence doit notamment permettre au prestataire de collaborer avec un prestataire de détection d'incidents de sécurité ;

d) 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, n'ayant pas obtenu une attestation individuelle de compétence ou ayant fait l'objet d'une inscription au bulletin n° 3 du casier judiciaire.

VI.1.3. Responsabilités

La convention de service doit :

a) stipuler que le prestataire ne réalisera la prestation qu'après une autorisation formelle et écrite du commanditaire ;

b) stipuler que le prestataire informe le commanditaire en cas de manquement à la convention ;

c) stipuler que le prestataire s'engage à ce que les actions réalisées dans le cadre de la prestation restent strictement en adéquation avec les objectifs de la prestation ;

d) stipuler que le commanditaire garantit disposer de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou d'avoir recueilli l'accord des éventuels tiers, et notamment de ses prestataires ou de ses partenaires, dont les systèmes d'information entreraient dans le périmètre ;

e) stipuler que le commanditaire et le prestataire remplissent toutes les obligations légales et réglementaires nécessaires aux activités d'audit ;

f) stipuler que le commanditaire autorise provisoirement le prestataire, aux seules fins de réaliser la prestation, d'accéder et de se maintenir dans tout ou partie du périmètre et d'effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données ;

g) stipuler que le commanditaire autorise provisoirement le prestataire à reproduire, collecter et analyser, aux seules fins de réaliser la prestation, des données appartenant au périmètre du système d'information cible ;

h) définir les responsabilités et les précautions d'usage à respecter par l'ensemble des parties concernant les risques potentiels 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 ;

i) stipuler si le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés lors de la réalisation des activités d'audit et, le cas échéant, préciser la couverture de celle-ci et inclure l'attestation d'assurance.

VI.1.4. Confidentialité

La convention de service ou marché doit :

a) 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 ;

b) stipuler que le prestataire peut, sauf refus formel et écrit du commanditaire, conserver certains types d'informations liées à la prestation une fois celle-ci terminée. Le prestataire devra identifier ces types d'informations dans la convention (ex : livrables, informations, documents, etc.) ;

c) stipuler que le prestataire anonymise et décontextualise (suppression de toute information permettant d'identifier le commanditaire, de toute information à caractère personnel, etc.) l'ensemble des informations que le commanditaire l'autorise à conserver ;

d) stipuler que le prestataire détruit, de manière irréversible, l'ensemble des informations relatives au commanditaire à l'issue de la prestation à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire ;

e) préciser les modalités (contenu, forme, portée, etc.) de rédaction des recommandations ;

f) Il est recommandé que la convention prévoie une procédure de recueil du consentement des audités et des éventuels partenaires pour la réalisation de l'audit.

VI.1.5. Lois et réglementations

La convention de service ou marché doit :

a) être rédigée en français. Le prestataire doit fournir une traduction de courtoisie de la convention de service si le commanditaire en fait la demande ;

b) stipuler que seule la version française fait foi, notamment dans le cadre d'un litige ;

c) stipuler que la législation applicable à la convention de service est la législation monégasque ;

d) préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour le respect de la législation monégasque applicable notamment ceux concernant :

- ✓ les données à caractère personnel [LOI_1165] ;
- ✓ la protection des données relatives à la sécurité nationale [LOI_1430] ;
- ✓ les obligations des Opérateurs d'Importance Vitale [LOI_1435] ;
- ✓ le secret professionnel [CP_ART_308] ;
- ✓ le secret des correspondances privées [CP_ART_341] ;
- ✓ l'atteinte à la vie privée [CP_ART_308-2] ;
- ✓ les délits relatifs aux systèmes d'information [CP_ART_389-1] ;

e) préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité ;

f) prévoir les exigences à respecter par le prestataire dans le cadre d'une affaire judiciaire, civile ou arbitrale ;

g) définir la durée de conservation des informations liées à la prestation et notamment les évènements collectés et les incidents de sécurité détectés. Si besoin, une distinction de la durée de conservation peut être faite en fonction des types d'information. La durée minimale de conservation est de six mois sous réserve de la législation et de la réglementation monégasque en vigueur.

VI.1.6. Sous-traitance

a) La convention doit préciser que le prestataire peut sous-traiter une partie des activités à un autre prestataire qualifié sur ces activités conformément aux exigences du référentiel qui lui sont applicables sous réserve que :

- ✓ il existe une convention ou un cadre contractuel documenté entre le prestataire et son sous-traitant ;
- ✓ le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire.

b) La convention doit préciser que le prestataire peut faire intervenir un expert sur une partie des activités, pour des besoins ponctuels, sous réserve que :

- ✓ il existe une convention ou un cadre contractuel documenté entre le prestataire et l'expert ;
- ✓ le recours à un expert est connu et formellement accepté par écrit par le commanditaire ;
- ✓ l'expert est encadré par le responsable de l'équipe d'audit.

VI.1.7. Livrables

La convention de service ou marché doit préciser que tous les livrables produits par le prestataire au titre de la prestation sont fournis en langue française sauf si le commanditaire en fait la demande formelle et écrite.

VI.1.8. Qualification

La convention de service ou marché doit :

a) indiquer que la prestation réalisée est :

- ✓ une prestation qualifiée et inclure l'attestation de qualification du prestataire et des éventuels sous-traitants ;
- ✓ une prestation non qualifiée. Dans ce cas, le prestataire doit sensibiliser le commanditaire aux risques de ne pas exiger une prestation qualifiée ;

b) indiquer que les auditeurs disposent d'une attestation individuelle de compétence pour les activités d'audit et inclure ces attestations.

VI.2. Étape 2 - Préparation et déclenchement de la prestation

a) Le prestataire doit nommer un responsable d'équipe d'audit pour tout audit qu'il effectue ;

b) Le responsable d'équipe d'audit doit :

- ✓ constituer une équipe d'auditeurs ayant les compétences adaptées à la nature de l'audit. Le responsable d'équipe d'audit peut, s'il dispose des compétences suffisantes, réaliser l'audit lui-même et seul,
- ✓ dès le début de la préparation de l'audit, établir un contact avec le Correspondant d'Audit (CA). Ce contact, formel ou informel, a notamment pour objectif de mettre en place les circuits de communication et de décision et de préciser les modalités d'exécution de la prestation. Il doit également obtenir du CA la liste des points de contact nécessaires à la réalisation de la prestation,
- ✓ s'assurer auprès du commanditaire et de l'audité que les représentants légaux des entités impactées par l'audit ont été préalablement avertis et qu'ils ont donné leur accord,
- ✓ élaborer 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 et notamment celles éventuellement menées chez l'audité, 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 ;

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

d) En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, au préalable, toute la documentation existante de l'audité (exemples : 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 ;

e) L'audit ne doit débuter qu'après une réunion formelle 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. Cette réunion peut être téléphonique mais doit, dans ce cas, faire l'objet d'une confirmation écrite ;

f) Le prestataire doit sensibiliser avant l'audit son client sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées ;

g) Au préalable, et dans le cas spécifique des tests d'intrusion, une fiche d'autorisation doit être signée par le commanditaire, l'audité et d'éventuelles tierces parties. Elle précise en particulier :

- ✓ la liste des cibles auditées (adresses IP, noms de domaine, etc.) ;
- ✓ la liste des adresses IP de provenance des tests ;
- ✓ la date et les heures exclusives des tests ;
- ✓ la durée de l'autorisation.

VI.3. Étape 3 - Exécution de la prestation

a) Le responsable d'équipe d'audit doit tenir informé le commanditaire 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.

b) L'audit doit être réalisé dans le respect des personnels et des infrastructures physiques et logiques de l'audité.

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

d) Les auditeurs doivent rendre compte des constats d'audit au responsable d'équipe d'audit, lequel peut en avertir sans délai sa hiérarchie ainsi que l'audité, dans le respect des clauses de confidentialité fixées dans la convention d'audit.

e) 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.

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

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

h) 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.

VI.4. Exigences relatives au prestataire

Lorsqu'elles sont demandées par le commanditaire, les activités d'audit réalisées par le prestataire doivent être conformes aux exigences précisées dans les chapitres VI.4.1 à VI.4.5.

Le cas échéant, conformément à la PSSI-E, il est recommandé d'utiliser des produits qualifiés.

Remarques :

- ✓ les activités techniques décrites dans les paragraphes VI.4.1 à VI.4.4 n'excluent pas l'évaluation de l'organisation de la sécurité logique et physique des éléments audités. Cette évaluation consiste en la vérification que les politiques de sécurité et procédures définies pour assurer le maintien en conditions de sécurité du système d'information audité sont conformes à l'état de l'art ;
- ✓ les énumérations listées dans les chapitres VI.4.1 à VI.4.5 sont données à titre indicatif et ne sont pas exhaustives. Par ailleurs, elles ne doivent être réalisées que lorsqu'elles sont applicables à la cible auditée.

VI.4.1. Audit d'architecture

a) Le prestataire doit procéder à la revue des documents suivants lorsqu'ils existent :

- ✓ schémas d'architectures de niveau 2 et 3 du modèle OSI ;
- ✓ matrices de flux ;
- ✓ règles de filtrage ;
- ✓ configuration des équipements réseau (routeurs et commutateurs) ;
- ✓ interconnexions avec des réseaux tiers ou Internet ;
- ✓ analyses de risques système ;
- ✓ documents d'architecture technique liés à la cible.

b) Le prestataire doit pouvoir organiser des entretiens avec le personnel concerné par la mise en place et l'administration de la cible auditée, notamment en ce qui concerne les procédures d'administration.

VI.4.2. Audit de configuration

a) Les éléments de configuration des cibles auditées doivent être fournis au prestataire. Ils peuvent être récupérés manuellement ou automatiquement, à partir d'un accès privilégié sur les cibles auditées, sous la forme de fichiers de configuration ou de captures d'écran.

Cette action peut être entreprise directement par l'auditeur après accord de l'audité.

Il est recommandé que le prestataire vérifie, conformément à l'état de l'art ou aux exigences et règles spécifiques de l'audité, la sécurité des configurations :

- ✓ des équipements réseau filaire ou sans fil de type commutateurs ou routeurs ;

- ✓ des équipements de sécurité (type pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage, chiffreurs, etc.) ;
- ✓ des systèmes d'exploitation ;
- ✓ des systèmes de gestion de bases de données ;
- ✓ des services d'infrastructure ;
- ✓ des serveurs d'applications ;
- ✓ des postes de travail ;
- ✓ des équipements de téléphonie ;
- ✓ des environnements de virtualisation.

b) Le prestataire doit pouvoir organiser des entretiens avec le personnel concerné par la mise en place et l'administration de la cible auditée, notamment en ce qui concerne les standards de configuration.

VI.4.3. Audit de code source

a) Le code source, la documentation relative à la mise en œuvre, les méthodes et rapports de tests et l'architecture du système d'information audité doivent être fournis au prestataire ainsi que la configuration des éléments de compilation et d'exécution, dans les limites des droits dont disposent le commanditaire et l'audité.

b) Il est recommandé de procéder à des entretiens avec un développeur ou le responsable de la mise en œuvre du code source audité afin de disposer d'informations relatives au contexte applicatif, aux besoins de sécurité et aux pratiques liées au développement.

c) Il est recommandé que l'audit de code fasse préalablement l'objet d'une analyse de la sécurité de l'application auditée afin de limiter l'audit aux parties critiques de son code.

d) Il est recommandé que le prestataire vérifie la sécurité des parties du code source relatives :

- ✓ aux mécanismes d'authentification ;
- ✓ aux mécanismes cryptographiques ;
- ✓ à la gestion des utilisateurs ;
- ✓ au contrôle d'accès aux ressources ;
- ✓ aux interactions avec d'autres applications ;
- ✓ aux relations avec les systèmes de gestion de bases de données ;
- ✓ à la conformité à des exigences de sécurité relative à l'environnement dans laquelle est déployée l'application.

e) Il est recommandé que le prestataire recherche les vulnérabilités les plus répandues dans les domaines suivants : cross-site scripting, injections SQL, cross-site request forgery, erreurs de logique applicative, débordement de tampon, exécution de commandes arbitraires, inclusion de fichiers (locaux ou distants).

L'audit de code source doit permettre d'éviter les fuites d'information et les altérations du fonctionnement du système d'information.

f) Les audits de code source peuvent être réalisés manuellement ou automatiquement par des outils spécialisés. Les phases automatisées, ainsi que les outils utilisés, doivent être identifiés dans les livrables et en particulier dans le rapport d'audit.

VI.4.4. Tests d'intrusion

a) L'équipe d'audit en charge de la réalisation d'un test d'intrusion sur une cible donnée peut effectuer une ou plusieurs des phases suivantes :

- ✓ phase boîte noire : l'auditeur ne dispose d'aucune autre information que les adresses IP et URL associées à la cible auditée. Cette phase est généralement précédée de la découverte d'informations et l'identification de la cible par interrogation des services DNS, par le balayage des ports ouverts, par la découverte de la présence d'équipements de filtrage, etc ;
- ✓ phase boîte grise : les auditeurs disposent des connaissances d'un utilisateur standard du système d'information (authentification légitime, poste de travail « standard », etc.). Les identifiants peuvent appartenir à des profils d'utilisateurs différents afin de tester des niveaux de privilèges distincts ;
- ✓ phase boîte blanche : les auditeurs disposent du maximum d'informations techniques (architecture, code source, contacts téléphoniques, identifiants, etc.) avant de démarrer l'analyse. Ils ont également accès à des contacts techniques liés à la cible.

Si plusieurs de ces prestations sont effectuées, il est recommandé de préserver l'ordre d'exécution décrit ci-dessus.

b) Le prestataire et le commanditaire doivent, préalablement à tout test d'intrusion, définir un profil d'attaquant simulé.

c) Le prestataire doit avoir un contact permanent avec l'audité et l'auditeur doit prévenir le commanditaire et l'audité avant toute action qui pourrait entraîner un dysfonctionnement, voire un déni de service de la cible auditée.

d) Lorsqu'elles sont connues pour rendre la cible auditée instable voire provoquer un déni de service, les vulnérabilités découvertes ne devraient pas être exploitées sauf accord du commanditaire et de l'audité. L'absence de tentative d'exploitation de telles vulnérabilités doit être indiquée et justifiée dans le rapport d'audit.

e) Les vulnérabilités non publiques découvertes lors de l'audit doivent être communiquées à l'Agence Monégasque de Sécurité Numérique.

VI.4.5. Audit organisationnel et physique

a) Le prestataire doit analyser l'organisation de la sécurité des systèmes d'information sur la base des référentiels techniques et réglementaires en accord avec les réglementations et méthodes applicables dans le domaine d'activité de l'audité.

b) L'audit organisationnel et physique doit permettre de mesurer la conformité du système d'information audité par rapport aux référentiels et identifier les écarts présentant les vulnérabilités majeures du système audité.

c) Cet audit peut intégrer l'analyse des éléments liés à la sécurité des aspects physiques des systèmes d'information et notamment la protection des locaux hébergeant les systèmes d'information et les données de l'audité ou le contrôle d'accès de ces locaux.

VI.4.6. Audit d'un système industriel

a) Le prestataire doit réaliser les activités suivantes sur le périmètre du système industriel et le cas échéant de son centre de contrôle :

- ✓ audit de l'architecture ;
- ✓ audit de configuration des composants ;
- ✓ audit organisationnel et physique ;

b) Le prestataire doit pouvoir organiser des entretiens avec le personnel concerné par la sécurité du système industriel, notamment le RSSI, le responsable opérationnel du système et le cas échéant, les correspondants techniques.

c) Il est recommandé au prestataire de sensibiliser le commanditaire aux risques de la réalisation de tests d'intrusion sur un environnement comportant des systèmes industriels.

VI.5. Étape 4 - Restitution

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 et le commanditaire des constats et des premières conclusions de l'audit.

Le cas échéant, il présente les vulnérabilités majeures et critiques qui nécessiteraient une action rapide et décrit les recommandations associées.

VI.6. Étape 5 - Élaboration du rapport d'audit

a) Le prestataire doit, pour toute prestation, élaborer un rapport d'audit et le transmettre au commanditaire.

b) Le prestataire doit mentionner explicitement dans le rapport d'audit si la prestation réalisée est une prestation qualifiée.

c) rapport d'audit doit contenir en particulier :

- ✓ une synthèse, compréhensible par des non experts, qui précise ;
  - le contexte et le périmètre de la prestation ;
  - les vulnérabilités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
  - l'appréciation du niveau de sécurité du système d'information audité par rapport à l'état de l'art et en considération du périmètre d'audit.
- ✓ un tableau synthétique des résultats de l'audit, qui précise :
  - la synthèse des vulnérabilités relevées, classées selon une échelle de valeur ;
  - la synthèse des mesures correctives proposées, classées par criticité et par complexité ou coût estimé de correction ;
- ✓ lorsque réalisés, une description du déroulement linéaire des tests d'intrusion et de la méthodologie employée pour détecter les vulnérabilités et, le cas échéant, les exploiter ;
- ✓ une analyse de la sécurité du système d'information audité, qui présente les résultats des différentes activités d'audit réalisées.

d) Le rapport d'audit doit être adapté en fonction de l'activité d'audit réalisée par le prestataire.

e) Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, doivent être classées en fonction de leur impact sur la sécurité du système d'information et leur difficulté d'exploitation.

Il est recommandé d'utiliser l'échelle proposée en Appendice 4. À défaut, le prestataire doit être en mesure de proposer une échelle pertinente.

f) Chaque vulnérabilité doit être associée à une ou plusieurs recommandations adaptées au système d'information de l'audité. Les recommandations décrivent les solutions permettant de résoudre temporairement ou définitivement la vulnérabilité et d'améliorer le niveau de sécurité.

g) Le rapport d'audit peut également présenter des recommandations générales non associées à des vulnérabilités et destinées à conseiller l'audité pour les actions liées à la sécurité de son système d'information qu'il entreprend.

h) Le rapport d'audit doit mentionner les réserves relatives à l'exhaustivité des résultats de l'audit (liées aux délais alloués, à la disponibilité des informations demandées, à la collaboration de l'audité, etc.) ou à la pertinence de la cible auditée.

i) Le rapport d'audit doit mentionner les noms et coordonnées des auditeurs, responsables d'équipe d'audit et commanditaires de l'audit.

j) Le rapport d'audit doit mentionner s'il s'agit d'une prestation d'audit qualifiée et préciser les activités d'audit associées.

VI.7. Étape 6 - Clôture de la prestation

a) Il est recommandé qu'une réunion de clôture de l'audit soit organisée avec le commanditaire et l'audité suite à la livraison du rapport d'audit. Cette réunion permet de présenter la synthèse du rapport d'audit, des scénarios d'exploitation de certaines failles, des recommandations et d'organiser un jeu de questions / réponses. Elle est également l'occasion d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres solutions plus aisées à mettre en œuvre.

b) Le responsable d'équipe d'audit doit demander à l'audité de signer un document attestant que le système d'information qui a été audité est, à l'issue de l'audit, dans un état dont la sécurité n'est pas dégradée par rapport à l'état initial, dégageant ainsi, dans le principe, la responsabilité des auditeurs et du prestataire de tout problème postérieur à l'audit.

c) 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 à la convention d'audit. Le cas échéant, le responsable d'audit produit un procès-verbal de destruction de ces données qu'il remet à l'audité et précisant les données détruites et leur mode de destruction.

d) Afin qu'il puisse s'assurer de la pertinence des mesures correctives mises en œuvre pour corriger les vulnérabilités découvertes lors de l'audit, le commanditaire peut demander au prestataire la fourniture des développements spécifiques autonomes réalisés lors de l'audit pour valider les scénarios d'exploitation des vulnérabilités. Ces développements peuvent être fournis sous la forme de scripts ou de programmes compilés, accompagnés de leur code source, ainsi que d'une brève documentation de mise en œuvre et d'utilisation. Les modalités relatives à cette mise à disposition sont précisées dans la convention.

e) La prestation est considérée comme terminée lorsque toutes les activités prévues ont été réalisées et que le commanditaire a reçu et attesté, formellement et par écrit, que le rapport d'audit est conforme aux objectifs visés dans la convention.

f) Il est recommandé que le prestataire propose au commanditaire d'effectuer ultérieurement un audit de validation afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

VII. Référentiel d'exigences applicables aux prestataires d'audit de la sécurité des systèmes d'information pour les besoins de la sécurité nationale

Ce chapitre définit les exigences applicables à un prestataire d'audit (PASSI) délivrant des prestations pour les besoins de la sécurité nationale, dans le cadre de l'application de l'article 28 de la loi n° 1.435 du 8 novembre 2016, précitée.

La liste des systèmes d'information d'importance vitale et les rapports d'audit sont couverts par le secret de sécurité nationale. Ces prestataires de service seront donc amenés à manipuler de telles informations.

Un prestataire d'audit de la sécurité des systèmes d'information pour les besoins de la sécurité nationale doit :

- ✓ satisfaire les exigences du présent référentiel ;
- ✓ être habilité en tant que personne morale au niveau Confidentiel de Sécurité Nationale ou équivalent dans un autre pays ayant signé un Accord Général de Sécurité avec la Principauté ;

- ✓ disposer d'au moins un auditeur habilité au niveau Confidentiel de Sécurité Nationale ou équivalent dans un autre pays ayant signé un Accord Général de Sécurité avec la Principauté et disposant d'une attestation de compétence pour chacune des activités d'audit qu'il assurera pour les besoins de la sécurité nationale ;
- ✓ disposer, sur le territoire de la Principauté, de locaux aptes à traiter de l'information au niveau Confidentiel de Sécurité Nationale ou utiliser les locaux aptes à traiter de l'information au niveau Confidentiel de Sécurité Nationale de l'audité si besoin ;
- ✓ disposer d'un système d'information homologué au niveau Confidentiel de Sécurité Nationale ou utiliser un système d'information homologué au niveau Confidentiel de Sécurité Nationale de l'audité si besoin.

Appendice 1 :

Documents cités en référence

Norme internationale ISO/IEC 17020 :1998 : Critères généraux pour le fonctionnement de différents types d'organismes procédant à l'inspection.

Norme internationale ISO/IEC 19011 :2002 : Lignes directrices pour l'audit des systèmes de management de la qualité ou de management environnemental.

Norme internationale ISO/IEC 27001 : 2005 : Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences.

Norme internationale ISO/IEC 27002 : 2005 : Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information.

Norme internationale ISO/IEC 27011 : 2008 : Lignes directrices de la gestion de la sécurité de l'information pour les télécoms.

Guides de l'Agence Monégasque de Sécurité Numérique et de l'ANSSI publiés sur les sites respectifs https://amsn.gouv.mc et https://www.ssi.gouv.fr et notamment :

- ✓ Méthode de gestion de risques EBIOS 2010 ;
- ✓ Méthodologie d'analyse de risque et de rédaction d'objectifs de sécurité ;
- ✓ Guide d'hygiène informatique ;
- ✓ Modèle de politique de sécurité des systèmes d'information ;
- ✓ Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information ;
- ✓ Guide d'intégration de la sécurité des systèmes d'information dans les projets ;
- ✓ Guide relatif à la maturité SSI ;
- ✓ Guide de l'externalisation ;
- ✓ La défense en profondeur appliquée aux systèmes d'information ;
- ✓ Sécurité et langage Java (Javasec).

Guides et documentation de l'Open Web Application Security Project (OWASP). Guides de développement sécurisé Microsoft[3] .

Guides de développement sécurité Java[4] .

Guides de l'ENISA, notamment Technical Guideline for Minimum Security Measures.

Appendice 2 :

Missions et compétences attendues du personnel du prestataire

I. Responsable d'équipe d'audit

I.1. Missions

Le responsable d'équipe d'audit doit assurer les missions suivantes :

- ✓ mettre en œuvre une organisation adaptée aux objectifs de la prestation (voir chapitre VI.2) ;
- ✓ structurer l'équipe d'auditeurs (compétences, effectif) ;
- ✓ assurer la définition, le pilotage et le contrôle des activités des auditeurs (voir chapitre VI.3) ;
- ✓ mettre en œuvre les moyens adaptés aux objectifs de la prestation (voir chapitre VI.2) ;
- ✓ définir et gérer les priorités ;
- ✓ maintenir à jour un état de la progression de l'audit et présenter l'information utile au commanditaire ;
- ✓ soutenir l'audité dans l'évaluation des impacts métier associés menaces pouvant potentiellement exploiter les vulnérabilités découvertes au cours de la prestation, notamment en matière de confidentialité, d'intégrité et de disponibilité ;

[3] http://msdn.microsoft.com/fr-fr/library/ms954624.aspx

[4] http://www.oracle.com/technetwork/java/seccodeguide-139067.html

✓ proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;

✓ contrôler la qualité des productions ;

✓ valider les livrables.

I.2. Compétences

Le responsable d'équipe d'audit doit avoir des compétences approfondies dans la plupart des domaines requis pour les auditeurs qu'il encadre.

Il doit par ailleurs avoir les qualités suivantes :

✓ savoir piloter des équipes d'auditeurs ;

✓ savoir définir et gérer les priorités ;

✓ savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;

✓ savoir rédiger des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.).

I.3. Compétences requises pour l'audit de systèmes industriels

Le responsable d'équipe d'audit de systèmes industriels doit de plus disposer de compétences approfondies dans les domaines techniques suivants :

✓ architectures fonctionnelles à base d'automate programmable industriel ;

✓ 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 (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850),
- technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la couche 802.15.4) ;

✓ rôle fonctionnel des différents équipements.

II. Auditeur d'architecture

II.1. Missions

L'auditeur d'architecture doit assurer les missions suivantes :

✓ adopter une vision globale du système d'information afin d'identifier :

- les vulnérabilités et les éventuels chemins d'attaque associés,
- les éléments pertinents à auditer ;

✓ collecter les éléments de configuration des équipements réseau à auditer ;

✓ auditer la configuration des équipements réseau préalablement choisis ;

✓ développer des outils adaptés à la cible auditée, le cas échéant ;

✓ mener les entretiens avec les administrateurs réseau ;

✓ identifier les vulnérabilités présentes dans l'architecture et dans la configuration des équipements audités ;

✓ proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;

✓ capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

II.2. Compétences

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

✓ 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 ;

- ✓ équipements et logiciels de sécurité :
  - pare-feu,
  - système de sauvegarde,
  - système de stockage mutualisé,
  - dispositifs de chiffrement des communications,
  - serveurs d'authentification,
  - serveurs mandataires inverses,
  - solutions de gestion de la journalisation,
  - équipements de détection et prévention d'intrusion.

Il doit par ailleurs avoir les qualités suivantes :

- ✓ savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- ✓ savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- ✓ savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

II.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur d'architecture de systèmes industriels doit de plus disposer de compétences approfondies dans les domaines techniques suivants :

- ✓ architectures fonctionnelles à base de 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 (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850),
  - technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la couche 802.15.4) ;
- ✓ rôle fonctionnel des différents équipements.

III. Auditeur de configuration

III.1. Missions

L'auditeur de configuration doit assurer les missions suivantes :

- ✓ adopter une vision globale du système d'information afin :
  - de comprendre le rôle de l'infrastructure à auditer,
  - d'identifier les éléments pertinents à auditer ;
- ✓ collecter les éléments de configuration des éléments à auditer ;
- ✓ auditer la configuration des éléments préalablement choisis ;
- ✓ développer des outils adaptés à la cible auditée, le cas échéant ;
- ✓ mener les entretiens avec les administrateurs système et/ou applicatifs ;
- ✓ identifier les vulnérabilités présentes dans la configuration des éléments audités ;
- ✓ proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- ✓ capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

III.2. Compétences

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

- ✓ 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 ;

- ✓ équipements et logiciels de sécurité :
  - pare-feu,
  - système de sauvegarde,
  - système de stockage mutualisé,
  - dispositif de chiffrement des communications,
  - serveur d'authentification,
  - serveur mandataire inverse,
  - solution de gestion de la journalisation,
  - équipement de détection et prévention d'intrusion,
  - logiciels de sécurité côté poste client ;
- ✓ systèmes d'exploitation (environnement et durcissement) :
  - systèmes Microsoft,
  - systèmes UNIX/Linux,
  - systèmes centralisés (basés par exemple sur OS400 ou zOS),
  - solution de virtualisation ;
- ✓ couche applicative :
  - applications de type client/serveur,
  - langages de programmation utilisés pour la configuration (ex : scripts, filtres WMI, etc.),
  - mécanismes cryptographiques,
  - socle applicatif :
    - o serveurs web,
    - o serveurs d'application,
    - o systèmes de gestion de bases de données,
    - o progiciels ;
- ✓ techniques d'intrusion.

Il doit par ailleurs avoir les qualités suivantes :

- ✓ savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- ✓ savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- ✓ savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

III.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur de configuration de systèmes industriels doit de plus disposer de compétences approfondies dans les domaines techniques suivants :

- ✓ réseaux et protocoles industriels :
  - protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850),
  - technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la couche 802.15.4) ;
- ✓ équipements :
  - configuration et sécurisation des principaux automates et équipements industriels du marché.

IV. Auditeur de code source

IV.1. Missions

L'auditeur de code source doit assurer les missions suivantes :

- ✓ adopter une vision globale du système d'information afin de comprendre le rôle de l'application à auditer ;
- ✓ identifier au sein de l'application les éléments pertinents à auditer au sein du code source ;
- ✓ auditer le code source ;
- ✓ développer des outils adaptés à la cible auditée, le cas échéant ;
- ✓ employer des techniques d'ingénierie inverse, le cas échéant ;
- ✓ mener les entretiens avec les développeurs, le cas échéant ;
- ✓ identifier les vulnérabilités présentes dans le code source ;

✓ proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;

✓ capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

IV.2. Compétences

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

✓ couche applicative :

- guides et principes de développement sécurité,
- 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,
- socle applicatif :
  - o serveurs web,
  - o serveurs d'application,
- systèmes de gestion de bases de données,
- Progiciels ;

✓ attaques :

- principes et méthodes d'intrusion applicatives,
- contournement des mesures de sécurité logicielles,
- techniques d'exploitation de vulnérabilités et d'élévation de privilèges.

Il doit par ailleurs avoir les qualités suivantes :

✓ savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;

✓ savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;

✓ savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

IV.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur de code source d'applications présentes dans des systèmes industriels doit de plus disposer de compétences approfondies dans les domaines techniques suivants :

✓ architectures fonctionnelles à base de PLC ;

✓ architectures applicatives SCADA (basées ou non sur un progiciel) ;

✓ architectures applicatives des programmes utilisateur présents dans les automates programmables industriels ;

✓ réseaux et protocoles industriels :

- protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850).

V. Auditeur en tests d'intrusion

V.1. Missions

L'auditeur en tests d'intrusion doit assurer les missions suivantes :

✓ adopter une vision globale du système d'information afin d'identifier :

- les cibles pertinentes à attaquer (exemples : documents métier, données sensibles, serveurs sensibles, etc.),
- les scénarios d'attaque adaptés ;

✓ identifier au sein de l'infrastructure les éléments à attaquer permettant d'exécuter les scénarios d'attaque choisis ;

✓ réaliser des attaques pertinentes sur l'infrastructure cible ;

✓ développer des outils adaptés à la cible attaquée, le cas échéant ;

✓ employer des techniques d'ingénierie inverse, le cas échéant ;

✓ identifier les vulnérabilités présentes dans tout élément de l'infrastructure permettant de mener à bien les attaques ;

✓ proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;

✓ capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

V.2. Compétences

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

✓ 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 ;

✓ équipements et logiciels de sécurité :

- pare-feu,
- système de sauvegarde,
- système de stockage mutualisé,
- dispositif de chiffrement des communications,
- serveur d'authentification,
- serveur mandataire inverse,
- solution de gestion de la journalisation,
- équipement de détection et prévention d'intrusion,
- logiciels de sécurité côté poste client ;

✓ systèmes d'exploitation :

- systèmes Microsoft,
- systèmes UNIX/Linux,
- systèmes centralisés (basés par exemple sur OS400 ou zOS),
- solutions de virtualisation ;

✓ couche applicative :

- guides et principes de développement sécurité,
- applications de type client/serveur,
- langages de programmation dans le cadre d'audits de code,
- mécanismes cryptographiques,
- mécanismes de communication (internes au système et par le réseau) et protocoles associés,
- socle applicatif :
  - o serveurs web,
  - o serveurs d'application,
  - o systèmes de gestion de bases de données,
  - o progiciels ;

✓ attaques :

- principes et méthodes d'intrusion applicatives,
- contournement des mesures de sécurité logicielles,
- techniques d'exploitation de vulnérabilités et d'élévation de privilèges.

Il doit par ailleurs avoir les qualités suivantes :

✓ savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;

✓ savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;

✓ savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

V.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur en tests d'intrusion de systèmes industriels doit de plus disposer de compétences approfondies dans les domaines techniques suivants :

✓ architectures fonctionnelles à base de 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 (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850),
- technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la couche 802.15.4) ;

✓ équipements :

- configuration et sécurisation des principaux automates et équipements industriels du marché.

VI. Auditeur en sécurité organisationnelle et physique

VI.1. Missions

L'auditeur en sécurité organisationnelle et physique doit assurer les missions suivantes :

✓ adopter une vision globale de l'organisation afin d'identifier :

- les politiques et processus pertinents à auditer,
- les lieux pertinents à auditer,
- les vulnérabilités et les éventuels chemins d'attaque physiques associés ;

✓ collecter les documents associés aux processus à auditer ;

✓ auditer les processus et lieux préalablement choisis ;

✓ mener les entretiens avec les responsables de processus et responsables de la sureté ;

✓ identifier les vulnérabilités présentes dans les processus et l'architecture physique des lieux audités ;

✓ proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;

✓ capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

VI.2. Compétences

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

✓ maîtrise des référentiels techniques ;

✓ maîtrise du cadre normatif :

- les normes [ISO27001] et [ISO27002],
- les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes.

✓ maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :

- analyse des risques,
- politique de sécurité des systèmes d'information,
- chaines de responsabilités en sécurité des systèmes d'information,
- sécurité liée aux ressources humaines,
- gestion de l'exploitation et de l'administration du système d'information,
- contrôle d'accès logique au système d'information,
- développement et maintenance des applications,
- gestion des incidents liés à la sécurité de l'information,
- gestion du plan de continuité de l'activité,
- sécurité physique ;

✓ maîtrise des pratiques liées à l'audit :

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

Il doit par ailleurs avoir les qualités suivantes :

✓ savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;

✓ savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;

✓ savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

VI.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur en sécurité organisationnelle et physique doit être familier avec les sujets suivants :

- ✓ normes de sécurité fonctionnelle telle que l'IEC 61508 ;
- ✓ architectures fonctionnelles à base de PLC ;
- ✓ rôles et utilisation des protocoles industriels ;
- ✓ connaissance du rôle fonctionnel des différents équipements.

Appendice 3 :

Recommandations à l'intention des commanditaires d'audits

Cet Appendice liste les recommandations à l'intention des commanditaires d'audits, dans le cadre de la passation de marchés publics ou d'un accord contractuel, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil.

L'Agence Monégasque de Sécurité Numérique peut être consultée pour participer à la définition du cahier des charges des audits faisant l'objet d'un appel d'offres par les « services de l'État » ou pour les OIV.

1. Recommandations générales

a) Il est recommandé que le prestataire d'audit puisse fournir des références permettant d'estimer de sa compétence : références clients, participation à des programmes de recherche, etc.

b) Les audits devraient être le plus exhaustif possible, tout en tenant compte des contraintes temporelles et budgétaires allouées à l'audit.

c) La durée de l'audit demandé par les commanditaires d'audits devrait être adaptée en fonction :

- ✓ du périmètre d'audit et de sa complexité ;
- ✓ des exigences de sécurité attendues du système d'information audité.

d) Afin de réduire le volume global d'éléments à auditer et donc le coût de l'audit, et tout en conservant un périmètre d'audit pertinent, il devrait être réalisé un échantillonnage respectant les principes suivants :

- ✓ pour les audits de configuration, seuls les serveurs les plus sensibles sont audités : contrôleurs de domaine Active Directory, serveurs de fichiers, serveurs d'infrastructure (DNS, SMTP, etc.), serveurs applicatifs, etc.
- ✓ pour un audit de code source, seules les parties sensibles du code source sont auditées : gestion des authentifications, gestion des contrôles d'accès des utilisateurs, accès aux bases de données, contrôle des saisies utilisateur, etc.

e) Il est préférable de réaliser les tests d'intrusion sur un environnement de test (ou de « pré-production ») afin d'éviter les conséquences liées aux éventuels dysfonctionnements sur un environnement de production. Ceci dit, afin de garantir la pertinence de l'audit, il convient de s'assurer que cet environnement est similaire à celui de production.

L'applicabilité des résultats des audits techniques dans l'environnement de production doit être vérifiée. Les audits d'architecture, de configuration, de code source et organisationnels doivent être réalisés dans l'environnement de production.

f) La définition du périmètre d'un audit doit être basée sur une analyse préalable des risques « métier » de l'audité. Il est recommandé au commanditaire de l'audit d'indiquer les éléments les plus sensibles de la cible auditée au prestataire d'audit.

g) Il est recommandé que le commanditaire de l'audit désigne, en son sein, un référent chargé de la gestion des relations avec le prestataire d'audit et des modalités de réalisation des activités d'audit (horaires des interventions, autorisations, etc.).

h) Il est recommandé que le commanditaire et l'audité prennent les mesures de sauvegarde nécessaires à la protection de leurs systèmes d'information et de leurs données préalablement à tout audit.

i) Il est recommandé que le commanditaire de l'audit ait la capacité à révoquer un auditeur.

j) Il est recommandé que le commanditaire de l'audit demande au prestataire d'audit de lui fournir les attestations de compétence des auditeurs.

2. Types d'audit recommandés par l'Agence Monégasque de Sécurité Numérique

L'Agence Monégasque de Sécurité Numérique recommande aux commanditaires d'audits et aux prestataires d'audit de recourir et demander des audits composés des activités d'audit suivantes :

- ✓ audit applicatif :
  - o audit de code source,
  - o audit de configuration (serveur d'application, serveur HTTP, base de données, etc.) ;
- ✓ audit d'un centre serveur :
  - o audit d'architecture (liaison entre les différentes zones et entités, filtrage, etc.),
  - o audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure),
  - o audit organisationnel et physique ;
- ✓ audit d'un réseau bureautique :
  - o audit d'architecture,
  - o audit de configuration (postes bureautique, équipements réseau, serveurs bureautique, serveurs AD, etc.),
  - o audit organisationnel et physique ;
- ✓ audit d'une plate-forme de téléphonie :
  - o audit d'architecture,
  - o audit de configuration (équipements réseau et de sécurité, IPBX, téléphones, etc.) ;
- ✓ audit d'une plate-forme de virtualisation :
  - o audit d'architecture,
  - o audit de configuration (équipements réseau et de sécurité, systèmes de virtualisation, etc.) ;
- ✓ audit de système industriel, dont la salle de contrôle :
  - o audit d'architecture,
  - o audit de configuration (automates programmables industriels, capteurs/ actionneurs, serveurs d'applications, stations opérateur, stations d'ingénierie, consoles de programmation, équipements réseau et de sécurité, serveurs d'authentification, etc.),
  - o audit organisationnel et physique,
  - o audit de code source (automates programmables industriels, pupitres, systèmes embarqués, applications métier, etc.).

Cette liste est non exhaustive et peut être complétée par les commanditaires d'audits et les prestataires d'audit.

a) Chacun des types d'audit décrits ci-dessus peut inclure l'activité de tests d'intrusion.

b) En revanche, l'activité de tests d'intrusion ne doit jamais être réalisée seule et sans aucune autre activité d'audit. En effet, un test d'intrusion peut servir de complément pour un audit de configuration ou de code auquel il est adossé afin d'améliorer la portée, en terme d'impacts, de ce dernier. Ceci permet par exemple de vérifier qu'une faille découverte lors d'un audit de code source est bien exploitable dans les conditions d'exploitation de la plate-forme, ainsi que les conséquences de cette exploitation (exécution de code, fuite d'informations, rebond, etc.).

c) Les tests d'intrusion ne devraient pas être réalisés sur des plates-formes d'hébergement mutualisées sauf accord express de l'hébergeur et après que les risques aient été évalués et maîtrisés, et que les responsabilités aient été clairement établies.

Appendice 4 :

Échelle de classification des vulnérabilités

Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, sont classées en fonction du risque qu'elles font peser sur le système d'information, c'est-à-dire en fonction de l'impact de la vulnérabilité sur le système d'information et de sa difficulté d'exploitation.

Le niveau du risque lié à chaque vulnérabilité est apprécié selon l'échelle de valeur suivante :

- ✓ Mineur : faible risque sur le système d'information et pouvant nécessiter une correction ;
- ✓ Important : risque modéré sur le système d'information et nécessitant une correction à moyen terme ;
- ✓ Majeur : risque majeur sur le système d'information nécessitant une correction à court terme ;
- ✓ Critique : risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

La facilité d'exploitation correspond au niveau d'expertise et aux moyens nécessaires à la réalisation de l'attaque. Elle est appréciée selon l'échelle suivante :

- ✓ Facile : exploitation triviale, sans outil particulier ;
- ✓ Modérée : exploitation nécessitant des techniques simples et des outils disponibles publiquement ;
- ✓ Elevée : exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d'information et le développement d'outils simples ;
- ✓ Difficile : exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d'information et le développement d'outils spécifiques et ciblés.

L'impact correspond aux conséquences que l'exploitation de la vulnérabilité peut entrainer sur le système d'information de l'audité. Il est apprécié selon l'échelle suivante :

- ✓ Mineur : pas de conséquence directe sur la sécurité du système d'information audité ;
- ✓ Important : conséquences isolées sur des points précis du système d'information audité ;
- ✓ Majeur : conséquences restreintes sur une partie du système d'information audité ;
- ✓ Critique : conséquences généralisées sur l'ensemble du système d'information audité.

Appendice 5 :

Protection des systèmes d'information des prestataires d'audit de la sécurité des systèmes d'information (PASSI)

1. Définitions

Certaines informations qu'il n'y a pas lieu de classifier peuvent recevoir, de la part de leur émetteur, une marque de confidentialité destinée à restreindre leur diffusion à un domaine spécifique (précisé par une mention particulière[5]) ou à garantir leur protection (telle que DIFFUSION RESTREINTE)[6].

Les systèmes d'information sensibles sont ceux qui traitent de ces informations. Les systèmes d'information des PASSI qualifiés sont des systèmes d'information sensibles.

2. Champ d'application

Cet Appendice s'applique aux systèmes d'information des PASSI dans le cadre de leurs prestations d'audit qualifié.

3. Principes stratégiques appliqués

Les règles décrites dans le présent Appendice s'appuient sur cinq principes stratégiques :

- ✓ mettre en place une organisation consacrée à la sécurité des systèmes d'information, incluant des volets préventifs et défensifs et reposant sur des moyens humains, matériels et financiers identifiés ;
- ✓ évaluer les risques périodiquement, dans une démarche d'amélioration continue de la sécurité de chaque système pendant leur durée de vie ;
- ✓ défendre en profondeur, en s'assurant dès la conception que si l'une des mesures de sécurité est compromise ou défaillante, d'autres assurent la protection des informations sensibles ;
- ✓ respecter les règles élémentaires d'hygiène informatique, mises en œuvre par des administrateurs de systèmes d'information formés à cet effet ;
- ✓ recourir à des produits de sécurité agréés, qualifiés ou, à défaut, certifiés et à des prestataires de services de confiance qualifiés par l'Agence Monégasque de Sécurité Numérique conformément à l'arrêté ministériel, à paraître ultérieurement, portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré (Référentiel Général de Sécurité et ses Annexes) et les référentiels et guides relatifs à la sécurité des systèmes d'information de l'Agence Monégasque de Sécurité Numérique (voir Appendice 1), précité.

4. Application des règles

Les PASSI qui mettent en œuvre des systèmes d'information sensibles appliquent les règles prévues au paragraphe 5 du présent Appendice en plus de celles de leur politique de sécurité des systèmes d'information (PSSI). Cette PSSI s'inspirera de la PSSI de l'État (PSSI-E, annexe à l'arrêté ministériel n° 2017-56 du 1er février 2017 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée).

---

[5] Par exemple : « *Confidentiel Personnel* », « *Confidentiel Médical* »,» « *Confidentiel Technologie* », « *Confidentiel Industrie* », « *Confidentiel Commercial* », « *Confidentiel Concours* », information non classifiée soumise à un contrôle, ou encore « *Spécial Monaco* ».

[6] Voir l'arrêté ministériel n° 2016-723 du 12 décembre 2016, portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

5. Protection des systèmes d'information sensibles

5.1. Détermination de la sensibilité des informations

Chaque PASSI mettant en œuvre un système d'information sensible :

- ✓ identifie l'information sensible qu'il traite ;
- ✓ marque cette information par les moyens de son choix ;
- ✓ détermine, si besoin, une échelle de sensibilité correspondant à des niveaux en matière de disponibilité, d'intégrité et de confidentialité des informations de son système d'information sensible ;
- ✓ applique des mesures de protection adaptées.

Lorsque les informations sensibles transitent entre plusieurs entités, leur niveau de sensibilité est explicitement mentionné par l'entité émettrice afin qu'elles soient protégées en conséquence par l'entité destinataire en termes de disponibilité, d'intégrité et de confidentialité, pendant et après leur transit.

5.2. Gouvernance de la protection des systèmes d'information.

Les PASSI :

- ✓ appliquent leur politique de sécurité des systèmes d'information (PSSI), validée au plus haut niveau des entités et couvrant tous les aspects, techniques ou non, de la sécurité (communication, ressources humaines et financières, aspects juridiques, etc.) ;
- ✓ organisent la gouvernance et attribuent les responsabilités en matière de sécurité des systèmes d'information.

5.3. Maîtrise des risques

La PSSI des PASSI résulte d'une analyse des risques menée :

- ✓ pour tous les risques, pas seulement techniques, qu'ils soient d'origine humaine ou non ;
- ✓ pour chacun des systèmes d'information ;
- ✓ en appréciant l'impact qu'une menace sur un composant du système pourrait avoir sur les missions de l'entité, son image, son patrimoine ou la sécurité des biens et des personnes.

5.4. Homologation des systèmes d'information sensibles

Tout système d'information sensible doit faire l'objet d'une homologation de sécurité avant sa mise en service. Dans le dossier d'homologation figurent notamment les risques résiduels, c'est-à-dire ceux qui ne sont pas couverts par des mesures de protection.

L'autorité d'homologation doit être choisie au sein des PASSI, au niveau hiérarchique suffisant pour assumer la responsabilité afférente à la décision d'homologation. Elle accepte notamment les risques résiduels. Elle est en principe l'autorité qui emploie le système.

En prononçant sa décision d'homologation, l'autorité d'homologation déclare que le système d'information est conforme aux règles prévues par le présent Appendice.

5.5. Protection des systèmes d'information

Les PASSI disposent d'une cartographie de l'ensemble des systèmes d'information dont ils sont responsables. Cette cartographie est tenue à jour. Elle est nécessaire pour assurer la protection de leurs systèmes d'information.

Les PASSI protègent leurs systèmes d'information contre les menaces identifiées pendant toute leur durée de vie. La protection repose sur plusieurs volets :

- ✓ physique: elle retarde ou empêche l'accès physique des personnes non autorisées aux locaux, aux systèmes et aux informations, tout en maintenant la disponibilité des accès pour les personnes autorisées. Elle permet également d'éviter et de détecter les incidents physiques tels les défauts d'alimentation, les défauts de climatisation, les incendies et les dégâts des eaux ;
- ✓ logique : elle permet de se prémunir contre les attaques informatiques malveillantes et accidentelles mais surtout de protéger les réseaux, les équipements, les données et leurs supports, les accès logiques ainsi que l'administration des systèmes ;
- ✓ organisationnel : elle est mise en œuvre selon des processus explicitement définis dans la PSSI des PASSI.

En cas d'élévation du niveau de la menace, les PASSI renforcent les mesures de vigilance et de protection de leurs systèmes.

5.6. Gestion des incidents de sécurité des systèmes d'information

Même protégés, les PASSI doivent se préparent à subir des attaques sur leurs systèmes d'information. Ils intègrent la sécurité des systèmes d'information dans leurs procédures de gestion de crise et dans leurs exercices périodiques. Pour être en mesure d'agir pour réduire l'impact des attaques et des incidents, ils se dotent :

- ✓ d'une capacité de détection, d'analyse, de qualification et de réaction, afin notamment d'assurer la continuité de leurs missions ;
- ✓ d'un dispositif de gestion des incidents afin de détecter et d'analyser les attaques et de réagir face à des événements anormaux.

Des retours d'expérience de traitement des incidents sont prévus après chaque événement.

5.7. Évaluation du niveau de sécurité

Les PASSI évaluent en permanence le niveau de sécurité de leurs systèmes d'information et les risques résiduels. Ils effectuent régulièrement des vérifications et réalisent des audits fonctionnels et techniques de sécurité des systèmes d'information. Cette évaluation permet de réduire l'impact des attaques et des incidents et d'assurer la continuité de service.

imprimé sur papier PEFC

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO